Dyer, Lara

From: Dyer, Lara
Sent: September-19-13 6:24 PM
To: Picard, Josée
Subject: Re: Media Request: Hill Times - Lawful Access

Thanks, Josee! Have a good night.

Lara

From: Picard, Josée
Sent: Thursday, September 19, 2013 05:32 PM
To: Dyer, Lara
Cc: Miller, Kevin; Duval, Jean Paul; Willey, Chris; Carta, John; Chayer, Marie-Helene; Plunkett, Shawn
Subject: RE: Media Request: Hill Times - Lawful Access

Lara, please find Industry Canada`s final response to the third question:

The condition of licence on lawful access on spectrum licences requires a valid warrant to be presented, and has remained essentially the same since it was first imposed in 1996 at the request of the then-Solicitor General of Canada. The minor changes made since then have simply ensured that the condition of licence remains relevant with respect to changes in legislation and technology.

Have a good evening,
Josée

From: Dyer, Lara
Sent: September-19-13 4:39 PM
To: Picard, Josée
Cc: Miller, Kevin; Duval, Jean Paul; Willey, Chris; Carta, John; Chayer, Marie-Helene; Plunkett, Shawn
Subject: RE: Media Request: Hill Times - Lawful Access

Great, thank you – please note one factual correction to the lines provided; the second bullet should read "being made" instead of "being contemplated". In other words:

- Public Safety Canada and Industry Canada have been working together since 1995 with respect to the lawful interception condition of licence. The only change **being made** to the lawful interception condition of licence is simply to bring the language of the condition in line with today's technologies.

Many thanks,
Lara

From: Picard, Josée
Sent: Thursday, September 19, 2013 4:34 PM
To: Dyer, Lara
Cc: Miller, Kevin; Duval, Jean Paul; Willey, Chris; Carta, John; Chayer, Marie-Helene; Plunkett, Shawn
Subject: RE: Media Request: Hill Times - Lawful Access

Thanks Lara, very much appreciated.

We will share the final responses from IC for your information upon receipt.

Thanks,
Josée

From: Dyer, Lara
Sent: September-19-13 4:25 PM
To: Picard, Josée
Cc: Miller, Kevin; Duval, Jean Paul; Willey, Chris; Carta, John; Chayer, Marie-Helene; Plunkett, Shawn
Subject: RE: Media Request: Hill Times - Lawful Access

Hi, folks – please find following lines that have been approved by Michael MacDonald, in case they are needed at some point. If you have any questions, please let us know.

Best,
Lara

Lara Dyer
613.991.3240

*****

Q3. Some critics say that the government has approved expanded telecomms surveillance without legislation, through spectrum licensing for example. How does your office respond to this claim?

- Public Safety Canada's mission is to build a safe and resilient Canada. We do this in part by ensuring that law enforcement and national security agencies have the tools they need to protect Canada and Canadians.
- Industry Canada is responsible for the lawful interception condition of licence.
- Public Safety Canada and Industry Canada have been working together since 1995 with respect to the lawful interception condition of licence. The only change being contemplated to the lawful interception condition of licence is simply to bring the language of the condition in line with today's technologies.
- For example, the original condition of licence referred to 'circuit-switched' network technologies; however, telecommunications companies are currently moving away from 'circuit-switched' networks toward newer, state-of-the-art technologies. As technologies advance, so too must the tools that regulate them.
- A court-authorized warrant is required at all times to intercept the communications of Canadians, except in rare circumstances of imminent harm (such as bomb threats or kidnappings). This safeguard ensures that we balance the protection of Canadian life and property with the protection of privacy.

From: Plunkett, Shawn
Sent: Thursday, September 19, 2013 3:18 PM
To: Picard, Josée
Cc: Miller, Kevin; Duval, Jean Paul; Willey, Chris; Carta, John; Dyer, Lara
Subject: RE: Media Request: Hill Times - Lawful Access

Hi Josée, we are working on your request and will have approved lines for you as soon as we can.

Thanks

From: Picard, Josée
Sent: September-19-13 3:14 PM
To: Plunkett, Shawn
Cc: Miller, Kevin; Duval, Jean Paul; Willey, Chris; Carta, John
Subject: RE: Media Request: Hill Times - Lawful Access

Hi Shawn, just following up on the request below.

Thanks,
Josée

From: Picard, Josée
Sent: September-19-13 2:06 PM
To: Plunkett, Shawn
Cc: Miller, Kevin; Duval, Jean Paul; Willey, Chris; Carta, John
Subject: Media Request: Hill Times - Lawful Access

Good afternoon Shawn,

We received a request from the Hill Times on Lawful Access (via our MO). DoJ has agreed to take the first two questions, however, they advised that they can`t respond to Q3 re: spectrum licensing.

Please find our proposed response for your review and approval.

Please note that the reporter`s deadline is 4pm. Glad to discuss as needed.

Many thanks,
Josée
613-949-4288

Q3. Some critics say that the government has approved expanded telecomms surveillance without legislation, through spectrum licensing for example. How does your office respond to this claim?

- Current federal legislation *allows* telecommunications service providers to release basic subscriber information to authorities without a warrant. However, *they are not required to do so.*

- Access to the actual content of communications, or tracking of an individual or a telecommunications device, requires judicial authorization, except in exigent or exceptional circumstances, as per current legislation governing interception.

Request:

s.19(1)

Title	[redacted]
Media Outlet	The Hill Times
Call Date	9/18/2013 4:00 PM
Telephone	Office: [redacted] / Cell: [redacted]
E-mail address	[redacted]@hilltimes.com
Deadline	9/18/2013 4:00 PM
Status	Consulting
Branch	NS

Subject	Lawful Access
Questions	I'm following the issue of lawful access and telecommunications surveillance this week and I am looking for some response to the following questions. My questions are: 1. Will the government reintroduce lawful access legislation when Parliament returns? 2. What checks are in place to protect citizens' privacy from unwarranted surveillance? 3. Some critics say that the government has approved expanded telecomms surveillance without legislation, through spectrum licensing for example. How does your office respond to this claim? I'm putting these questions to your office as it was the previous Public Safety Minister who previously introduced lawful access legislation. My deadline is tomorrow at 5, please let me know who the response are attributable to. Thanks for your help,

Josée Picard
Media Relations / Relations avec les médias
Ministère de la sécurité publique | Department of Public Safety
T : 613-949-4288 | F : 613-954-4779
josee.picard@ps-sp.gc.ca

Dyer, Lara

From:	Dyer, Lara
Sent:	September-19-13 4:43 PM
To:	MacDonald, Michael
Cc:	Chayer, Marie-Helene
Subject:	FW: Media Request: Hill Times - Lawful Access

FYI – Shawn noted that the decision has already been taken.

From: Dyer, Lara
Sent: Thursday, September 19, 2013 4:39 PM
To: Picard, Josée
Cc: Miller, Kevin; Duval, Jean Paul; Willey, Chris; Carta, John; Chayer, Marie-Helene; Plunkett, Shawn
Subject: RE: Media Request: Hill Times - Lawful Access

Great, thank you – please note one factual correction to the lines provided; the second bullet should read "being made" instead of "being contemplated". In other words:

- Public Safety Canada and Industry Canada have been working together since 1995 with respect to the lawful interception condition of licence. The only change **being made** to the lawful interception condition of licence is simply to bring the language of the condition in line with today's technologies.

Many thanks,
Lara

From: Picard, Josée
Sent: Thursday, September 19, 2013 4:34 PM
To: Dyer, Lara
Cc: Miller, Kevin; Duval, Jean Paul; Willey, Chris; Carta, John; Chayer, Marie-Helene; Plunkett, Shawn
Subject: RE: Media Request: Hill Times - Lawful Access

Thanks Lara, very much appreciated.

We will share the final responses from IC for your information upon receipt.

Thanks,
Josée

From: Dyer, Lara
Sent: September-19-13 4:25 PM
To: Picard, Josée
Cc: Miller, Kevin; Duval, Jean Paul; Willey, Chris; Carta, John; Chayer, Marie-Helene; Plunkett, Shawn
Subject: RE: Media Request: Hill Times - Lawful Access

Hi, folks – please find following lines that have been approved by Michael MacDonald, in case they are needed at some point. If you have any questions, please let us know.

Best,
Lara

Lara Dyer
613.991.3240

*****

Q3. Some critics say that the government has approved expanded telecomms surveillance without legislation, through spectrum licensing for example. How does your office respond to this claim?

- Public Safety Canada's mission is to build a safe and resilient Canada. We do this in part by ensuring that law enforcement and national security agencies have the tools they need to protect Canada and Canadians.
- Industry Canada is responsible for the lawful interception condition of licence.
- Public Safety Canada and Industry Canada have been working together since 1995 with respect to the lawful interception condition of licence. The only change being contemplated to the lawful interception condition of licence is simply to bring the language of the condition in line with today's technologies.
- For example, the original condition of licence referred to 'circuit-switched' network technologies; however, telecommunications companies are currently moving away from 'circuit-switched' networks toward newer, state-of-the-art technologies. As technologies advance, so too must the tools that regulate them.
- A court-authorized warrant is required at all times to intercept the communications of Canadians, except in rare circumstances of imminent harm (such as bomb threats or kidnappings). This safeguard ensures that we balance the protection of Canadian life and property with the protection of privacy.

From: Plunkett, Shawn
Sent: Thursday, September 19, 2013 3:18 PM
To: Picard, Josée
Cc: Miller, Kevin; Duval, Jean Paul; Willey, Chris; Carta, John; Dyer, Lara
Subject: RE: Media Request: Hill Times - Lawful Access

Hi Josée, we are working on your request and will have approved lines for you as soon as we can.

Thanks

From: Picard, Josée
Sent: September-19-13 3:14 PM
To: Plunkett, Shawn
Cc: Miller, Kevin; Duval, Jean Paul; Willey, Chris; Carta, John
Subject: RE: Media Request: Hill Times - Lawful Access

Hi Shawn, just following up on the request below.

Thanks,
Josée

From: Picard, Josée
Sent: September-19-13 2:06 PM
To: Plunkett, Shawn
Cc: Miller, Kevin; Duval, Jean Paul; Willey, Chris; Carta, John
Subject: Media Request: Hill Times - Lawful Access

Good afternoon Shawn,

We received a request from the Hill Times on Lawful Access (via our MO). DoJ has agreed to take the first two questions, however, they advised that they can`t respond to Q3 re: spectrum licensing.

Please find our proposed response for your review and approval.

Please note that the reporter`s deadline is 4pm. Glad to discuss as needed.

Many thanks,
Josée
613-949-4288

Q3. Some critics say that the government has approved expanded telecomms surveillance without legislation, through spectrum licensing for example. How does your office respond to this claim?

- Current federal legislation *allows* telecommunications service providers to release basic subscriber information to authorities without a warrant. However, *they are not required to do so.*

- Access to the actual content of communications, or tracking of an individual or a telecommunications device, requires judicial authorization, except in exigent or exceptional circumstances, as per current legislation governing interception.

Request:

Title	[redacted]
Media Outlet	The Hill Times
Call Date	9/18/2013 4:00 PM
Telephone	Office: [redacted] / Cell: [redacted]
E-mail address	[redacted]@hilltimes.com
Deadline	9/18/2013 4:00 PM
Status	Consulting
Branch	NS
Subject	Lawful Access
Questions	I'm following the issue of lawful access and telecommunications surveillance this week and I am looking for some response to the following questions. My questions are: 1. Will the government reintroduce lawful access legislation when Parliament returns? 2. What checks are in place to protect citizens' privacy from unwarranted surveillance? 3. Some critics say that the government has approved expanded telecomms surveillance without legislation, through spectrum licensing for example. How does your office respond to this claim? I'm putting these questions to your office as it was the previous Public Safety Minister who previously introduced lawful access legislation. My deadline is tomorrow at 5, please let me know who the response are attributable to. Thanks for your help,

s.19(1)

Josée Picard
Media Relations / Relations avec les médias
Ministère de la sécurité publique | Department of Public Safety
T : 613-949-4288 | F : 613-954-4779
josee.picard@ps-sp.gc.ca

Dyer, Lara

From: Plunkett, Shawn
Sent: September-19-13 4:34 PM
To: Dyer, Lara
Subject: RE: Media Request: Hill Times - Lawful Access

Not sure that these will be used, but if so would need to change 'contemplated', as the decision has already been taken.

From: Dyer, Lara
Sent: September-19-13 4:25 PM
To: Picard, Josée
Cc: Miller, Kevin; Duval, Jean Paul; Willey, Chris; Carta, John; Chayer, Marie-Helene; Plunkett, Shawn
Subject: RE: Media Request: Hill Times - Lawful Access

Hi, folks – please find following lines that have been approved by Michael MacDonald, in case they are needed at some point. If you have any questions, please let us know.

Best,
Lara

Lara Dyer
613.991.3240

*****

Q3. Some critics say that the government has approved expanded telecomms surveillance without legislation, through spectrum licensing for example. How does your office respond to this claim?

- Public Safety Canada's mission is to build a safe and resilient Canada. We do this in part by ensuring that law enforcement and national security agencies have the tools they need to protect Canada and Canadians.
- Industry Canada is responsible for the lawful interception condition of licence.
- Public Safety Canada and Industry Canada have been working together since 1995 with respect to the lawful interception condition of licence. The only change being contemplated to the lawful interception condition of licence is simply to bring the language of the condition in line with today's technologies.
- For example, the original condition of licence referred to 'circuit-switched' network technologies; however, telecommunications companies are currently moving away from 'circuit-switched' networks toward newer, state-of-the-art technologies. As technologies advance, so too must the tools that regulate them.
- A court-authorized warrant is required at all times to intercept the communications of Canadians, except in rare circumstances of imminent harm (such as bomb threats or kidnappings). This safeguard ensures that we balance the protection of Canadian life and property with the protection of privacy.

From: Plunkett, Shawn
Sent: Thursday, September 19, 2013 3:18 PM
To: Picard, Josée
Cc: Miller, Kevin; Duval, Jean Paul; Willey, Chris; Carta, John; Dyer, Lara
Subject: RE: Media Request: Hill Times - Lawful Access

Hi Josée, we are working on your request and will have approved lines for you as soon as we can.

Thanks

From: Picard, Josée
Sent: September-19-13 3:14 PM
To: Plunkett, Shawn
Cc: Miller, Kevin; Duval, Jean Paul; Willey, Chris; Carta, John
Subject: RE: Media Request: Hill Times - Lawful Access

Hi Shawn, just following up on the request below.

Thanks,
Josée

From: Picard, Josée
Sent: September-19-13 2:06 PM
To: Plunkett, Shawn
Cc: Miller, Kevin; Duval, Jean Paul; Willey, Chris; Carta, John
Subject: Media Request: Hill Times - Lawful Access

Good afternoon Shawn,

We received a request from the Hill Times on Lawful Access (via our MO). DoJ has agreed to take the first two questions, however, they advised that they can`t respond to Q3 re: spectrum licensing.

Please find our proposed response for your review and approval.

Please note that the reporter`s deadline is 4pm. Glad to discuss as needed.

Many thanks,
Josée
613-949-4288

Q3. Some critics say that the government has approved expanded telecomms surveillance without legislation, through spectrum licensing for example. How does your office respond to this claim?

- Current federal legislation *allows* telecommunications service providers to release basic subscriber information to authorities without a warrant. However, *they are not required to do so.*

- Access to the actual content of communications, or tracking of an individual or a telecommunications device, requires judicial authorization, except in exigent or exceptional circumstances, as per current legislation governing interception.

Request:

s.19(1)

Title	[redacted]
Media Outlet	The Hill Times
Call Date	9/18/2013 4:00 PM
Telephone	Office: [redacted] / Cell: [redacted]
E-mail address	[redacted]@hilltimes.com

Deadline	9/18/2013 4:00 PM
Status	Consulting
Branch	NS
Subject	Lawful Access
Questions	I'm following the issue of lawful access and telecommunications surveillance this week and I am looking for some response to the following questions. My questions are: 1. Will the government reintroduce lawful access legislation when Parliament returns? 2. What checks are in place to protect citizens' privacy from unwarranted surveillance? 3. Some critics say that the government has approved expanded telecomms surveillance without legislation, through spectrum licensing for example. How does your office respond to this claim? I'm putting these questions to your office as it was the previous Public Safety Minister who previously introduced lawful access legislation. My deadline is tomorrow at 5, please let me know who the response are attributable to. Thanks for your help,

Josée Picard
Media Relations / Relations avec les médias
Ministère de la sécurité publique | Department of Public Safety
T : 613-949-4288 | F : 613-954-4779
josee.picard@ps-sp.gc.ca

Dyer, Lara

From:	Dyer, Lara
Sent:	September-19-13 3:48 PM
To:	Chayer, Marie-Helene
Subject:	RE: Media Request: Hill Times - Lawful Access (Deadline 4pm)

Tks!

From: Chayer, Marie-Helene
Sent: Thursday, September 19, 2013 3:47 PM
To: Dyer, Lara
Subject: Re: Media Request: Hill Times - Lawful Access (Deadline 4pm)

Looks good. Thanks.

From: Dyer, Lara
Sent: Thursday, September 19, 2013 03:44 PM
To: Chayer, Marie-Helene
Subject: FW: Media Request: Hill Times - Lawful Access (Deadline 4pm)

Update: IC has indicated that they want to respond. We've asked to see their lines, for info. Just in case things change again, we'll finalize our lines with Mike and provide to Comms. Here's the current version... if you have comments, please let me know.

- Public Safety Canada's mission is to build a safe and resilient Canada. We do this in part by ensuring that law enforcement and national security agencies have the tools they need to protect Canada and Canadians.
- Industry Canada is responsible for the lawful interception condition of licence.
- Public Safety Canada and Industry Canada have been working together since 1995 with respect to the lawful interception condition of licence. The only change being contemplated to the lawful intercept condition of spectrum licence is simply to bring the language of the condition in line with today's technologies.
- For example, the original condition of licence referred to 'circuit-switched' network technologies; however, telecommunications companies are currently moving away from 'circuit-switched' networks toward newer, state-of-the-art technologies. As technologies advance, so too must the tools that regulate them.
- A warrant is required at all times to intercept the communications of Canadians, except in rare circumstances of imminent harm (such as bomb threats or kidnappings). This safeguard ensures that we balance the protection of Canadian life and property with the protection of privacy.

From: Chayer, Marie-Helene
Sent: Thursday, September 19, 2013 3:11 PM
To: Hawrylak, Maciek; Plunkett, Shawn; Dyer, Lara
Subject: Re: Media Request: Hill Times - Lawful Access (Deadline 4pm)

s.21(1)(b)

[redacted]

From: Hawrylak, Maciek
Sent: Thursday, September 19, 2013 03:09 PM
To: Chayer, Marie-Helene; Plunkett, Shawn; Dyer, Lara
Subject: RE: Media Request: Hill Times - Lawful Access (Deadline 4pm)

The line is:

"With the exception of situations where there is imminent harm, such as bomb threats or kidnappings, the communications of Canadians will never be intercepted without a warrant. At all times we will balance protection of Canadian life and property with the protection of privacy."

Maciek

From: Chayer, Marie-Helene
Sent: September-19-13 3:08 PM
To: Plunkett, Shawn; Hawrylak, Maciek; Dyer, Lara
Subject: Re: Media Request: Hill Times - Lawful Access (Deadline 4pm)

Agreed.
I would however keep comms last bullet about the requirement for a warrant. However, let's use the language we developed on this. We used it in a ministerial correspondence that Maciek worked on recently.

If Mike is around, he should approve the lines.
Thx

From: Plunkett, Shawn
Sent: Thursday, September 19, 2013 02:53 PM
To: Dyer, Lara
Cc: Hawrylak, Maciek; Chayer, Marie-Helene
Subject: RE: Media Request: Hill Times - Lawful Access (Deadline 4pm)

I amended the fourth bullet (and removed the last). I would also suggest that we recommend to comms that IC comms be consulted (they should sign off on any references to the condition).

From: Plunkett, Shawn
Sent: September-19-13 2:27 PM
To: Chayer, Marie-Helene; Dyer, Lara
Cc: Hawrylak, Maciek
Subject: FW: Media Request: Hill Times - Lawful Access (Deadline 4pm)
Importance: High

I would proposed the following in lieu of the proposed comms response. The below lines (except for the first bullet) were approved by Mike last year in response to a Wire Report article that suggested the CoL was an attempt to "sneak" lawful access through the backdoor. **Deadline is 4pm**.

Q3 Some critics say that the government has approved expanded telecomms surveillance without legislation, through spectrum licensing for example. How does your office respond to this claim?

- Industry Canada is responsible for the lawful interception condition of licence.
- Public Safety Canada's mission is to build a safe and resilient Canada. We do this in part by ensuring that law enforcement and national security agencies have the tools they need to protect Canada and Canadians.

- As such, Public Safety Canada and Industry Canada have been working together since 1995 with respect to the lawful interception condition of licence.
- Changes are being made to the lawful intercept condition of licence simply to bring the language of the condition in line with today's technologies.

From: Picard, Josée
Sent: September-19-13 2:06 PM
To: Plunkett, Shawn
Cc: Miller, Kevin; Duval, Jean Paul; Willey, Chris; Carta, John
Subject: Media Request: Hill Times - Lawful Access

Good afternoon Shawn,

We received a request from the Hill Times on Lawful Access (via our MO). DoJ has agreed to take the first two questions, however, they advised that they can`t respond to Q3 re: spectrum licensing.

Please find our proposed response for your review and approval.

Please note that the reporter`s deadline is 4pm. Glad to discuss as needed.

Many thanks,
Josée
613-949-4288

Q3. Some critics say that the government has approved expanded telecomms surveillance without legislation, through spectrum licensing for example. How does your office respond to this claim?

- Current federal legislation *allows* telecommunications service providers to release basic subscriber information to authorities without a warrant. However, *they are not required to do so.*

- Access to the actual content of communications, or tracking of an individual or a telecommunications device, requires judicial authorization, except in exigent or exceptional circumstances, as per current legislation governing interception.

Request:

s.19(1)

Title	[redacted]
Media Outlet	The Hill Times
Call Date	9/18/2013 4:00 PM
Telephone	Office: [redacted] / Cell: [redacted]
E-mail address	[redacted]@hilltimes.com
Deadline	9/18/2013 4:00 PM
Status	Consulting
Branch	NS
Subject	Lawful Access
Questions	I'm following the issue of lawful access and telecommunications surveillance this week and I am looking for some response to the following questions. My questions are: 1. Will the government reintroduce lawful access legislation when Parliament returns? 2. What checks are in place to protect citizens' privacy from unwarranted surveillance?

3. Some critics say that the government has approved expanded telecomms surveillance without legislation, through spectrum licensing for example. How does your office respond to this claim?

I'm putting these questions to your office as it was the previous Public Safety Minister who previously introduced lawful access legislation. My deadline is tomorrow at 5, please let me know who the response are attributable to.

Thanks for your help,

Josée Picard
Media Relations / Relations avec les médias
Ministère de la sécurité publique | Department of Public Safety
T : 613-949-4288 | F : 613-954-4779
josee.picard@ps-sp.gc.ca

Emmett, Jamie

From: Dyer, Lara
Sent: September-19-13 3:46 PM
To: Plunkett, Shawn; Hawrylak, Maciek; Chayer, Marie-Helene
Cc: McKinnon, Korey
Subject: RE: Media Request: Hill Times - Lawful Access (Deadline 4pm)

Great, Shawn... thanks. I'll ask Mike to review the lines when he's back in the office, then we can provide to Comms.

Lara

From: Plunkett, Shawn
Sent: Thursday, September 19, 2013 3:43 PM
To: Hawrylak, Maciek; Chayer, Marie-Helene; Dyer, Lara
Cc: McKinnon, Korey
Subject: RE: Media Request: Hill Times - Lawful Access (Deadline 4pm)

Hi,
Just got off the phone with comms. Industry Canada wants the question, so we can stand down (they did suggest that it would be useful to approve the lines we developed just in case).

I've asked comms to try and get IC's lines.

Thanks everyone for their efforts.

From: Hawrylak, Maciek
Sent: September-19-13 3:17 PM
To: Chayer, Marie-Helene; Plunkett, Shawn; Dyer, Lara
Subject: RE: Media Request: Hill Times - Lawful Access (Deadline 4pm)

s.21(1)(b)

[redacted]

Maciek

From: Chayer, Marie-Helene
Sent: September-19-13 3:11 PM
To: Hawrylak, Maciek; Plunkett, Shawn; Dyer, Lara
Subject: Re: Media Request: Hill Times - Lawful Access (Deadline 4pm)

[redacted]

From: Hawrylak, Maciek
Sent: Thursday, September 19, 2013 03:09 PM
To: Chayer, Marie-Helene; Plunkett, Shawn; Dyer, Lara
Subject: RE: Media Request: Hill Times - Lawful Access (Deadline 4pm)

The line is:

"With the exception of situations where there is imminent harm, such as bomb threats or kidnappings, the communications of Canadians will never be intercepted without a warrant. At all times we will balance protection of Canadian life and property with the protection of privacy."

Maciek

From: Chayer, Marie-Helene
Sent: September-19-13 3:08 PM
To: Plunkett, Shawn; Hawrylak, Maciek; Dyer, Lara
Subject: Re: Media Request: Hill Times - Lawful Access (Deadline 4pm)

Agreed.
I would however keep comms last bullet about the requirement for a warrant. However, let's use the language we developed on this. We used it in a ministerial correspondence that Maciek worked on recently.

If Mike is around, he should approve the lines.
Thx

From: Plunkett, Shawn
Sent: Thursday, September 19, 2013 02:53 PM
To: Dyer, Lara
Cc: Hawrylak, Maciek; Chayer, Marie-Helene
Subject: RE: Media Request: Hill Times - Lawful Access (Deadline 4pm)

I amended the fourth bullet (and removed the last). I would also suggest that we recommend to comms that IC comms be consulted (they should sign off on any references to the condition).

From: Plunkett, Shawn
Sent: September-19-13 2:27 PM
To: Chayer, Marie-Helene; Dyer, Lara
Cc: Hawrylak, Maciek
Subject: FW: Media Request: Hill Times - Lawful Access (Deadline 4pm)
Importance: High

I would proposed the following in lieu of the proposed comms response. The below lines (except for the first bullet) were approved by Mike last year in response to a Wire Report article that suggested the CoL was an attempt to "sneak" lawful access through the backdoor. **Deadline is 4pm**.

Q3 Some critics say that the government has approved expanded telecomms surveillance without legislation, through spectrum licensing for example. How does your office respond to this claim?

- Industry Canada is responsible for the lawful interception condition of licence.
- Public Safety Canada's mission is to build a safe and resilient Canada. We do this in part by ensuring that law enforcement and national security agencies have the tools they need to protect Canada and Canadians.
- As such, Public Safety Canada and Industry Canada have been working together since 1995 with respect to the lawful interception condition of licence.
- Changes are being made to the lawful intercept condition of licence simply to bring the language of the condition in line with today's technologies.

From: Picard, Josée
Sent: September-19-13 2:06 PM
To: Plunkett, Shawn
Cc: Miller, Kevin; Duval, Jean Paul; Willey, Chris; Carta, John
Subject: Media Request: Hill Times - Lawful Access

Good afternoon Shawn,

We received a request from the Hill Times on Lawful Access (via our MO). DoJ has agreed to take the first two questions, however, they advised that they can`t respond to Q3 re: spectrum licensing.

Please find our proposed response for your review and approval.

Please note that the reporter`s deadline is 4pm. Glad to discuss as needed.

Many thanks,
Josée
613-949-4288

Q3. Some critics say that the government has approved expanded telecomms surveillance without legislation, through spectrum licensing for example. How does your office respond to this claim?

- Current federal legislation *allows* telecommunications service providers to release basic subscriber information to authorities without a warrant. However, *they are not required to do so.*
- Access to the actual content of communications, or tracking of an individual or a telecommunications device, requires judicial authorization, except in exigent or exceptional circumstances, as per current legislation governing interception.

Request:

s.19(1)

Title	[redacted]
Media Outlet	The Hill Times
Call Date	9/18/2013 4:00 PM
Telephone	Office: [redacted] / Cell: [redacted]
E-mail address	[redacted]@hilltimes.com
Deadline	9/18/2013 4:00 PM
Status	Consulting
Branch	NS
Subject	Lawful Access
Questions	I'm following the issue of lawful access and telecommunications surveillance this week and I am looking for some response to the following questions. My questions are: 1. Will the government reintroduce lawful access legislation when Parliament returns? 2. What checks are in place to protect citizens' privacy from unwarranted surveillance? 3. Some critics say that the government has approved expanded telecomms surveillance without legislation, through spectrum licensing for example. How does your office respond to this claim? I'm putting these questions to your office as it was the previous Public Safety Minister who previously introduced lawful access legislation. My deadline is tomorrow at 5, please let me know who the response are attributable to. Thanks for your help,

Josée Picard
Media Relations / Relations avec les médias
Ministère de la sécurité publique | Department of Public Safety
T : 613-949-4288 | F : 613-954-4779
josee.picard@ps-sp.gc.ca

Dyer, Lara

From: Dyer, Lara
Sent: September-19-13 3:16 PM
To: Chayer, Marie-Helene
Subject: RE: Media Request: Hill Times - Lawful Access (Deadline 4pm)

P.S. Mike was running off to a meeting, but I've arranged with him that he'll approve the lines before we send them to Comms.

From: Chayer, Marie-Helene
Sent: Thursday, September 19, 2013 3:11 PM
To: Hawrylak, Maciek; Plunkett, Shawn; Dyer, Lara
Subject: Re: Media Request: Hill Times - Lawful Access (Deadline 4pm)

[redacted]

s.21(1)(b)

From: Hawrylak, Maciek
Sent: Thursday, September 19, 2013 03:09 PM
To: Chayer, Marie-Helene; Plunkett, Shawn; Dyer, Lara
Subject: RE: Media Request: Hill Times - Lawful Access (Deadline 4pm)

The line is:

"With the exception of situations where there is imminent harm, such as bomb threats or kidnappings, the communications of Canadians will never be intercepted without a warrant. At all times we will balance protection of Canadian life and property with the protection of privacy."

Maciek

From: Chayer, Marie-Helene
Sent: September-19-13 3:08 PM
To: Plunkett, Shawn; Hawrylak, Maciek; Dyer, Lara
Subject: Re: Media Request: Hill Times - Lawful Access (Deadline 4pm)

Agreed.
I would however keep comms last bullet about the requirement for a warrant. However, let's use the language we developed on this. We used it in a ministerial correspondence that Maciek worked on recently.

If Mike is around, he should approve the lines.
Thx

From: Plunkett, Shawn
Sent: Thursday, September 19, 2013 02:53 PM
To: Dyer, Lara
Cc: Hawrylak, Maciek; Chayer, Marie-Helene
Subject: RE: Media Request: Hill Times - Lawful Access (Deadline 4pm)

I amended the fourth bullet (and removed the last). I would also suggest that we recommend to comms that IC comms be consulted (they should sign off on any references to the condition).

From: Plunkett, Shawn
Sent: September-19-13 2:27 PM
To: Chayer, Marie-Helene; Dyer, Lara
Cc: Hawrylak, Maciek
Subject: FW: Media Request: Hill Times - Lawful Access (Deadline 4pm)
Importance: High

I would proposed the following in lieu of the proposed comms response. The below lines (except for the first bullet) were approved by Mike last year in response to a Wire Report article that suggested the CoL was an attempt to "sneak" lawful access through the backdoor. **Deadline is 4pm**.

Q3 Some critics say that the government has approved expanded telecomms surveillance without legislation, through spectrum licensing for example. How does your office respond to this claim?

- Industry Canada is responsible for the lawful interception condition of licence.
- Public Safety Canada's mission is to build a safe and resilient Canada. We do this in part by ensuring that law enforcement and national security agencies have the tools they need to protect Canada and Canadians.
- As such, Public Safety Canada and Industry Canada have been working together since 1995 with respect to the lawful interception condition of licence.
- Changes are being made to the lawful intercept condition of licence simply to bring the language of the condition in line with today's technologies.

From: Picard, Josée
Sent: September-19-13 2:06 PM
To: Plunkett, Shawn
Cc: Miller, Kevin; Duval, Jean Paul; Willey, Chris; Carta, John
Subject: Media Request: Hill Times - Lawful Access

Good afternoon Shawn,

We received a request from the Hill Times on Lawful Access (via our MO). DoJ has agreed to take the first two questions, however, they advised that they can`t respond to Q3 re: spectrum licensing.

Please find our proposed response for your review and approval.

Please note that the reporter`s deadline is 4pm. Glad to discuss as needed.

Many thanks,
Josée
613-949-4288

Q3. Some critics say that the government has approved expanded telecomms surveillance without legislation, through spectrum licensing for example. How does your office respond to this claim?

- Current federal legislation *allows* telecommunications service providers to release basic subscriber information to authorities without a warrant. However, *they are not required to do so.*

- **Access to the actual content of communications, or tracking of an individual or a telecommunications device, requires judicial authorization, except in exigent or exceptional circumstances, as per current legislation governing interception.**

Request:

s.19(1)

Title	[redacted]
Media Outlet	The Hill Times
Call Date	9/18/2013 4:00 PM
Telephone	Office: [redacted] / Cell: [redacted]
E-mail address	[redacted]@hilltimes.com
Deadline	9/18/2013 4:00 PM
Status	Consulting
Branch	NS
Subject	Lawful Access
Questions	I'm following the issue of lawful access and telecommunications surveillance this week and I am looking for some response to the following questions. My questions are: 1. Will the government reintroduce lawful access legislation when Parliament returns? 2. What checks are in place to protect citizens' privacy from unwarranted surveillance? 3. Some critics say that the government has approved expanded telecomms surveillance without legislation, through spectrum licensing for example. How does your office respond to this claim? I'm putting these questions to your office as it was the previous Public Safety Minister who previously introduced lawful access legislation. My deadline is tomorrow at 5, please let me know who the response are attributable to. Thanks for your help,

Josée Picard
Media Relations / Relations avec les médias
Ministère de la sécurité publique | Department of Public Safety
T : 613-949-4288 | F : 613-954-4779
josee.picard@ps-sp.gc.ca

Dyer, Lara

From: Dyer, Lara
Sent: September-19-13 3:15 PM
To: Chayer, Marie-Helene
Subject: RE: Media Request: Hill Times - Lawful Access (Deadline 4pm)

Marie – at Mike's suggestion, I ran the following by Michèle… your thoughts on this approach?

- Public Safety Canada's mission is to build a safe and resilient Canada. We do this in part by ensuring that law enforcement and national security agencies have the tools they need to protect Canada and Canadians.
- Industry Canada is responsible for the lawful interception condition of licence.
- Public Safety Canada and Industry Canada have been working together since 1995 with respect to the lawful interception condition of licence. The only change being contemplated to the lawful intercept condition of spectrum licence is simply to bring the language of the condition in line with today's technologies.
- For example, the original condition of licence referred to 'circuit-switched' network technologies; however, telecommunications companies are currently moving away from 'circuit-switched' networks toward newer, state-of-the-art technologies. As technologies advance, so too must the tools that regulate them.

From: Chayer, Marie-Helene
Sent: Thursday, September 19, 2013 3:11 PM
To: Hawrylak, Maciek; Plunkett, Shawn; Dyer, Lara
Subject: Re: Media Request: Hill Times - Lawful Access (Deadline 4pm)

[redacted]

s.21(1)(b)

From: Hawrylak, Maciek
Sent: Thursday, September 19, 2013 03:09 PM
To: Chayer, Marie-Helene; Plunkett, Shawn; Dyer, Lara
Subject: RE: Media Request: Hill Times - Lawful Access (Deadline 4pm)

The line is:

"With the exception of situations where there is imminent harm, such as bomb threats or kidnappings, the communications of Canadians will never be intercepted without a warrant. At all times we will balance protection of Canadian life and property with the protection of privacy."

Maciek

From: Chayer, Marie-Helene
Sent: September-19-13 3:08 PM
To: Plunkett, Shawn; Hawrylak, Maciek; Dyer, Lara
Subject: Re: Media Request: Hill Times - Lawful Access (Deadline 4pm)

Agreed.
I would however keep comms last bullet about the requirement for a warrant. However, let's use the language we developed on this. We used it in a ministerial correspondence that Maciek worked on recently.

If Mike is around, he should approve the lines.
Thx

From: Plunkett, Shawn
Sent: Thursday, September 19, 2013 02:53 PM
To: Dyer, Lara
Cc: Hawrylak, Maciek; Chayer, Marie-Helene
Subject: RE: Media Request: Hill Times - Lawful Access (Deadline 4pm)

I amended the fourth bullet (and removed the last). I would also suggest that we recommend to comms that IC comms be consulted (they should sign off on any references to the condition).

From: Plunkett, Shawn
Sent: September-19-13 2:27 PM
To: Chayer, Marie-Helene; Dyer, Lara
Cc: Hawrylak, Maciek
Subject: FW: Media Request: Hill Times - Lawful Access (Deadline 4pm)
Importance: High

I would proposed the following in lieu of the proposed comms response. The below lines (except for the first bullet) were approved by Mike last year in response to a Wire Report article that suggested the CoL was an attempt to "sneak" lawful access through the backdoor. **Deadline is 4pm**.

Q3 Some critics say that the government has approved expanded telecomms surveillance without legislation, through spectrum licensing for example. How does your office respond to this claim?

- Industry Canada is responsible for the lawful interception condition of licence.
- Public Safety Canada's mission is to build a safe and resilient Canada. We do this in part by ensuring that law enforcement and national security agencies have the tools they need to protect Canada and Canadians.
- As such, Public Safety Canada and Industry Canada have been working together since 1995 with respect to the lawful interception condition of licence.
- Changes are being made to the lawful intercept condition of licence simply to bring the language of the condition in line with today`s technologies.

From: Picard, Josée
Sent: September-19-13 2:06 PM
To: Plunkett, Shawn
Cc: Miller, Kevin; Duval, Jean Paul; Willey, Chris; Carta, John
Subject: Media Request: Hill Times - Lawful Access

Good afternoon Shawn,

We received a request from the Hill Times on Lawful Access (via our MO). DoJ has agreed to take the first two questions, however, they advised that they can`t respond to Q3 re: spectrum licensing.

Please find our proposed response for your review and approval.

Please note that the reporter`s deadline is 4pm. Glad to discuss as needed.

Many thanks,
Josée
613-949-4288

Q3. Some critics say that the government has approved expanded telecomms surveillance without legislation, through spectrum licensing for example. How does your office respond to this claim?

- Current federal legislation *allows* telecommunications service providers to release basic subscriber information to authorities without a warrant. However, *they are not required to do so.*
- Access to the actual content of communications, or tracking of an individual or a telecommunications device, requires judicial authorization, except in exigent or exceptional circumstances, as per current legislation governing interception.

Request:

s.19(1)

Title	[redacted]
Media Outlet	The Hill Times
Call Date	9/18/2013 4:00 PM
Telephone	Office: [redacted] / Cell: [redacted]
E-mail address	[redacted]@hilltimes.com
Deadline	9/18/2013 4:00 PM
Status	Consulting
Branch	NS
Subject	Lawful Access
Questions	I'm following the issue of lawful access and telecommunications surveillance this week and I am looking for some response to the following questions. My questions are: 1. Will the government reintroduce lawful access legislation when Parliament returns? 2. What checks are in place to protect citizens' privacy from unwarranted surveillance? 3. Some critics say that the government has approved expanded telecomms surveillance without legislation, through spectrum licensing for example. How does your office respond to this claim? I'm putting these questions to your office as it was the previous Public Safety Minister who previously introduced lawful access legislation. My deadline is tomorrow at 5, please let me know who the response are attributable to. Thanks for your help,

Josée Picard
Media Relations / Relations avec les médias
Ministère de la sécurité publique | Department of Public Safety
T : 613-949-4288 | F : 613-954-4779
josee.picard@ps-sp.gc.ca

Emmett, Jamie

From: Dyer, Lara
Sent: September-16-13 9:34 AM
To: Plunkett, Shawn
Subject: RE: Media Request: Lawful Interception Enforcement Standards

tks

From: Plunkett, Shawn
Sent: Monday, September 16, 2013 9:32 AM
To: Dyer, Lara
Subject: FW: Media Request: Lawful Interception Enforcement Standards

FYI. This was the comms request received late Friday. This request relates to today's article.

From: Chayer, Marie-Helene
Sent: September-13-13 5:29 PM
To: Picard, Josée; Plunkett, Shawn
Cc: Carta, John; Miller, Kevin
Subject: RE: Media Request: Lawful Interception Enforcement Standards

Josée,

J'en ai discuté avec mon DG - on est d'accord avec votre réponse.

Merci et bonne fin de semaine

Marie-Hélène

Marie-Hélène Chayer
Director – Investigative Technology and Telecommunications Policy /
Directrice – Politique sur les technologies d'enquête et les télécommunications
National Security Operations Division / Division des Opérations de sécurité nationale
Public Safety Canada / Sécurité Publique Canada
(613)949-3181

From: Picard, Josée
Sent: September-13-13 5:10 PM
To: Plunkett, Shawn; Chayer, Marie-Helene
Cc: Carta, John; Miller, Kevin
Subject: Media Request: Lawful Interception Enforcement Standards
Importance: High

s.19(1)

Shawn, Marie-Helene,

We received another follow-up request from [redacted] (Globe and Mail) today on a Lawful Interception Enforcement Standards request [redacted] made back in December 2012. [redacted] is looking to know if we have anything more to say at this time.

Unless anything has changed since June, do you have any concerns with the following response?:

- "Further to your follow-up request today, we have nothing further to add at this time."

Many thanks,
Josée

Josée Picard
Media Relations / Relations avec les médias
Ministère de la sécurité publique | Department of Public Safety
T : 613-949-4288 | F : 613-954-4779
josee.picard@ps-sp.gc.ca

Previous Calls (2):

s.19(1)

Title	[redacted]
Media Outlet	Globe and Mail
Call Date	6/10/2013 4:00 PM
Telephone	[redacted]
E-mail address	[redacted]@globeandmail.com
Deadline	
Status	Final
Branch	NS
Subject	Lawful Interception Enforcement Standards

Questions

The reporter is following up on a request [redacted] had sent us this winter, see summary below. [redacted] wants to see if there is anything more that can be said on this at this time.

****

PREVIOUS REQUEST

Title: [redacted]
Media Outlet: Globe and Mail
Call Date: 12/31/2012 3:00 PM
Telephone: [redacted]
E-mail address: [redacted]@globeandmail.com
Status: Response sent to the reporter
Branch: NS
Subject: Lawful Interception Enforcement Standards (re:Lawful Access)
Questions:
I am reviewing a document put together by Public Safety Canada's National Security Technology Division regarding 22 specific interception standards that telecom carriers were asked to provide police circa 2008.

I am seeking a discussion with someone in the division to discuss these specific 22 measures. Would that be possible?

Document info:
- "Solicitor General's Enforcement Standards for the Lawful Interception of Telecommunications -- Compliance Table."
- said to be "current as of Nov. 17 2008"
- 22 standards make explicit what the government is seeking from telecom networks and carriers
- Annotated with italics further explaining the standards
- Among measures made explicit are needs for intercepting various modalities (call forwarding / real-time audio / data-voice correlation accuracy measures / encryption algorithms, etc etc etc)
- Prepared by Public Safety's National Security Technology Division

Final Response:
We respectfully decline your request for an interview and would note that the document entitled Solicitor General Enforcement Standards for Lawful Interception of Telecommunications, is provided to radio and spectrum licence holders to assist them in complying with their lawful interception condition of licence. This document contains sensitive

content and is not publicly available.

s.19(1)

Reporter and Outlet	[redacted] Globe and Mail
Actions Taken	No existing entries.
Draft Response	Further to your follow-up request today, we have nothing further to add at this time.

Title	[redacted]
Media Outlet	Globe and Mail
Call Date	12/31/2012 3:00 PM
Telephone	[redacted]
E-mail address	[redacted]@globeandmail.com
Deadline	
Status	Final
Branch	NS
Subject	Lawful Interception Enforcement Standards (re:Lawful Access)
Questions	I am reviewing a document put together by Public Safety Canada's National Security Technology Division regarding 22 specific interception standards that telecom carriers were asked to provide police circa 2008. I am seeking a discussion with someone in the division to discuss these specific 22 measures. Would that be possible? Document info: - "Solicitor General's Enforcement Standards for the Lawful Interception of Telecommunications -- Compliance Table." - said to be "current as of Nov. 17 2008" - 22 standards make explicit what the government is seeking from telecom networks and carriers - Annotated with italics further explaining the standards - Among measures made explicit are needs for intercepting various modalities (call forwarding / real-time audio / data-voice correlation accuracy measures / encryption algorithms, etc etc etc) - Prepared by Public Safety's National Security Technology Division
Reporter and Outlet	[redacted] Globe and Mail
Actions Taken	No existing entries.
Draft Response	
Approvals	Shawn Plunkett Michael MacDonald Andrew Swift Stéphanie Durand MO
Final Response	We respectfully decline your request for an interview and would note that the document entitled Solicitor General Enforcement Standards for Lawful Interception of Telecommunications, is provided to radio and spectrum licence holders to assist them in complying with their lawful interception condition of licence. This document contains sensitive content and is not publicly available.

Emmett, Jamie

From:	Plunkett, Shawn
Sent:	September-13-13 5:34 PM
To:	Chayer, Marie-Helene
Subject:	Re: Media Request: Lawful Interception Enforcement Standards

The unannotated version was released, but [redacted] appears to have gotten a copy of the annotated version.
Shawn Plunkett
[redacted]
PS/SP Canada

From: Chayer, Marie-Helene
Sent: Friday, September 13, 2013 05:15 PM
To: Plunkett, Shawn
Subject: RE: Media Request: Lawful Interception Enforcement Standards

Has it been released under an ATI request yet? I can`t remember if the package went out.

Marie-Hélène Chayer
Director – Investigative Technology and Telecommunications Policy /
Directrice – Politique sur les technologies d'enquête et les télécommunications
National Security Operations Division / Division des Opérations de sécurité nationale
Public Safety Canada / Sécurité Publique Canada
(613)949-3181

From: Plunkett, Shawn
Sent: September-13-13 5:13 PM
To: Chayer, Marie-Helene
Subject: Re: Media Request: Lawful Interception Enforcement Standards

I'm fine with the proposed response. Not sure there is much more we can say.
Shawn Plunkett
[redacted]
PS/SP Canada

s.19(1)

From: Picard, Josée
Sent: Friday, September 13, 2013 05:09 PM
To: Plunkett, Shawn; Chayer, Marie-Helene
Cc: Carta, John; Miller, Kevin
Subject: Media Request: Lawful Interception Enforcement Standards

Shawn, Marie-Helene,

We received another follow-up request from [redacted] (Globe and Mail) today on a Lawful Interception Enforcement Standards request [redacted] made back in December 2012. [redacted] s looking to know if we have anything more to say at this time.

Unless anything has changed since June, do you have any concerns with the following response?:

- "Further to your follow-up request today, we have nothing further to add at this time."

Many thanks,
Josée

Josée Picard
Media Relations / Relations avec les médias
Ministère de la sécurité publique | Department of Public Safety
T : 613-949-4288 | F : 613-954-4779
josee.picard@ps-sp.gc.ca

s.19(1)

Previous Calls (2):

Title	[redacted]
Media Outlet	Globe and Mail
Call Date	6/10/2013 4:00 PM
Telephone	[redacted]
E-mail address	[redacted]@globeandmail.com
Deadline	
Status	Final
Branch	NS
Subject	Lawful Interception Enforcement Standards
Questions	The reporter is following up on a request [redacted] had sent us this winter, see summary below. [redacted] wants to see if there is anything more that can be said on this at this time.

****

PREVIOUS REQUEST

Title: [redacted]
Media Outlet: Globe and Mail
Call Date: 12/31/2012 3:00 PM
Telephone: [redacted]
E-mail address: [redacted]@globeandmail.com
Status: Response sent to the reporter
Branch: NS
Subject: Lawful Interception Enforcement Standards (re:Lawful Access)
Questions:
I am reviewing a document put together by Public Safety Canada's National Security Technology Division regarding 22 specific interception standards that telecom carriers were asked to provide police circa 2008.

I am seeking a discussion with someone in the division to discuss these specific 22 measures. Would that be possible?

Document info:
- "Solicitor General's Enforcement Standards for the Lawful Interception of Telecommunications -- Compliance Table."
- said to be "current as of Nov. 17 2008"
- 22 standards make explicit what the government is seeking from telecom networks and carriers
- Annotated with italics further explaining the standards
- Among measures made explicit are needs for intercepting various modalities (call forwarding / real-time audio / data-voice correlation accuracy measures / encryption algorithms, etc etc etc)
- Prepared by Public Safety's National Security Technology Division

Final Response:
We respectfully decline your request for an interview and would note that the document entitled Solicitor General Enforcement Standards for Lawful Interception of Telecommunications, is provided to radio and spectrum licence holders to assist them in complying with their lawful interception condition of licence. This document contains sensitive content and is not publicly available.

Reporter and Outlet [redacted] Globe and Mail

Actions Taken No existing entries.

Draft Response Further to your follow-up request today, we have nothing further to add at this time.

Title [redacted]

Media Outlet Globe and Mail

Call Date 12/31/2012 3:00 PM

Telephone [redacted]

E-mail address [redacted]@globeandmail.com

Deadline

Status Final

Branch NS

Subject Lawful Interception Enforcement Standards (re:Lawful Access)

Questions s.19(1)

I am reviewing a document put together by Public Safety Canada's National Security Technology Division regarding 22 specific interception standards that telecom carriers were asked to provide police circa 2008.

I am seeking a discussion with someone in the division to discuss these specific 22 measures. Would that be possible?

Document info:
- "Solicitor General's Enforcement Standards for the Lawful Interception of Telecommunications -- Compliance Table."
- said to be "current as of Nov. 17 2008"
- 22 standards make explicit what the government is seeking from telecom networks and carriers
- Annotated with italics further explaining the standards
- Among measures made explicit are needs for intercepting various modalities (call forwarding / real-time audio / data-voice correlation accuracy measures / encryption algorithms, etc etc etc)
- Prepared by Public Safety's National Security Technology Division

Reporter and Outlet [redacted] - Globe and Mail

Actions Taken No existing entries.

Draft Response

Approvals

Shawn Plunkett
Michael MacDonald
Andrew Swift
Stéphanie Durand
MO

Final Response We respectfully decline your request for an interview and would note that the document entitled Solicitor General Enforcement Standards for Lawful Interception of Telecommunications, is provided to radio and spectrum licence holders to assist them in complying with their lawful interception condition of licence. This document contains sensitive content and is not publicly available.

Classification: Unclassified
Date: 9 September 2013

PRIVACY PROTECTION AND ELECTRONIC SURVEILLANCE

ISSUE:

The protection of privacy and the conduct of electronic surveillance for national security purposes in Canada.

BACKGROUND:

Protection of Privacy

The protection of privacy in Canada is enshrined in legislation, including the *Canadian Charter of Rights and Freedoms* (the *Charter*, 1982), the *Privacy Act* (1983), and the *Personal Information Protection and Electronic Documents Act* (2001).

The *Charter* establishes that "everyone has the right to be secure against unreasonable search and seizure". Courts determine if a search or seizure is reasonable or not by examining whether:

- the information collected benefitted from a reasonable expectation of privacy;
- the search was consistent with the law;
- the law under which the information was collected is reasonable; and
- the search was executed in accordance with the law.

A warrant or reasonable lawful authority is required to conduct a search in cases where the information involves a reasonable expectation of privacy.

The *Privacy Act* imposes limits on the collection, use and disclosure of personal information by government departments and agencies. The Act prohibits the disclosure of personal information without the consent of the individual implicated, except in specific circumstances, including where an investigative body demonstrates its lawful authority to request the personal information, or has a judicial authorization to do so.

The *Personal Information Protection and Electronic Documents Act* provides similar safeguards to the *Privacy Act*, but with respect to how the private sector may collect, use or disclose personal information gathered for business purposes. The *Personal Information Protection and Electronic Documents Act* limits the collection, use, and disclosure of personal information without consent to specific circumstances, including where a government institution demonstrates its lawful authority to request or obtain the information or has a judicial authorization to do so.

Electronic Surveillance

The legal power to intercept communications, and to search and seize electronic data, is provided for in legislation such as the *Criminal Code* and the *Canadian Security Intelligence Service Act* (*CSIS Act*, 1985).

The *Criminal Code* contains safeguards pertaining to electronic surveillance. For instance, the interception of communications requires a judicial authorization (with certain exceptions, such as in situations of imminent harm, including bomb threats or kidnappings). Judges must be satisfied, prior to issuing an authorization, that:

- there are reasonable grounds to believe that the interception would be in the best interest of the administration of justice;
- the information gleaned would assist the investigation; and
- other investigative procedures have failed, are unlikely to succeed, or the urgency of the case makes it impractical to try them (except in terrorism and organized crime cases, to which this condition does not apply).

Authorizations are limited to 60 days, except in terrorism and organized crime cases, where the limit is one year. In each case, police may submit new applications seeking to renew the authorization for the same period. Individuals whose communications were intercepted must be notified within 90 days after the interception ends that their communications were intercepted (one year in the case of terrorism and organized crime cases). Authorities, however, may seek to delay this notification when warranted in the interests of justice (e.g. the case is still on-going and notifying the individuals would alert them to the police's investigation). Moreover, the Minister of Public Safety and Emergency Preparedness, as well as provincial Attorneys General, must annually publish reports on the lawful interception of communications, including statistics on the number of interception warrants issued.

Other investigative powers related to electronic surveillance include, for example, production orders, and the installation of tracking devices and number recorders. Production orders allow police to request that telecommunications service providers provide historical electronic data in their possession. Tracking devices permit police to track an individual's location, while number recorders allow police to access an individual's call detail information (e.g. the number dialled, time of day, duration, etc.). In all three cases, a judicial authorization is required (except in exigent circumstances for tracking devices), and judges must be satisfied that there are reasonable grounds to suspect that a crime has been or will be committed, and that information gleaned from the investigative tool can be obtained. There is no reporting on the use of these tools.

The *CSIS Act* permits CSIS officials to secure the Minister of Public Safety's leave to seek Federal Court authorizations to conduct electronic surveillance. CSIS must have reasonable grounds to believe that the electronic surveillance is necessary to investigate a threat to the security of Canada. CSIS must convince the Federal Court judge that other investigative procedures have failed or are unlikely to succeed, that the urgency of the case makes it impractical to try them, or that information of importance regarding the threat is unlikely to be obtained otherwise. Court authorizations may not be issued for longer than 60 days in the case of a subversion threat, and up to one year for other threats such as terrorism, espionage and sabotage. The authorizations may be renewed by the court. The Security Intelligence Review Committee, an independent review body that reports to Parliament on the operations of CSIS, produces an annual report showing the number of Federal Court warrants that were approved in the past three fiscal years.

Emmett, Jamie

From:	Plunkett, Shawn
Sent:	August-28-13 8:57 AM
To:	Chayer, Marie-Helene
Subject:	FW: Minister MacKay statement on Lawful Access

As mentioned yesterday. Mackay comment below.

From: Plunkett, Shawn
Sent: August-27-13 10:14 AM
To: Hawrylak, Maciek
Subject: Minister MacKay statement on Lawful Access

I didn't see this until this morning, (from Aug 17, meeting at the Canadian Bar Association) MacKay's attributed as saying the following:

MacKay said he also won't be intimidated or deterred from considering new lawful access provisions despite privacy concerns that ultimately led to the death of previous bills. [Calgary Herald]

It was within the context of cyberbullying, so likely refers to Justice provisions.

Shawn Plunkett
Senior Policy Advisor / Conseiller principal en politiques
Investigative Technologies and Telecommunications Policy (ITTP) /
Technologies d'enquêtes et politiques des télécommunications (TEPT)
National Security Operations Directorate / Direction des opérations de sécurité nationale
Public Safety Canada / Sécurité Publique Canada
Tel: (613) 990-7066
Email: shawn.plunkett@ps-sp.gc.ca

Dyer, Lara

From: Lisa.Foley@ic.gc.ca
Sent: August-20-13 3:31 PM
To: Hawrylak, Maciek; Dyer, Lara
Cc: John.Clare@ic.gc.ca; Angele.Dumont@ic.gc.ca; Bruce.Wallace@ic.gc.ca
Subject: RE: Lawful Access - PMR 2012-2013

Hi Maciek and Lara,

Our ADM, Lawrence Hanson, has approved the PMR.

Lisa

Lisa Foley
Policy Analyst | Analyste des politiques
Security and Privacy Policy Directorate | Direction de la politique sur la sécurité et la protection des renseignements personnels.

Digital Policy Branch | Direction générale de la politique numérique.
Spectrum, Information Technologies and Telecommunications Sector | Secteur du Spectre, des technologies de l'information et des télécommunications
Industry Canada | Industrie Canada
300 Slater Street | 300, rue Slater
Ottawa, Ontario, Canada K1A 0C8
Telephone: 613-952-3424 | Téléphone: 613-952-3424
Email: Lisa.Foley@ic.gc.ca | Courriel: Lisa.Foley@ic.gc.ca

From: Hawrylak, Maciek [mailto:Maciek.Hawrylak@ps-sp.gc.ca]
Sent: Friday, August 16, 2013 1:34 PM
To: Foley, Lisa: DPB-DGPN
Cc: Clare, John: DPB-DGPN; Dumont, Angele: DPB-DGPN; Dyer, Lara: PS
Subject: RE: Lawful Access - PMR 2012-2013

Lisa,
Thanks, that's great. Please send the email to Lara Dyer (copied) if you would like to send it before the 23rd. Otherwise, just send it to me, and I'll make note of it when I'm back. It's not due until the 28th.
Maciek

From: Lisa.Foley@ic.gc.ca [mailto:Lisa.Foley@ic.gc.ca]
Sent: August-16-13 1:21 PM
To: Hawrylak, Maciek
Cc: John.Clare@ic.gc.ca; Angele.Dumont@ic.gc.ca
Subject: RE: Lawful Access - PMR 2012-2013

s.19(1)

Hi Maciek,

The PMR is being sent to our ADM's office today. If he's signs off on it after [redacted] (next Wednesday), either John Clare or Angele Dumont, cc'd above, will pass the information along to Public Safety. You mentioned you were also [redacted] so who should be notified in your absence?

Lisa

From: Hawrylak, Maciek [mailto:Maciek.Hawrylak@ps-sp.gc.ca]
Colleagues,
I'm pleased to report that the PMR has been approved at PS at the DG level, and we will be distributing copies to you today. The next stage is for you to seek ADM approval within your respective organizations. Please provide us with an email signaling the approval of your ADM by end of day **Wednesday 28 August**.
At that point, we will seek Senior ADM approval at PS, and the PMR will then be forwarded to TBS in advance of the 15 September deadline.
Many thanks,
Maciek

Maciek Hawrylak
National Security Operations Directorate | Direction des Operations de Sécurité Nationale
Public Safety Canada | Sécurité Publique Canada
Tel | Tél : 613-991-6036
Fax | Téléc : 613-991-4669
Maciek.Hawrylak@ps-sp.gc.ca

Emmett, Jamie

From:	Plunkett, Shawn
Sent:	August-20-13 3:09 PM
To:	Chayer, Marie-Helene
Cc:	Dyer, Lara
Subject:	RE: Request for Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications

s.19(1)

Already sent.
I did get an out of office message from the requester, but can follow-up with [redacted]n [redacted]turn to determine why [redacted] is seeking the document.

From: Chayer, Marie-Helene
Sent: August-20-13 2:50 PM
To: Plunkett, Shawn
Cc: Dyer, Lara
Subject: Re: Request for Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications

Thanks. Did you send it already? If not, I'd like to take a look at the accompanying message tomorrow. I also would like to know why they are asking.

From: Plunkett, Shawn
Sent: Tuesday, August 20, 2013 02:40 PM
To: Chayer, Marie-Helene
Cc: Dyer, Lara
Subject: FW: Request for Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications

FYI. I spoke with Yves this afternoon and he was fine with releasing to Calgary Police.

In order to caveat the document, I thought it better to send myself than comms. They were okay with that approach.

From: Plunkett, Shawn
Sent: August-20-13 2:37 PM
To: [redacted]@calgarypolice.ca'
Cc: Communications_
Subject: Request for Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications

s.19(1)

[redacted]

I have been forwarded your request for the document entitled the Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications.
Please find enclosed the requested document.

Please note that while this document is not classified, it is not currently published (online or otherwise) as it contains sensitive information. Therefore, we request that you not publish this document and that any circulation be limited.

Should you have any questions regarding this document, please do not hesitate to contact me (details below).

Thank you.

Shawn Plunkett
Senior Policy Advisor / Conseiller principal en politiques
National and Cyber Security Branch / Secteur de la sécurité et de la cybersécurité nationale
Public Safety Canada / Sécurité Publique Canada
340 Ave Laurier W, Ottawa,
Ontario, Canada, K1A 0P9
Telephone | Téléphone: (613) 990-7066
Facsimile | Télécopieur: (613) 991-4669
Email | Courriel: shawn.plunkett@ps.gc.ca

Public Safety Canada Sécurité publique Canada

Emmett, Jamie

From:	Plunkett, Shawn
Sent:	August-20-13 2:49 PM
To:	Levert, Jean-Philippe
Subject:	FW: Public enquiry - Solicitor General's enforcement standards for lawful interception of telecommunications

Hi Jean-Philippe,
I forwarded the document to the requester as discussed (copied the Communications email address).

Not sure if you need for your records or not, but the email address for the requester is [redacted]@calgarypolice.ca. (not @calgarypolice.gc.ca)

Thanks for sending along. Appreciate it.

s.19(1)

From: Levert, Jean-Philippe
Sent: Tuesday, August 20, 2013 10:31 AM
To: Chayer, Marie-Helene
Cc: Communications_
Subject: FW: Public enquiry - Solicitor General's enforcement standards for lawful interception of telecommunications

Good morning,
Please see the enquiry below.
Would you be able to respond to her directly or provide us a response so that we may close this call on our end?
Thank you for your assistance in this matter.

Name	[redacted]
Enquiry Date	8/12/2013
Language	English
Phone #	[redacted]
Location	Alberta
E-mail	[redacted]@calgarypolice.gc.ca
Type of Enquiry	Unrelated to PS and portfolio
Method of Enquiry	Telephone
Organization	
PS Branch	
Program	
Portfolio Agency/Review Bodies	
Questions	He is looking for a copy of the "Solicitor General's enforcement standards for lawful interception of telecommunications". He can't find it online.

Jean-Philippe Levert

Adjoint aux communications | Communications Assistant

Gestion des enjeux, Affaires publiques | Issues Management Team, Public Affairs Division
Ministère de la sécurité publique | Department of Public Safety
T : 613-949-1703

Emmett, Jamie

From:	Plunkett, Shawn
Sent:	August-20-13 2:37 PM
To:	[redacted]@calgarypolice.ca
Cc:	Communications_
Subject:	Request for Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications
Attachments:	Solicitor General's Enforcement Standards for Lawful Interception of Tel....pdf

s.19(1)

[redacted]

I have been forwarded your request for the document entitled the Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications.
Please find enclosed the requested document.

Please note that while this document is not classified, it is not currently published (online or otherwise) as it contains sensitive information. Therefore, we request that you not publish this document and that any circulation be limited.

Should you have any questions regarding this document, please do not hesitate to contact me (details below).

Thank you.

Shawn Plunkett
Senior Policy Advisor / Conseiller principal en politiques
National and Cyber Security Branch / Secteur de la sécurité et de la cybersécurité nationale
Public Safety Canada / Sécurité Publique Canada
340 Ave Laurier W, Ottawa,
Ontario, Canada, K1A 0P9
Telephone | Téléphone: (613) 990-7066
Facsimile | Télécopieur: (613) 991-4669
Email | Courriel: shawn.plunkett@ps.gc.ca

Public Safety Canada Sécurité publique Canada

Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications - Compliance Table

Solicitor Generals Standards

Standard 1: Law enforcement agencies require access to the entire telecommunications transmitted, or caused to be transmitted, to and from the number or other identifier of the target service used by the interception subject. Law enforcement agencies also require access to the call-associated data that is generated to process the call.

Standard 2: Law enforcement agencies require access to all mobile interception subjects operating temporarily or permanently within a telecommunications system.

Standard 3: Law enforcement agencies require access in cases where the interception subject may be using features to divert calls to other telecommunications service or terminal equipment, including calls that traverse more than one network or are processed by more than one network operator/service provider before completing.

Standard 4: Law enforcement agencies require that the telecommunications to and from a target service be provided to the exclusion of any telecommunications that do not fall within the scope of the interception authorization.

Standard 5: Law enforcement agencies require access to available call associated data such as:

A) Signaling of access ready status

B) Called party number for outgoing connections even if there is no successful connection established

C) Calling party number for incoming connections even if there is no successful connection established

D) All digits dialed by the target, including post-connection dialed digits used to activate features such as conference calling and call transfer

E) Beginning, end, and duration of the connection

F) Actual destination and intermediate directory numbers if call has been diverted.

Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications - Compliance Table

Standard 6: Law enforcement agencies require information on the most accurate geographical location known to the network for mobile subscribers.

Standard 7: Law enforcement agencies require data on the specific service used by the interception subject and the technical parameters for that type of communication.

Standard 8: Law enforcement agencies require a real- time, full-time monitoring capability for the interception of telecommunications. Call associated data should also be provided in real-time. If call associated data cannot be made available in real time, law enforcement agencies require the data to be available as soon as possible upon call termination.

Standard 9: Law enforcement agencies require network operators/service providers to provide one or more interfaces from which the intercepted communications can be transmitted to the law enforcement monitoring facility. These interfaces have to be commonly agreed on by the interception authorities and the network operators/service providers. Other issues associated with these interfaces will be handled according to generally accepted practices.

Standard 10: Law enforcement agencies require network operators/service providers to provide call associated data and call content from the target service in a way that allows for the accurate correlation of call associated data with call content.

Standard 11: Law enforcement agencies require that the format for transmitting the intercepted communications to the monitoring facility be a generally available format.

Standard 12: If network operators/service providers initiate encoding, compression or encryption of telecommunications traffic, law enforcement agencies require the network operators/service providers to provide intercepted communications en clair.

Standard 13: Law enforcement agencies require network operators/service providers to be able to transmit the intercepted communications to the law enforcement monitoring facility via fixed or switched connections.

Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications - Compliance Table

Standard 14: Law enforcement agencies require that the transmission of the intercepted communications to the monitoring facility meet applicable Government of Canada security requirements.

Standard 15: Law enforcement agencies require interceptions to be implemented so that neither the interception target nor any other unauthorized person is aware of any changes made to fulfill the interception order. In particular, the operation of the target service must appear unchanged to the interception subject.

Standard 16: Law enforcement agencies require the interception to be designed and implemented to preclude unauthorized or improper use and to safeguard the information related to the interception.

Standard 17: Law enforcement agencies require network operators/service providers to protect information on which and how many interceptions are being or have been performed, and not disclose information on how interceptions are carried out.

Standard 18: Law enforcement agencies require network operators/service providers to ensure that intercepted communications are only transmitted to the monitoring agency specified in the interception authorization.

Standard 19: Based on a lawful inquiry and before implementation of the interception, law enforcement agencies require **(1)** the interception subject's identity service number or other distinctive identifier, **(2)** information on the services and features of the telecommunications system used by the interception subject and delivered by network operators/service providers, and **(3)** information on the technical parameters of the transmission to the law enforcement monitoring facility.

Standard 20: During the interception law enforcement agencies may require information and/or assistance from the network operators/service providers to ensure that the communications acquired at the interception interface are those communications associated with the target service.

Standard 21: Law enforcement agencies require network operators/service providers to make provisions for implementing a number of simultaneous intercepts. Multiple interceptions may be required for a single target service to allow monitoring by more than one law enforcement agency. In this case, network operators/service providers should take precautions to safeguard the identities of the monitoring agencies and ensure the confidentiality of the investigations.

Standard 22: Law enforcement agencies require network operators/service providers to implement interceptions as quickly as possible (in urgent cases within a few hours or minutes). The response requirements of law enforcement agencies will vary by the type of target service to be intercepted.

Standard 23: For the duration of the interception, law enforcement agencies require that the reliability of the services supporting the interception at least equals the reliability of the target services provided to the interception subject. Law enforcement agencies require the quality of service of the intercepted transmissions forwarded to the monitoring facility to comply with the performance standards of the network operators/service providers.

Dyer, Lara

From:	Chayer, Marie-Helene
Sent:	August-20-13 11:31 AM
To:	Plunkett, Shawn
Cc:	Dyer, Lara
Subject:	Re: Public enquiry - Solicitor General's enforcement standards for lawful interception of telecommunications

Sounds good. Thanks.

From: Plunkett, Shawn
Sent: Tuesday, August 20, 2013 11:27 AM
To: Chayer, Marie-Helene
Cc: Dyer, Lara
Subject: RE: Public enquiry - Solicitor General's enforcement standards for lawful interception of telecommunications

Hi,
The unannotated version of the SGES have now been publicly released on at least two occasions (with a third upcoming) based on ATIs. I believe we have not yet released as a result of a comms request.

I would recommend providing a copy to the Calgary Police following consultation with the RCMP.

I'll call the RCMP and see if they had been approached by the Calgary Police before with this request.
If they have no concerns, I can speak with comms and provide [redacted] with a copy.

s.19(1)

From: Chayer, Marie-Helene
Sent: August-20-13 11:16 AM
To: Plunkett, Shawn
Cc: Dyer, Lara
Subject: Fw: Public enquiry - Solicitor General's enforcement standards for lawful interception of telecommunications

Hi,
Were they released under an ATI request?
What is your advice on the way forward?
Mh

From: Levert, Jean-Philippe
Sent: Tuesday, August 20, 2013 10:31 AM
To: Chayer, Marie-Helene
Cc: Communications_
Subject: FW: Public enquiry - Solicitor General's enforcement standards for lawful interception of telecommunications

Good morning,
Please see the enquiry below.
Would you be able to respond to her directly or provide us a response so that we may close this call on our end?
Thank you for your assistance in this matter.

Name	[redacted]
Enquiry Date	8/12/2013
Language	English
Phone #	[redacted]
Location	Alberta
E-mail	[redacted]@calgarypolice.gc.ca
Type of Enquiry	Unrelated to PS and portfolio
Method of Enquiry	Telephone
Organization	
PS Branch	
Program	
Portfolio Agency/Review Bodies	
Questions	[redacted] is looking for a copy of the "Solicitor General's enforcement standards for lawful interception of telecommunications". [redacted] can't find it online.

s.19(1)

Jean-Philippe Levert

Adjoint aux communications | Communications Assistant
Gestion des enjeux, Affaires publiques | Issues Management Team, Public Affairs Division
Ministère de la sécurité publique | Department of Public Safety
T : 613-949-1703

Dyer, Lara

From: Dyer, Lara
Sent: August-20-13 10:13 AM
To: Rosales-List, Rodrigo
Subject: RE: Availability for lawful access meeting

Great – thanks so much. I'll send a calendar invite.

From: Rosales-List, Rodrigo
Sent: Tuesday, August 20, 2013 10:13 AM
To: Dyer, Lara
Subject: RE: Availability for lawful access meeting

Tomorrow looks good!
Thanks Lara.

From: Dyer, Lara
Sent: Tuesday, August 20, 2013 10:02 AM
To: Rosales-List, Rodrigo
Subject: RE: Availability for lawful access meeting

Hi, Rod – my director would like to meet to go over your comments... I know this is a busy time for you, so even if we could just talk about the first page (high-level) that would be really helpful. Would you be able to carve out 30 minutes tomorrow afternoon?

Thanks in advance,
Lara

s.21(1)(a)
s.21(1)(b)

From: Rosales-List, Rodrigo
Sent: Monday, August 19, 2013 3:49 PM
To: Hawrylak, Maciek; Dyer, Lara
Cc: Maynard, Stephen
Subject: RE: Availability for lawful access meeting

Maciek and Lara,

Thanks for the opportunity to comment. First off, we rarely get good first drafts to review like this one. It looks good to us, and the measures to be implemented are relevant, and seem very specific and measurable.

A few considerations:

[redacted]

[redacted]

The rest looks good. There are many ways of developing logic models and there is no perfect answer, you need to use what is the most meaningful for your group and the best communication tool for your audience. One word of advice, the bulk of the work is in the collection and then in the analysis of the data collected. That's where you will really reap the benefits, but it is also labor-intensive. Try to limit the of indicators, to a manageable number, so you can actually spend the required resources in measuring and analyzing them.

Feel free to contact me if you have any questions.

s.21(1)(a)

s.21(1)(b)

Rod

Rodrigo Rosales-List
Manager | Gestionnaire
Strategic Policy Branch | Secteur des politiques stratégiques
Public Safety Canada | Sécurité publique Canada
Tel. (613) 949-9920
rodrigo.rosales-list@ps-sp.gc.ca

From: Hawrylak, Maciek
Sent: Friday, August 16, 2013 3:25 PM
To: Rosales-List, Rodrigo
Cc: Dyer, Lara
Subject: RE: Availability for lawful access meeting

Rodrigo,

s.19(1)

[redacted] When we finished chatting, you mentioned you might be able to get me your thoughts on our logic model and indicators before my return on the 26th, since we are meeting with the agencies early next week. My director has asked if you could provide your comments by **COB Monday 19 August**. I realize this leaves you very little time, but whatever guidance you may be able to provide at that time would be most appreciated. I would be grateful if you could be sure to copy my colleagues, Lara Dyer (in cc) on your response.

Many thanks,
Maciek

From: Rosales-List, Rodrigo
Sent: August-14-13 11:42 AM
To: Hawrylak, Maciek
Subject: RE: Availability for lawful access meeting

Yes. We should be ok.
Can I get a draft copy of the logic model, I will look at it this afternoon.

Merci.

Rod

From: Hawrylak, Maciek
Sent: Wednesday, August 14, 2013 11:25 AM
To: Rosales-List, Rodrigo
Subject: RE: Availability for lawful access meeting

Rod,

Just following up on this. You had mentioned you were very busy with other matters, but that you should be available tomorrow. If you could please let me know if this is still the case, I can plan accordingly. Please advise.

Thanks,
Maciek

From: Hawrylak, Maciek
Sent: August-13-13 12:02 PM
To: Rosales-List, Rodrigo
Subject: RE: Availability for lawful access meeting

Rod,

You mentioned you would be available to discuss our draft logic model on Thursday. Is there a time that day that works best for you? We had a meeting with agencies today to go over the first draft, and while we're far from a final version, I thought it would be worthwhile to check in with you about whether we're on the right track.

Thanks,
Maciek

From: Rosales-List, Rodrigo
Sent: August-08-13 1:03 PM
To: Hawrylak, Maciek
Subject: RE: Availability for lawful access meeting

The groups are currently developing them.
That's why we need Performance Measurement Strategies for everybody.

The closest we have to measures and targets are the overall ones, for the Departmental PMF.
You can find them here: 875338

From: Hawrylak, Maciek
Sent: Thursday, August 08, 2013 12:10 PM
To: Rosales-List, Rodrigo
Subject: RE: Availability for lawful access meeting

Rod,

Are you also able share the indicators and targets for the logic models that you referenced?

Maciek

From: Rosales-List, Rodrigo
Sent: August-08-13 11:20 AM
To: Hawrylak, Maciek
Subject: RE: Availability for lawful access meeting

Hi Maciek,

As discussed, you will find attached the Logic Model Guide.
Also we have a folder with all the logic models the Department has so far, it is RDIMS: 523057

As you'll see there aren't many for NS programs, but I suggest you take a look at some of the Countering crime ones for ideas, for example the one for integrated proceeds of crime (812106), or the major international security cost framework (818624).

If you send me something through DRAGON, please send me a notification email on the unsecured network.
Cheers,

Rod

Dyer, Lara

From:	Dyer, Lara
Sent:	August-19-13 4:14 PM
To:	Rosales-List, Rodrigo; Hawrylak, Maciek
Cc:	Maynard, Stephen
Subject:	RE: Availability for lawful access meeting

Hi, Rod;

Thanks very much for your time and comments – we realize this is a busy time for you! The credit for the logic model is all Maciek's – he's done a great job, I agree. We'll go through the comments in detail and, as discussed, will follow up with any questions.

Thanks again,
Lara

Lara Dyer
Senior Policy Analyst | Analyste principale en politique
National and Cyber Security Branch | Secteur de la sécurité nationale et de la cybersécurité
Public Safety Canada | Sécurité publique Canada
613.991.3240

From: Rosales-List, Rodrigo
Sent: Monday, August 19, 2013 3:49 PM
To: Hawrylak, Maciek; Dyer, Lara
Cc: Maynard, Stephen
Subject: RE: Availability for lawful access meeting

s.21(1)(a)
s.21(1)(b)

Maciek and Lara,

Thanks for the opportunity to comment. First off, we rarely get good first drafts to review like this one. It looks good to us, and the measures to be implemented are relevant, and seem very specific and measurable.

A few considerations:

[redacted]

[redacted]

The rest looks good. There are many ways of developing logic models and there is no perfect answer, you need to use what is the most meaningful for your group and the best communication tool for your audience. One word of advice, the bulk of the work is in the collection and then in the analysis of the data collected. That's where you will really reap the benefits, but it is also labor-intensive. Try to limit the of indicators, to a manageable number, so you can actually spend the required resources in measuring and analyzing them.

Feel free to contact me if you have any questions.

s.21(1)(a)
s.21(1)(b)

Rod

Rodrigo Rosales-List
Manager | Gestionnaire
Strategic Policy Branch | Secteur des politiques stratégiques
Public Safety Canada | Sécurité publique Canada
Tel. (613) 949-9920
rodrigo.rosales-list@ps-sp.gc.ca

From: Hawrylak, Maciek
Sent: Friday, August 16, 2013 3:25 PM
To: Rosales-List, Rodrigo
Cc: Dyer, Lara
Subject: RE: Availability for lawful access meeting

Rodrigo,

s.19(1)

[redacted] When we finished chatting, you mentioned you might be able to get me your thoughts on our logic model and indicators before my return on the 26th, since we are meeting with the agencies early next week. My director has asked if you could provide your comments by **COB Monday 19 August**. I realize this leaves you very little time, but whatever guidance you may be able to provide at that time would be most appreciated. I would be grateful if you could be sure to copy my colleagues, Lara Dyer (in cc) on your response.

Many thanks,
Maciek

From: Rosales-List, Rodrigo
Sent: August-14-13 11:42 AM

To: Hawrylak, Maciek
Subject: RE: Availability for lawful access meeting

Yes. We should be ok.
Can I get a draft copy of the logic model, I will look at it this afternoon.

Merci.

Rod

From: Hawrylak, Maciek
Sent: Wednesday, August 14, 2013 11:25 AM
To: Rosales-List, Rodrigo
Subject: RE: Availability for lawful access meeting

Rod,

Just following up on this. You had mentioned you were very busy with other matters, but that you should be available tomorrow. If you could please let me know if this is still the case, I can plan accordingly. Please advise.

Thanks,
Maciek

From: Hawrylak, Maciek
Sent: August-13-13 12:02 PM
To: Rosales-List, Rodrigo
Subject: RE: Availability for lawful access meeting

Rod,

You mentioned you would be available to discuss our draft logic model on Thursday. Is there a time that day that works best for you? We had a meeting with agencies today to go over the first draft, and while we're far from a final version, I thought it would be worthwhile to check in with you about whether we're on the right track.

Thanks,
Maciek

From: Rosales-List, Rodrigo
Sent: August-08-13 1:03 PM
To: Hawrylak, Maciek
Subject: RE: Availability for lawful access meeting

The groups are currently developing them.
That's why we need Performance Measurement Strategies for everybody.

The closest we have to measures and targets are the overall ones, for the Departmental PMF.
You can find them here: 875338

From: Hawrylak, Maciek
Sent: Thursday, August 08, 2013 12:10 PM

To: Rosales-List, Rodrigo
Subject: RE: Availability for lawful access meeting

Rod,

Are you also able share the indicators and targets for the logic models that you referenced?

Maciek

From: Rosales-List, Rodrigo
Sent: August-08-13 11:20 AM
To: Hawrylak, Maciek
Subject: RE: Availability for lawful access meeting

Hi Maciek,

As discussed, you will find attached the Logic Model Guide.
Also we have a folder with all the logic models the Department has so far, it is RDIMS: 523057

As you'll see there aren't many for NS programs, but I suggest you take a look at some of the Countering crime ones for ideas, for example the one for integrated proceeds of crime (812106), or the major international security cost framework (818624).

If you send me something through DRAGON, please send me a notification email on the unsecured network.
Cheers,

Rod

Hawrylak, Maciek

From:	Rosales-List, Rodrigo	
Sent:	August-19-13 3:49 PM	
To:	Hawrylak, Maciek; Dyer, Lara	
Cc:	Maynard, Stephen	s.21(1)(a)
Subject:	RE: Availability for lawful access meeting	s.21(1)(b)

Maciek and Lara,

Thanks for the opportunity to comment. First off, we rarely get good first drafts to review like this one. It looks good to us, and the measures to be implemented are relevant, and seem very specific and measurable.

A few considerations:

[redacted]

The rest looks good. There are many ways of developing logic models and there is no perfect answer, you need to use what is the most meaningful for your group and the best communication tool for your audience. One word of advice, the bulk of the work is in the collection and then in the analysis of the data collected. That's where you will really reap the benefits, but it is also labor-intensive. Try to limit the of indicators, to a manageable number, so you can actually spend the required resources in measuring and analyzing them.

Feel free to contact me if you have any questions.

Rod

Rodrigo Rosales-List
Manager | Gestionnaire
Strategic Policy Branch | Secteur des politiques stratégiques
Public Safety Canada | Sécurité publique Canada
Tel. (613) 949-9920
rodrigo.rosales-list@ps-sp.gc.ca

From: Hawrylak, Maciek
Sent: Friday, August 16, 2013 3:25 PM
To: Rosales-List, Rodrigo
Cc: Dyer, Lara
Subject: RE: Availability for lawful access meeting

Rodrigo,

s.19(1)

[redacted] When we finished chatting, you mentioned you might be able to get me your thoughts on our logic model and indicators before my return on the 26th, since we are meeting with the agencies early next week. My director has asked if you could provide your comments by **COB Monday 19 August**. I realize this leaves you very little time, but whatever guidance you may be able to provide at that time would be most appreciated. I would be grateful if you could be sure to copy my colleagues, Lara Dyer (in cc) on your response.

Many thanks,
Maciek

From: Rosales-List, Rodrigo
Sent: August-14-13 11:42 AM
To: Hawrylak, Maciek
Subject: RE: Availability for lawful access meeting

Yes. We should be ok.
Can I get a draft copy of the logic model, I will look at it this afternoon.

Merci.

Rod

From: Hawrylak, Maciek
Sent: Wednesday, August 14, 2013 11:25 AM
To: Rosales-List, Rodrigo
Subject: RE: Availability for lawful access meeting

Rod,

Just following up on this. You had mentioned you were very busy with other matters, but that you should be available tomorrow. If you could please let me know if this is still the case, I can plan accordingly. Please advise.

Thanks,
Maciek

From: Hawrylak, Maciek
Sent: August-13-13 12:02 PM

To: Rosales-List, Rodrigo
Subject: RE: Availability for lawful access meeting

Rod,

You mentioned you would be available to discuss our draft logic model on Thursday. Is there a time that day that works best for you? We had a meeting with agencies today to go over the first draft, and while we're far from a final version, I thought it would be worthwhile to check in with you about whether we're on the right track.

Thanks,
Maciek

From: Rosales-List, Rodrigo
Sent: August-08-13 1:03 PM
To: Hawrylak, Maciek
Subject: RE: Availability for lawful access meeting

The groups are currently developing them.
That's why we need Performance Measurement Strategies for everybody.

The closest we have to measures and targets are the overall ones, for the Departmental PMF.
You can find them here: 875338

From: Hawrylak, Maciek
Sent: Thursday, August 08, 2013 12:10 PM
To: Rosales-List, Rodrigo
Subject: RE: Availability for lawful access meeting

Rod,

Are you also able share the indicators and targets for the logic models that you referenced?

Maciek

From: Rosales-List, Rodrigo
Sent: August-08-13 11:20 AM
To: Hawrylak, Maciek
Subject: RE: Availability for lawful access meeting

Hi Maciek,

As discussed, you will find attached the Logic Model Guide.
Also we have a folder with all the logic models the Department has so far, it is RDIMS: 523057

As you'll see there aren't many for NS programs, but I suggest you take a look at some of the Countering crime ones for ideas, for example the one for integrated proceeds of crime (812106), or the major international security cost framework (818624).

If you send me something through DRAGON, please send me a notification email on the unsecured network.
Cheers,

Rod

s.19(1)

s.23

Emmett, Jamie

From:	Plunkett, Shawn
Sent:	August-08-13 7:35 PM
To:	Ali, Kristen
Subject:	Re: Emailing [redacted]

Sure, no worries.
Shawn Plunkett
[redacted]
PS/SP Canada

From: Ali, Kristen
Sent: Thursday, August 08, 2013 06:34 PM
To: Plunkett, Shawn
Subject: RE: Emailing - [redacted]

Shawn,

Very sorry for the delay in getting back to you, I have had an urgent matter that came up on another file which kept me occupied all day unfortunately. I'll will try and give you a call tomorrow afternoon if that works.

Thanks,

Kristen Ali
Public Safety Legal Services | Sécurité publique services juridiques
Tel:/Tél: (613) 949-1514
Email/Courriel: Kristen.Ali@ps-sp.gc.ca
CONFIDENTIALITY NOTICE: This electronic mail message may contain solicitor-client privilege information.
AVIS DE CONFIDENTIALITÉ: Ce courrier électronique peut contenir de l'information protégée par le secret professionnel.

From: Plunkett, Shawn
Sent: Wednesday, August 07, 2013 4:54 PM
To: Ali, Kristen
Subject: RE: Emailing - [redacted]

Hi Kristen,
Sure. I am available most of tomorrow. I'm located at 340 so I can either head over to 269 to meet or you can give me a call tomorrow afternoon.

Thanks.

From: Ali, Kristen
Sent: August-07-13 4:44 PM
To: Plunkett, Shawn
Subject: RE: Emailing - [redacted]

Hello Shawn,

Shalin has provided me with the materials you had passed on, perhaps we can speak tomorrow afternoon once I have had the opportunity to review?

Thanks,
Kristen

s.23

Kristen Ali
Public Safety Legal Services | Sécurité publique services juridiques
Tel:/Tél: (613) 949-1514
Email/Courriel: Kristen.Ali@ps-sp.gc.ca
CONFIDENTIALITY NOTICE: This electronic mail message may contain solicitor-client privilege information.
AVIS DE CONFIDENTIALITÉ: Ce courrier électronique peut contenir de l'information protégée par le secret professionnel.

From: Sugunasiri, Shalin
Sent: Wednesday, August 07, 2013 2:19 PM
To: Plunkett, Shawn
Cc: Dyer, Lara; Ali, Kristen
Subject: RE: Emailing - [redacted]

Fyi - I have asked my colleague, Kristen, to follow up on your inquiry; she will be in touch shortly.

Cheers,
SMS

Solicitor-Client Privilege / Secret professionnel de l'avocat

From: Plunkett, Shawn
Sent: Tuesday, August 06, 2013 4:28 PM
To: Sugunasiri, Shalin
Cc: Dyer, Lara
Subject: Emailing - [redacted]

Hi Shalin,
Further to my message on the other system, [redacted]

Apologies, but I only have a marked-up copy (enclosed). I believe Claude had a copy, if you can track it down.

Let me know if you have any questions.

Thanks.

Shawn Plunkett
Senior Policy Advisor / Conseiller principal en politiques
Investigative Technologies and Telecommunications Policy (ITTP) /
Technologies d'enquêtes et politiques des télécommunications (TEPT)
National Security Operations Directorate / Direction des opérations de sécurité nationale
Public Safety Canada / Sécurité Publique Canada
Tel: (613) 990-7066
Email: shawn.plunkett@ps.gc.ca

Emmett, Jamie

From:	Plunkett, Shawn
Sent:	August-07-13 9:30 AM
To:	Dyer, Lara; Dincoy, Rana; Hawrylak, Maciek; Thompson, Julie; Emmett, Jamie
Subject:	FYI- Lawful Access Bill Would Have Allowed NSA-Style Spying In Canada
Importance:	Low

References a post from Geist from end of July.

From Huffington Post:
Lawful Access Bill Would Have Allowed NSA-Style Spying In Canada

The article has an interesting quote from our former Minister that I'm not sure if you have seen before.

Shawn Plunkett
Senior Policy Advisor / Conseiller principal en politiques
Investigative Technologies and Telecommunications Policy (ITTP) /
Technologies d'enquêtes et politiques des télécommunications (TEPT)
National Security Operations Directorate / Direction des opérations de sécurité nationale
Public Safety Canada / Sécurité Publique Canada
Tel: (613) 990-7066
Email: shawn.plunkett@ps.gc.ca

October 2, 2013

HUFF POST BUSINESS CANADA

Lawful Access Bill Would Have Allowed NSA-Style Spying In Canada: Geist

The Huffington Post Canada | Posted: 08/06/2013 5:09 pm EDT

A controversial bill that would have given the federal government greater power to track Canadians online included a provision that would have allowed for an NSA-style surveillance system, says a prominent digital law professor.

University of Ottawa professor Michael Geist says a provision in Bill C-30 would have given *carte blanche* to government agencies to install whatever monitoring equipment they want on telecom service providers' networks.

The Harper government withdrew Bill C-30 (known as the "Protecting Children from Internet Predators Act") earlier this year, after public concerns the bill would allow the government to surveil Canadians without a warrant online, but many political observers say the government is already sowing the seeds for a similar new bill to come.

In a recent blog post, Geist noted that section 14(4) of Bill C-30 would have given the government the power to "provide [a] telecommunications service provider with any equipment ... that the Minister considers the service provider needs to comply" with government requests under the new law.

"That provision would have given the government the power to decide what specific surveillance equipment must be installed on private ISP and telecom networks by allowing it to simply take over the ISP or telecom network and install its own equipment," Geist wrote.

He said the bill would have given the federal government "similar legal powers" to those enjoyed by the U.S. National Security Agency (NSA), whose own programs for warrantless tracking of social media activity and collection of millions of email records daily were recently exposed in a series of articles in the Guardian.

According to an article in Buzzfeed published last month, the NSA has the capability to install tracking equipment inside the offices of telecom providers, and force the providers to stay silent about it.

Geist had previously suggested that the Canadian government already has the capability to carry out NSA-style surveillance on Canadians.

The Harper government's "lawful access" legislation died a quiet death this spring, after many people reacted negatively to then-Public Security Minister Vic Toews' assertion that an opposition MP can "either stand with us or with the child pornographers" on the bill.

But as Geist and others point out, the bill, or something similar, may not be gone for good. Efforts to expand law enforcement's access to Canadians' online habits have been under proposal in one form or another since the 1990s, and the latest efforts appear to be shifting the focus away from catching child pornographers to stopping cyber-bullying.

A report on cyber-bullying issued by the federal Department of Justice last month "strongly recommends" a number of new legal provisions that would echo the old Bill C-30, or other similar legislation in other countries. Among the recommendations was the creation of a "preservation order" that would force Internet providers to keep a log for some mandated amount of time of all subscribers' internet use.

Another recommendation would see the government get enhanced powers to demand electronic communications from telecoms, as well as new powers to track communications online.

"Many of these powers were addressed in the lawful access bill and may be making a comeback in legislation this fall," Geist wrote on his blog.

s.23

Emmett, Jamie

From:	Plunkett, Shawn
Sent:	August-06-13 4:28 PM
To:	Sugunasiri, Shalin
Cc:	Dyer, Lara
Subject:	Emailing [redacted]
Attachments:	[redacted]

Hi Shalin,

Further to my message on the other system, [redacted]

Apologies, but I only have a marked-up copy (enclosed). I believe Claude had a copy, if you can track it down.

Let me know if you have any questions.

Thanks.

Shawn Plunkett
Senior Policy Advisor / Conseiller principal en politiques
Investigative Technologies and Telecommunications Policy (ITTP) /
Technologies d'enquêtes et politiques des télécommunications (TEPT)
National Security Operations Directorate / Direction des opérations de sécurité nationale
Public Safety Canada / Sécurité Publique Canada
Tel: (613) 990-7066
Email: shawn.plunkett@ps.gc.ca

Annie

Department of Justice
Canada

Constitutional and
Administrative Law
Section

Ministère de la Justice
Canada

Section du droit administratif
et constitutionnel

IND8912-115-4

Security classification – Cote de sécurité
Protected 10957-2

File number – Numéro de dossier
328145

Date
February 23, 1998

Telephone / FAX – Téléphone / Télécopieur
954-0281 / 941-1937

MEMORANDUM / NOTE DE SERVICE

s.23

TO / DEST: Heather Black, Counsel, Industry Canada Legal Services
VIA Martin Freeman, Director and General Counsel, C.A.L.S.

FROM / ORIG: Ken Katz, Counsel, Constitutional and Administrative Law Section

SUBJECT / OBJET: [redacted]

Do not write in this space / Ne pas écrire dans cet espace

Pages 80 to / à 86

are withheld pursuant to section

sont retenues en vertu de l'article

23

of the Access to Information

de la Loi sur l'accès à l'information

s.23

[redacted]

Please get in touch with me if there is anything further regarding this matter to discuss.

Kenneth Katz

Emmett, Jamie

From:	Plunkett, Shawn
Sent:	August-06-13 9:15 AM
To:	Dyer, Lara
Subject:	FW: Interception deck

Just making the last changes to the deck now. Once I'm done I'll let you know and you can touch base with Bob.
Tks.

From: Gordon, Robert
Sent: August-04-13 9:29 AM
To: MacDonald, Michael
Cc: Dyer, Lara; Chayer, Marie-Helene; Plunkett, Shawn
Subject: Re: Interception deck

s.19(1)

Mike
Sorry I missed your email [redacted] I will be in the office on Tuesday and can look at the deck then.
[redacted]
Bob

From: MacDonald, Michael
Sent: Friday, August 02, 2013 02:17 PM
To: Gordon, Robert
Cc: Dyer, Lara; Chayer, Marie-Helene; Plunkett, Shawn
Subject: Interception deck

Hi Bob,

[redacted] but wanted to let you know that we have created the deck to brief ADM IC on our interception challenges. Remember when you offered to take a look – we hope to call in the cards on that offer!!!!

Lara will drop by whenever you're around next week.

Thx again! Mike

30/07/2013

ISSUE

Comparing legislation, costs, and statistics related to interception in Australia, France, New Zealand, the United Kingdom (UK), and the United States (US).

AUSTRALIA

The power to intercept communications is found in the *Telecommunications (Interception and Access) Act* 1979 (TIA Act), which has been amended several times.[1]

Lawful Interception of Telecommunications

Under the TIA Act, there are two types of interception warrants: telecommunications service warrants (TSWs) and named person warrants (NPWs). TSWs allow the interception of one service at a time (e.g. one cellphone number) that is used or likely to be used by a named individual. NPWs allow the interception of any telecommunications services (e.g. a telephone number and an e-mail address) used or likely to be used by a named person. Both warrants may be issued for either national security (NS) or law enforcement (LE) purposes. In the Australian context, 'law enforcement' refers only to criminal law enforcement agencies (LEAs). A second term, 'enforcement agencies', refers to a broader category that also includes civil penalty enforcement agencies and public revenue agencies.

TSWs/NPWs are issued by a judicial authority to investigate serious offenses such as murder, acts of terrorism, and organized crime. They are valid for no more than 90 days and can be renewed in the same manner as original warrants. Applications must be made in writing except in urgent circumstances, such as sieges, where they can be made by telephone. As soon as practicable, the responsible agency must apply for a warrant. LE can also apply for a B-party interception warrant, which allows the interception of a service that is likely to be used by a non-suspect to communicate with the suspect. B-party warrants are used to identify the telecommunications services used by the suspect, or the suspect's identity or location. Such warrants are valid for no more than 45 days.

During the 2011/12 reporting period, 3,755 TSWs, 513 renewals of TSWs and 111 TSWs made by telephone (in urgent circumstances) were issued for LE, and one warrantless emergency interception was conducted. For the same period, 149 B-party interception warrants, 14 renewals of B-party interception warrants and 32 B-party interception warrants made by telephone were issued. The total expenditure (capital expenses, salaries, administrative support, and operational fees for interception) for all LEAs in connection with the execution of TSWs was AUD $50,554,007 (three-year average, AUD $49 million). For the same period, 701 NPWs, 160 renewals of NPWs and four NPWs

[1] Including the *National Crime Authority Act* 1984, the *Telecommunications Act* 1997, the *Telecommunication (Interception) Legislation Amendment Act* 2000, the *Telecommunications Interception Legislation Amendment Act* 2002, the *Stored Communications Amendment to the Interception Act* 2004 and the *Telecommunications (Interception) Amendment Act* 2006.

made by telephone (in urgent circumstances) were issued.[i] No figures on costs for NPWs were available.

With regard to NS, under the TIA Act, the Australian Security Intelligence Organisation (ASIO) can ask the Attorney General to issue an interception warrant in order to investigate activities prejudicial to NS or to collect foreign intelligence. Interception warrants issued to ASIO are valid for no more than six months. In emergency circumstances (defined in the TIA Act), ASIO's Director General may issue a NS warrant with a maximum duration of 48 hours. The Attorney General can also issue a B-party interception warrant, which is valid for no more than three months. Since ASIO's annual reports regarding lawful access activities are classified, no figures are available on matters such as the number of interceptions done by ASIO.

Access to Stored Communications

The TIA Act also permits an 'enforcement agency' to issue a stored communications warrant (SCW) to a service provider. SCWs can be issued by the same issuing authorities as interception warrants and by any other Commonwealth, State or Territory judge or magistrate. These warrants can be issued for serious offenses and serious contraventions (i.e. an offense punishable by a maximum period of imprisonment of at least three years, or an offense with an equivalent monetary penalty). An application for an SCW must be made in writing, except in urgent circumstances where it can be made by telephone. For the 2011/12 period, 483 SCWs were granted to enforcement agencies (two were refused).[ii] With regard to ASIO, warrants authorizing the agency to lawfully intercept telecommunications also allow accessing stored communications.

Access to Telecommunications Data under the TIA Act

Telecommunications data is not defined in Australia but is generally information about a communication (similar to Canada). It does not include content data. Under the TIA Act, there are two types of authorizations for telecommunications data: existing data and prospective data.

The disclosure of existing data (in existence prior to an authorization) may be authorized by an authorized officer of an 'enforcement agency' when it is considered reasonably necessary for the enforcement of a criminal law, a law imposing a pecuniary penalty or for the protection of the public revenue. For the 2011/12 period, 293,501 authorizations were issued for the enforcement of the criminal law and 10,936 authorizations were made for the enforcement of a law imposing a financial penalty or the protection of the public revenue.[iii] The disclosure of existing data can also be authorized by ASIO when the authorized official is satisfied that the disclosure would be connected to the functions of the agency.

The disclosure of prospective data (generated after the authorization) may only be authorized by <u>law</u> enforcement agencies when it is considered reasonably necessary for the investigation of an offence with a maximum prison term of at least three years and by

ASIO when the authorized official is satisfied that the disclosure would be connected to the functions of the agency. For the 2011-12 reporting period, 5,811 authorizations were made by LEAs.[iv]

C/CSPs' Lawful Access Obligations

Under the *Telecommunications Act* 1997, carriers and carriage service providers (C/CSPs) have to give authorities assistance in relation to the enforcement of criminal law and laws imposing a pecuniary penalty, protecting public revenue and safeguarding NS. A carrier is an entity who owns a telecom network unit to supply carriage services to the public and a carriage service provider is an entity who uses a telecom network unit to supply carriage services to the public (resellers). Social networking providers (e.g. Facebook) and cloud computing providers are not captured by the legislation).[v]

The TIA Act places an obligation on C/CSPs to have the capability to intercept and deliver telecommunications. It requires carriers and nominated carriage service providers (NCSPs, so designated by the Minister for Broadband, Communications and the Digital Economy) to submit an annual interception capability plan (IC Plan) explaining their strategy for complying with their responsibility to intercept and deliver telecommunications to interception agencies. Basic requirements for the interception capability are drawn from the European Telecommunications Standards Institute (ETSI).[vi]

The capital and ongoing costs of developing, installing and maintaining interception capability are borne by C/CSPs. Delivery costs (capital and operational) are borne by law enforcement. A C/CSP can charge operational fees for assistance on the basis that the C/CSP neither profits from, nor bears the costs of, giving that help.

An IC Plan acts as a guide to the interception capability of the C/NCSP. It provides information to the Australian Government and the intercepting agencies concerning the interception capability of the C/NCSP for each service or category of service that C/NCSP supplies, or intends to supply to the public. The IC plan informs agencies how each service will be intercepted. IC Plans are also used by the Australian Communications and Media Authority (ACMA) to determine if the C/NCSP's plan complies with its legislative obligations to provide interception capability. As such, these plans provide the ACMA, the Communications Access Co-ordinator (who liaises between law enforcement agencies and the telecommunications industry) and agencies with a tool for compliance monitoring.[vii]

Non-compliance with intercept capability obligations or the requirement to submit an IC Plan is considered a breach of a carrier licence condition[2] or a service provider rule and may lead to action in the Federal Court, where the Court may order the C/CSP in breach to pay to the Commonwealth a fine of up to AUD $10 million per breach. The

[2] Unlike in Canada, each carrier receives a licence to operate. In Canada, only wireless TSPs must have a licence.

Communications Access Co-ordinator may exempt a C/CSP from all or any obligations to provide interception capability.[viii]

The ACMA rarely uses its powers to enforce C/CSPs' compliance with the TIA Act because the only effective power available to it under the Act is court action, which is usually inappropriate or excessive under the circumstances and unhelpful from an interception agency perspective because it may publicly disclose that a particular C/CSP is not complying with its obligations. With regard to security standards, the TIA Act does not specifically address supply chain risks, hardware and software vulnerabilities or security risks to the confidentiality, integrity and availability of telecommunications infrastructure. Section 581 of the *Telecommunications Act* 1997 provides the Attorney-General (in consultation with the Prime Minister and the Minister for Broadband, Communications and the Digital Economy) the power to give a written direction to C/CSPs to cease supply of a carriage service if the use of that service is or would be prejudicial to NS. However, this section is non-specific, is not triggered by a specific set of circumstances and does not allow a practical graduated response to security risks. Forcing a C/CSP to cease supplying a carriage service is usually excessive.[ix]

In order to benefit from a more flexible compliance scheme, the Australian Government is considering potential amendments that would reinforce the ACMA's role by expanding the range of regulatory options available and modifying the standards with which the telecommunications industry must comply. The regulatory framework would implement detailed requirements for C/CSPs' interception obligations (e.g. by adding a requirement to assist agencies to decrypt information) and a penalty regime to encourage compliance.[x]

In addition, C/CSPs are obliged to contribute to a common Integrated Public Number Database (IPND) containing all public phone numbers. This is used for directory assistance, emergency services and assistance to enforcement agencies or for safeguarding NS. Sellers of pre-paid cards must identify the purchaser and post the details in the IPND. IPND only contains the service provider's name, the public number and the customer's name, address and directory listing information. With this system, there is no process for verifying the purchaser's proof of identity. Improvements to the current verification systems are expected to be implemented in 2013-2014. A key feature of the new system is the Attorney-General's Department Document Verification Service (DVS). Mobile service providers will be able to use the DVS to verify documents such as driver's licence, medicare card, visas and passports.

National Interception Technical Assistance Centre (NITAC)

In 2010, ASIO started a pilot study to establish a National Interception Technical Assistance Centre (NITAC). The NITAC provides a resource from which agencies can receive technical assistance to help keep pace with the rate and scale of technical change.[xi]

Safeguard Measures

Australia's lawful access system has many safeguard measures. The Commissioner of the Australian Federal Police must keep registers of warrants and submit them to the

Attorney-General for inspection every three months. Under the TIA Act, the Commonwealth Ombudsman is required to biannually inspect the records of the

Australian Federal Police and the Australian Crime Commission. Moreover, the Australian Parliament has two statutory committees and two standing committees whose functions include the monitoring of matters relating to the interception of telecommunications. The TIA Act also requires the Attorney General to table before each House of Parliament an annual report giving details about lawful access activities conducted by LE under the TIA Act. The ASIO also produces a classified annual report regarding its lawful access activities.

FRANCE

The power to intercept communications is found in the *Telecommunications Correspondence Secrecy Act of 1991* (the *1991 Act*) and the *Code of Criminal Proceedings.*

Security Interceptions and Judicial Interceptions

In France there are two types of interceptions: judicial interceptions (law enforcement) and security interceptions (intelligence agencies and law enforcement). For judicial interceptions, judicial approval can be sought from a 'juge d'instruction' (an investigative judge responsible for conducting the investigative hearing that precedes a criminal trial) for offences resulting in two years or more of imprisonment. Custodial judges may, at the request of a state prosecutor, approve interceptions related to urgent investigations, or for preliminary investigations related to the search for fugitives or crimes committed by organized crime such as murder and human trafficking. The duration is one month (renewable once).[xii] In 2010, there were around 32,000 judicial requisitions for content data.[xiii]

Concerning security interceptions, the *1991 Act* authorizes interception to safeguard NS and essential scientific and economic assets, or to prevent terrorism, criminality or organised delinquency. This authorization must be approved by the Prime Minister or designates. In 2010, 5,979 security interceptions were authorized.[xiv] Table 1 of the Annex lists France's main lawful access tools.[xv]

Data Retention Obligation

As a member state of the European Union (EU), France is subject to the 2006 Data Retention Directive.[3] Thus, French TSPs must retain telecommunications data (non-content data) for one year. Table 2 of the Annex summarizes the obligations for Internet Service Providers in France.

[3] TSPs from a member state of the EU must retain the following telecommunications data: information allowing the identification of a user; data related to telecommunications equipment used; technical characteristics as well as the date, time, and the duration of each telecommunication; data related to complementary services requested or used and their providers; and data allowing the identification of the recipient of the telecommunication. Data retention does not apply to the content of telecommunications

Access to Telecommunications Data

Telecommunications data (i.e. non-content data) can be accessed through a judicial requisition or through an administrative request prescribed by the law. With regard to judicial requisitions, criminal and preliminary investigations are regulated by the *Code of Criminal Proceedings*. Most judicial requisitions (which are made by an investigative judge or by a judicial police officer authorized by the judge) are only for telecommunications data (access to content data must meet the aforementioned criteria for judicial interceptions). For example, in 2003, 90% of the judicial requisitions were for the identification of subscribers or phone numbers. In 2010, there were around 11,000 judicial requests for tracking data and approximately 557,000 requests for detailed invoices.[xvi] Detailed invoices contain information regarding received and sent calls of a subscriber over a period of one month such as the phone number of each participant, and the time, date and duration of each call.

With regard to administrative requests, the *Anti-Terrorism Act of 2006* allows qualified officers individually designated from either police services or the National Gendarmerie involved in preventing terrorism to access technical data without a judicial authorization for the sole purpose of preventing terrorism. Requests from these officers include a justification and are submitted for approval to a qualified person designated by the Commission nationale de contrôle des interceptions de sécurité (CNCIS). In 2010, 38,566 requests were approved. Of this total, 72.8% were for the identification of subscribers and 27.57% were for traffic data.[xvii]

Intercept Capability Requirements for TSPs

The interception capability obligations of TSPs are part of broader requirements regarding public order, national defense and public safety contained in section D98-7 of the *Posts and Telecommunications Code*. The section compels operators (i.e. TSPs) to implement intercept solutions into their systems and assist authorities in conducting electronic surveillance. In the French context, an operator is someone that operates a public telecommunications network or provides a telecommunications service to the public. Each TSP must designate qualified employees (i.e. employees that have not been sentenced for certain criminal offenses, and who have been an employee of the TSP for at least 2 years) to carry out operations that are necessary for the implementation of the interception of telecommunications. Only these designated employees can use and control the systems used for interception, access data obtained, and share them to the authorized requesters.

The government covers all the costs for studying, engineering, conceptualizing, and deploying intercept capable networks. It also covers the costs for performing interceptions, maintaining intercept capable networks, and the rental of equipment allowing these networks to operate. Compensation is established through TSP-government agreements. In addition, the government also pays operational fees to TSPs for their assistance on each interception. Most of the fees service providers can charge for the provision of data are included and detailed in the legislation. All the choices (e.g.

the choice of an intercept solution) made by a TSP that would be eligible for compensation from the government are subject to validation by the minister in charge of telecommunications.

The Department of Justice negotiates the fees with TSPs and pays them. In 2005, the Délégations aux interceptions judiciaires (DIJ) was created to control costs related to judicial requisitions. The DIJ does not assess whether or not an interception should be authorized. According to a 2008 study, for each interception made on a fixed line, the government had to pay €467 to TSPs for designing and deploying intercept capable networks.[xviii] According to 2009 and 2011 reports published on the French Senate website, spending on operational fees declined from €69 million in 2005 to €35 million in 2010 (these amounts do not include fees for the rental of delivery lines and third party networks).[xix] However, the trend over the last three years has been gradually upward.[xx]

According to the *1991 Act*, any provider of encryption services (such as a TSP) can be obligated, upon receipt of notice, to provide their encryption keys to authorized officials, and assistance for the decryption of their products (unless the encryption provider shows that it is not in a position to fulfill these requisitions). Non-compliance with these obligations is punishable by a two-year prison term and a fine of €30,000.

Transmission Platforms

In order to reduce costs for the acquisition of data, the government decided to build a national platform for judicial requisitions. Without modifying the existing legal framework under which judicial interceptions are authorized by a judge, the platform will provide authorized officers with data related to traffic and the content of all types of telecommunications. The national platform, built by the company Thalès, is anticipated to be operational in September 2013 at a cost of €43 million (initial estimates were €17 million).[xxi]

Moreover, a mini platform or 'système de transmission des interceptions judiciaires' (STIJ) has been operational since 2008, though it only covers wireless services. It allows judicial police officers to receive a target's SMS and connection data (e.g. date and time) on their desktop. The cost for the implementation of the STIJ was €1 million, and it is estimated the STIJ saves the government €1.5 million annually. There are two other similar mini platforms currently operational (one for fixed Internet and the other one for mobile Internet). These three mini platforms will cease to be used once the national platform is operational.[xxii]

Safeguard Measures

The CNCIS is responsible for verifying the lawfulness of security interception requests and administrative requests for telecommunications data for the purpose of preventing terrorism, and preparing annual reports. With regard to judicial requisitions, there is no general report established, and the public is not informed due to investigative secrecy (any disclosure is an offense).

NEW ZEALAND

The power to intercept communications by LEAs in New Zealand is found in the *Search and Surveillance Act* 2012 (SASA).[4] The *New Zealand Intelligence Service Act* 1969 (the NZSIS Act) regulates lawful access to telecommunications by the New Zealand Secret Intelligence Service (the NZSIS). The Government Communications Security Bureau (GCSB)'s power to intercept telecommunications is detailed in *The Government Communications Security Bureau Act* 2003.

Lawful Interception of Telecommunications

The SASA allows LEAs, subject to receiving a surveillance device warrant signed by a judge, to intercept a telecommunication in relation to an offense that is punishable by a term of imprisonment of seven years or more, or specific offenses of the *Arms Act* 1983. These warrants are valid for no more than 60 days. Warrantless interceptions may be conducted in emergency situations (for a maximum duration of 48 hours), such as when an enforcement officer suspects that an offense punishable by a term of 14 years or more is about to be committed and obtaining a warrant is impractical in the circumstances.

Since the SASA came into force in April 2012, available data about the use of its powers only covers the period from April 18 to June 30, 2012. During this period, eight surveillance device warrants were issued and warrantless emergency powers were used three times. During the previous months of the same reporting year (2011/12), surveillance was conducted under a variety of other acts: 30 interception warrants (five renewals included), and one emergency permit (which allowed interceptions in emergency situations) were issued under the *Crimes Act* 1961; 38 interceptions warrants and three emergency permits were issued under the *Misuse of Drugs Act* 1978; and 24 tracking warrants (five renewals included) were issued. Thus, for the overall 2011/12 reporting period, around 76 interception authorizations were issued. For the 2010/11 and 2009/10 reporting periods, a total of 59 (one renewal included) and 100 interceptions were conducted under the *Misuse of Drugs Act* 1978 and the *Crimes Act* 1961, respectively.[xxiii] Thus, an average of around 78 interceptions warrants were issued annually over the last three reporting years. No figures on costs were available.

The NZSIS Act allows the NZSIS to carry out foreign and domestic intelligence warrants for interception. A foreign intelligence warrant is issued by the minister in charge of the NZSIS (traditionally the Prime Minister) where there are reasonable grounds to believe that no New Zealand citizen is going to be subject to the warrant and that any place to be specified in the warrant is occupied by a foreign organization or a foreign person. The

[4] The Act superseded lawful access powers contained in a range of other acts. The main ones include the *Crime Act* 1961, the *New Zealand Security Intelligence Service Act* 1969, the *Misuse of Drugs Amendment Act* 1978 and the *Terrorism Suppression Act* 2002.

Minister and the Commissioner of Security Warrants may jointly issue a domestic intelligence warrant for the detection of activities prejudicial to security. The Commissioner is appointed on the recommendation of the Prime Minister and is someone that formerly held office as a Judge of the High Court. His or her functions include considering requests for domestic intelligence warrants and issuing these warrants jointly with the Minister. Foreign and domestic warrants are valid for no more than 12 months.

From 2010 to 2012, an annual average of 24 domestic interception warrants were in force. Of those, an annual average of 14 were issued during the year under review, and an annual average of 10 were issued during the previous year but remained in force for some part of the year under review. During each year of the reporting period, foreign interception warrants were in force but the number of foreign interception warrants is not provided (this is not a requirement).[xxiv] No figures on costs were available.

Production Orders

The SASA also contains the power to issue a Production Order that allows LEAs to obtain specific non-content and content information that is collected and stored by TSPs in the normal course of business (there are no data retention requirements). Production orders must be issued by an issuing officer (e.g. a judge, justice of the peace, community magistrate, registrar, or deputy registrar). Production orders are valid for no more than 30 days. Orders may be issued for existing documents, or for documents that come into the service provider's possession or control at any time while the order is in force. No figures on production orders were available.

Access to Telecommunications Data

Under the SASA, LEAs can access telecommunications data by obtaining a surveillance device warrant or by issuing a production order if the information is collected by the TSP in the normal course of business.[5] The NZSIS can obtain non-content data, without a warrant or production order, through its authority to collect intelligence, coupled with exemptions under the *Privacy Act*. No figures related to this power were available.[xxv]

The Government Communications Security Bureau

The *Government Communications Security Bureau Act* 2003 provides for three main functions of the GCSB: information assurance and cyber-security, foreign intelligence, and co-operation with and assistance to other entities. The Act also confers three main interception powers on the GCSB: warrantless interceptions are allowed in situations not involving the physical connection of an interception device to a network, and not involving the installation of an interception device in any place in order to intercept

[5] Before the SASA came into force, LE could be issued call data warrant to access non-content data. The annual average number of call data warrants for the 2009/10 and 2010/11 reporting periods is 267.

telecommunications in that place; additionally, interception of communications by an interception device under an interception warrant and access to a computer system under a computer access authorization can be granted by the responsible minister. According to the Act, the GCSB cannot conduct foreign intelligence activities against New Zealanders. The way this restriction is incorporated in the Act suggests it also applies to the two other functions of the Bureau. This has resulted in a growing number of difficulties, and restricted the GCSB's ability to effectively carry out its other functions.[xxvi]

To resolve the difficulties in interpreting the GCSB Act (and other related matters), the New Zealand Government introduced the *Government Communications Security Bureau and related Legislation Amendment Bill* on May 8, 2013. The Bill outlines the functions of the GCSB and puts them into three separate clauses: intelligence gathering and analysis, co-operation with other entities to facilitate their functions, and information assurance and cyber-security. The bill clarifies that the restriction on targeting New Zealanders applies to the foreign intelligence activities of the GCSB and not to its other activities. To respect New Zealanders' privacy, any other activities that might involve intercepting the communications of New Zealanders would require an authorization jointly granted by the responsible minister and the Commissioner of Security Warrants (appointed under the *New Zealand Intelligence Service Act* 1969). Moreover, when the GCSB assists another entity under its ''co-operation with other entities to facilitate their functions'' power, the authorization processes and any restrictions or limitations that apply to that entity would apply to the Bureau's assistance.[xxvii]

Interception Capability Requirements

The *Telecommunications (Interception Capability) Act* 2004 (TICA) requires that a network operator must ensure that every public telecommunications network that the operator owns, controls, or operates, and every telecommunications service that the operator provides in New Zealand has an interception capability. The obligation to have an interception capability includes the duty to ensure that the interception capability is developed, installed, and maintained. The TICA also obliges TSPs (network providers and service providers) to assist surveillance agencies by making available any of the entity's officers, employees, or agents who are able to provide any reasonable technical assistance that may be necessary for the agency to intercept a telecommunication that is subject to the warrant or authority.[xxviii]

To be deemed intercept capable, a network operator must be able to obtain (without interfering with other telecommunications that are not authorized to be intercepted) content and non-content data related to the intercepted telecommunications in a format that is able to be used by surveillance agencies. A network operator must also decrypt telecommunications for which it provided the encryption. The Minister of the Crown may exempt any network operator from certain interception duties in special circumstances such as for a pilot trial for a new network.[xxix]

Network operators can determine their own interception capability design features as appropriate, including having the freedom to choose where and how they provide interception capability within their networks. The industry uses standards drawn from the European Telecommunications Standards Institute (ETSI).[xxx] The Ministry of Justice and the surveillance agencies maintain one Lawful Interception Administrator (LIA) that operates as a point of contact between the Government and the telecommunications industry. The LIA facilitates activities, such as compliance monitoring of lawful intercept solutions, as requested by the surveillance agencies and the Ministry of Justice.[xxxi]

In the case of non-compliance with interception obligations by a TSP (which include the duties to assist surveillance agencies), the High Court may make a compliance order requiring a TSP to do any specified thing or to cease any specified activity. If the High Court is satisfied that a TSP has acted in contravention of a compliance order, the Court may order the TSP to pay to the Crown a pecuniary penalty that must not exceed NZD $500,000 in addition to a further penalty of NZD $50,000 for each day the contravention continues.[xxxii]

The TICA came into force in April 2005 with a five year transition period, allowing for a gradual approach to full compliance. The costs to ensure that a public network has an interception capability must be paid by the network operator, with the exception of fixed and mobile networks that were operational on November 12, 2002, which were grandfathered by the government. The government estimated that the capital cost borne by TSPs over the transition period would be NZD $12 million.[xxxiii] Operational costs associated with providing assistance, as well as delivery of intercepted telecommunications, are borne by the government.[xxxiv]

The Telecommunications (Interception Capability and Security) Bill 2013

The *Telecommunications (Interception Capability and Security) Bill* 2013 (the TICS bill) was introduced on May 8, 2013, and seeks to replace the TICA. The bill would modify and clarify interception duties of TSPs and oblige network operators to engage with the GCSB on network security, where it might affect New Zealand's NS and economic well-being. Both the lawful interception and the network security frameworks would be underpinned by a compliance and enforcement framework.

With regard to interception capability, the bill would reduce or remove the obligations on some network operators in areas where capability is unnecessary for operational reasons, or duplicated or disproportionally expensive (standard obligations would remain substantially the same as in the TICA). Network operators with fewer than 4,000 customers would have the duty to be ''intercept ready'' (e.g. by pre-deploying certain access points on the network and reserving delivery ports and sufficient bandwidth to deliver intercepted material), wholesale network services would have to be ''intercept accessible'' (i.e. ensuring interception equipment can access their network, if required), and infrastructure-level services would have no capability obligation but an obligation to report customer names. The Minister would also be able to partially or fully reinstate capability obligations on TSPs with reduced obligations, if additional obligations are required for operational reasons.[xxxv]

The TICS bill clarifies obligations and duties of TSPs (which are substantially the same as in the current act). It states that the duty to assist is relevant to TSPs whether based in New Zealand or based overseas, and whether or not they have made prior investments in interception capability. The bill also specifies that network operators may share resources (e.g. equipment and staff) in order to meet their interception duties.[xxxvi]

The aforementioned measures would allow interception capability obligations to be extended, if needed, to TSPs that currently do not have any capability obligations such as application service providers (e.g. Facebook). The Bill would also provide for a new ministerial power to direct that off-shore TSPs must not be resold in New Zealand if there is insufficient interception capability on that service, and the direction is required to address a significant risk to NS or LE.[xxxvii]

With regard to network security, the TICS bill stipulates that network operators and the GCSB have to work co-operatively on identifying and addressing security risks. The bill obliges network operators to engage with the Director of the GCSB on the design, construction, and operation of networks where those may pose a risk to New Zealand's NS or economic well-being. Network providers would also have to notify the GCSB about procurement decisions related to areas in the network of particular NS interest.[xxxviii]

In addition, the Bill would provide for a ministerial direction power where either the Director of the GCSB is not satisfied with the network operator's proposal to address a significant NS risk, or a network operator has breached one of the requirements of the act and has proceeded with a decision or course of action that gives rise to a significant risk to NS.[xxxix]

In order to improve compliance, network operators would be required to register basic information (e.g. number of subscribers) with the government. Designated officers from LE and NS agencies would be allowed to require a network operator to supply information for the purpose of assisting a LE or NS agency to enforce compliance with interception duties or to execute an interception warrant or any other lawful interception authority. LE and NS agencies could also require certain network operators to have a staff with appropriate security clearances.[xl]

With regard to enforcement, the Bill would introduce a two-tiered enforcement regime for non-compliance that would distinguish between minor non-compliance, which would be dealt with by way of a notice requiring that the breach be remedied within a specified period of time, and serious non-compliance, which would be dealt with through the High Court.[xli]

Safeguard Measures

Under the SASA, officers must justify the use of production orders to neutral issuing officers. For interceptions, only a judge may issue a surveillance device warrant. Detailed reporting is required of the issuing officers and the chief executive of the relevant agency to Parliament. With regard to NS, the minister responsible of the NZSIS reviews all warrants issued each year and the Service's Annual Report to Parliament includes information about domestic warrants that were in force over that period. Also, details on operations conducted by the NZSIS under warrant are available to the Inspector General of Intelligence and Security. This independent authority is required by law to review the NZSIS's procedures. In addition, the Intelligence and Security Committee was established to review the NZSIS and the GCSB. This committee has a membership of five, including the Prime Minister and the Leader of the Opposition. The *Government Communications Security Bureau and related Legislation Amendment Bill* includes amendments that are focused on increasing the quality of external oversight over the intelligence agencies such as strengthening the office of the Inspector-General Intelligence and Security and improving the operation of Parliament's Intelligence and Security Committee.[xlii]

UNITED KINGDOM

The power to intercept telecommunications is found in the *Regulation of Investigatory Powers Act* 2000 (RIPA).

Lawful Interception of Telecommunications

RIPA warrants may be issued to intelligence or law enforcement agencies for the protection of NS, to safeguard the economic well-being of the UK, and to prevent and detect serious crimes. Instead of judicial authorizations, an administrative regime is established whereby Secretaries of State (usually the Home Secretary) or the Scottish Ministers approve a warrant. Warrants for the protection of NS and safeguarding the economic well-being of the UK are valid for no more than six months and those for the prevention and detection of serious crimes are valid for no more than three months. These warrants can be renewed (more than once) for a period of no more than the original number of months. RIPA permits warrantless interceptions in emergency situations such as when a kidnapper is telephoning relatives of a hostage.[xliii] Table 3 of the Annex outlines the main sections of the statute governing the use of RIPA powers and lists the agencies that can use RIPA's powers. The total number of lawful intercept warrants issued in

2011 under Part I, Chapter 1 of RIPA was 2,911.[xliv] In comparison, 1,983 and 1,973 warrants were issued in 2003 and 2004, respectively.[xlv]

Data Retention

As a member state of the European Union (EU), the UK is subject to the 2006 Data Retention Directive. UK TSPs must retain telecommunications data (i.e. non-content data) for 1 year. Table 4 lists the different telecommunications data types, as outlined in RIPA.

Requests for Telecommunications Data

RIPA requires requests for telecommunications data to be approved by a senior official in the applying agency, and the official must not be connected to the concerned investigation. The senior officer may only approve a request if he is satisfied that the tests of necessity and proportionality are met. An applicant must demonstrate that data is necessary in the investigation, and the senior official must assess the benefits of the requested data against invasion of privacy. According to the Interception of Communications Commissioner (ICC), 494,078 requests for telecommunications data were made in 2011 under Part I, Chapter 2 of RIPA (between January 2005 and March 2006, this number was 439,054).[xlvi] The Home Secretary may reimburse any expenses incurred by a service provider in complying with the provision of telecommunications data.

UK authorities are concerned that TSPs increasingly have less reason to keep certain types of telecommunications data that may nonetheless prove valuable for law enforcement. The UK government is considering whether to introduce a new bill that would enable the Home Secretary, when necessary, to require specific TSPs to retain telecommunications data where they would not otherwise retain it for business reasons. Under this bill, the Home Secretary would have the power to send notices, on a service-by-service basis, that describe the data that must be retained, where the data should be stored and, if necessary, how the data should be collected. The bill would cover overseas operators where they provide telecommunications services in the UK. No introduction date has been set for the bill.[xlvii]

Interception Capability Requirements for TSPs

The *Regulation of Investigatory Powers (Maintenance of Interception Capability) Order* 2002 defines the obligations of TSPs (and postal services) in accordance with section 12 of RIPA under which the Home Secretary can give notice to a TSP requiring it to maintain an interception capability. TSPs are obliged to provide assistance in giving effect to an interception warrant. Such obligations include providing intercepted materials to the relevant agencies, maintaining security and confidentiality, and facilitating the execution of the functions of the ICC. These obligations do not apply to service providers who provide service to less than 10,000 people in the UK or only provide a public telecommunications service in relation to the provision of banking, insurance, investment or other financial services.[xlviii] In the UK context, a public telecommunications service (i.e. a TSP) means any telecommunications service which is offered or provided to, or to a substantial section of, the public in any part of the UK. Thus, the requirement to maintain interception capability applies to TSPs such as ISPs and VoIP providers.

According to the provisions in the 2002 Order, TSPs need to enable an intercept within one working day of receiving a warrant, and ensure the completeness and near real-time transmission of intercepted data to the authorities. Moreover, the transmission of both the intercepted and related telecommunications data needs to be guaranteed. The handover interface must comply with any requirements communicated by the Secretary of State to the service provider, which, where practicable and appropriate, have to be in line with agreed industry standards such as those of the European Telecommunications Standards Institute (ETSI).[xlix]

Furthermore, a TSP must have the capability to simultaneously intercept the telecommunications of one in every 10,000 subscribers. The service provider must also be able to remove any encryption it applied to the intercepted telecommunication and the related telecommunications data. In addition, the service provider needs to ensure that the reliability of the interception carried out is at least equal the telecommunications service which would be transmitting the intercepted telecommunication.[l]

The intercept capability may be audited so that it is possible to confirm that the intercepted telecommunications and related telecommunications data are from or intended for the interception subject, or originate from or are intended for transmission to the premises named in the interception warrant. The service provider also has to comply with the aforementioned obligations in such a manner that the chance of the interception subject or unauthorized persons becoming aware of any interception is minimised. Non-compliance with intercept capability obligations may lead to civil proceedings by the Secretary of State.[li]

Concerning interception costs, section 14 of RIPA obliges the government to pay a "fair contribution".[lii] The government allocated a sum of £20 million to support TSPs for the three years from 2001 to 2004 in connection with RIPA intercept capability obligations, of which £14 million was spent in the first year.[liii]

Technical Advisory Board

If a TSP is served a notice to provide interception assistance and considers the technical or financial consequences of complying with the notice to be unreasonable, the service provider can refer the matter to the Technical Advisory Board (TAB). The TAB advises the Home Secretary on the reasonableness of any notice referred to it. This board comprises representatives from the UK government and the communications industry. After considering a report from the TAB, the Secretary of State may either withdraw the notice or give further notice confirming its effect, with or without modifications.[liv]

The National Technical Assistance Centre (NTAC)

Established after the introduction of RIPA in 2000 with £25 million in capital funding over two years, the National Technical Assistance Centre (NTAC) is currently part of the Government Communications Headquarters (GCHQ) and operates on behalf of all the LEAs and security and intelligence agencies, to provide a centralized facility for the implementation of interceptions and the processing of encrypted material. The centre has four main functions: conducting of lawful interception, enhancement of intercepts (e.g. the addition of data from other sources), decryption, and advice to government and industry.[lv]

Safeguard Measures

While there is no judicial involvement in granting interception warrants and access to telecommunications data, RIPA provides for the ICC (who must hold or have held judicial office) to oversee the use of lawful access powers by all surveillance agencies.[lvi] Moreover, the expenditure, administration and policies relating to lawful access activities conducted by MI5, MI6 and GCHQ are monitored by the Intelligence and Security Committee (ISC), a parliamentary committee.[lvii] In addition, the Intelligence Services Commissioner provides independent judicial oversight of MI6, MI5, GCHQ and a number of other public authorities such as NTAC.[lviii]

UNITED STATES

The power to intercept communications for LEAs is found in the *Omnibus Crime Control and Safe Streets Act of 1968* (Title III, for criminal investigations) and the *Electronic Communications Privacy Act* (ECPA). Electronic surveillance for foreign intelligence, counter intelligence, and terrorism investigations is governed by the *Foreign Intelligence Surveillance Act* (FISA). The *USA PATRIOT Act* strengthened surveillance authorities, mainly by adding provisions that broaden those already defined under FISA.

Lawful Interception of Communications

The number of authorized wiretap applications made by LEAs reported by year increased by 168% between 2000 and 2010. In 2011, a total of 2,732 intercepts were authorized by federal and states courts, and 98% of all authorized wiretaps were for portable devices (mobile telephones and digital pagers). For the same year, the average number of persons whose communications were intercepted was 113 per wiretap. FISA requires annual reports to Congress but these reports only note the total number of applications for surveillance (physical and electronic) and the total number of orders and extensions that were ordered, modified or extended. In 2011, 1,674 requests to conduct electronic surveillance were approved by the Foreign Intelligence Surveillance Court.[lix]

Access to Stored Communications

The *Stored Communications Act* lets LEAs retrieve and examine stored data (which includes stored emails, instant messages, web browsing history, search engine records as well as documents stored "in the cloud") and subscriber information (i.e. name; local and long distance telephone connection records, or records of session times and durations; length of service and types of services utilized; telephone or instrument number or other subscriber number or identity; and means and source of payment). Requirements to access data under this act range from probable cause search warrants to subpoena (no judicial approval required). Since there is no requirement to report on requests for stored communications and subscribers' records (except for requests made in emergency situations), there are no official statistics regarding such requests.[lx]

Access to Telecommunications Data

Pen register and ''trap and trace'' devices are used by LEAs to obtain telecommunications data (i.e. non-content data) in real time. The reporting requirements under the *Pen Register Act* only apply to LEAs within the Department of Justice. Thus, the true scale of non-content intercepts in the US is hard to assess, but it can be noted that in 2009, 12,444 pen registers and 11,041 trap and trace applications from LEAs within the Department of Justice were approved. Ten years before, in 1999, 4,949 pen registers and 1,553 trap and trace orders were issued.[lxi]

The FBI uses National Security Letters (NSLs) to retrieve financial, telecommunications, and credit information without judicial review on NS grounds. In 2011, the FBI made 16,511 NSL requests (excluding requests for subscriber information only) for information concerning US persons. Five federal statutes authorize intelligence officials to request certain business record information in connection with NS investigations via an NSL. One of these statutes, ECPA, specifically deals with telecommunications. NSLs issued by virtue of this act are addressed to telecommunications providers. In this instance, the authority is exclusive to the FBI. The FBI can request the name, address, length of service, and local and long distance toll billing records of a person or entity if the Director (or his designee) certifies in writing to a TSP that the subscriber information is relevant to an investigation to protect against international terrorism or clandestine intelligence activities. NSLs do not allow the FBI access to content data.[lxii]

TSPs' Obligations and Costs for the Government and LEAs

Under the *Communications Assistance for Law Enforcement Act* (CALEA) 1994 telecommunications carriers have to isolate, intercept, and deliver telecommunication content and call identifying information to LEAs pursuant to lawful authorization. Section 103 of the act (assistance capability requirements) requires that providers design and maintain capabilities that:

-allow customer traffic and signaling to be expeditiously and unobtrusively isolated;
-allow communications of multiple users to be simultaneously intercepted;
-allow transmission data to be isolated;
-allow the intercepted communication and the transmission data to be provided to LEAs;
-allow any measures taken to protect a communication such as encryption to be removed, where possible;
-ensure that all interceptions are kept confidential.

The CALEA requirements apply to telephone service providers, with the addition of facilities-based broadband Internet access providers, and providers of interconnected VoIP that offer services permitting users to receive calls from, and place calls to, the public switched telephone network. These requirements do not apply to intermediary services or to private networks.[lxiii]

The Federal Communications Commission (FCC) may exempt a class of telecommunications carriers from compliance with CALEA. The FCC may also take enforcement action under Section 229(a) of the *Communications Act* against entities that fail to comply with the CALEA obligations. CALEA provides that a non-compliant entity could be fined, after a court proceeding, up to $10,000 per day. Also, telecommunications carriers subject to CALEA are responsible for reviewing the FCC's regulations and analyzing how these regulations apply to their specific network architecture. The FCC does not get formally involved with the compliance standards development process unless a party files a special petition.[lxiv]

CALEA gives the lead role in setting electronic surveillance standards and solutions to the telecommunications industry. This delegation has created considerable tension between the FBI and the telecommunications industry throughout the standards development process. According to the FBI, LEAs' electronic surveillance needs are known to industry standards groups and only change to reflect the changes made in services offered by providers. For example, LEAs' need for location information is minimal in a wireline environment, but paramount for a wireless service. As a service provider offers more features, a provider's ability to furnish information regarding those features may need to increase.[lxv]

A TSP may comply with CALEA in three different ways. First, the TSP may design and implement its own compliance solution for its own network architecture. Second, the TSP may purchase a compliance solution from vendors such as the manufacturers of the equipment it is using to provide service. Finally, the TSP may purchase a compliance solution from a trusted third party (TTP). TTPs can provide a multitude of services for CALEA compliance to TSPs such as processing requests for intercepts, conducting electronic surveillance, and delivering relevant information to LEAs.[lxvi]

Also, CALEA requires TSPs to file and maintain an up-to-date Systems Security and Integrity (SSI) plan with the FCC, which contains information regarding the policies and procedures used for employee supervision and control, and to maintain secure and accurate records of each telecommunication interception or access to telecommunications data. Resellers of local exchange services, both facilities-based and switchless, must also comply with these rules by filing an SSI plan.[lxvii]

CALEA also assigns certain responsibilities to the Attorney General, equipment manufacturers, and the Department of Justice (DOJ) Office of the Inspector General (OIG). In 1995, the Attorney General delegated CALEA management to the Federal Bureau of Investigation (FBI).[lxviii] Table 5 summarizes the main CALEA statutory responsibilities of each entity previously mentioned.

TSPs must bear the costs of developing and installing intercept capable networks. Certain TSPs received funds from the government to upgrade equipment in use before January 1, 1995; $500 million was set aside by government to cover these costs. TSPs may charge operational fees for wiretaps, pen registers, trap and traces, and subscriber information look-ups, and costs associated with delivery.[lxix]

CALEA addresses what carriers need to provide to LEAs but does not address how data is delivered. Consequently, the delivery method of intercepted data varies by carrier. Due to the various delivery methods, LEAs must purchase additional equipment to receive the intercepted data from a carrier.[lxx]

TSPs' fees range from US$250 to US$3,100 to conduct pen register (for a 60-day period) and wiretaps (for a 30-day period). Fees for a traditional wiretap (i.e. without CALEA features[6]) are approximately US$250. In comparison, a wiretap with CALEA features costs LEAs approximately US$2,200. TSP invoices are not necessarily itemized (i.e. bills do not detail the charges for each intercept). When bills do not detail the charges for each intercept (e.g., initiation fee, maintenance fee, ''pinging'' fee, and cost of reports), LEAs can have difficulty assessing the reasonableness of the fees.[lxxi]

Safeguard Measures

In addition to judicial monitoring (such as submission of periodic reports to the judge who issued an interception order), oversight over lawful access activities is conducted in a number of ways. Surveillance conducted under Title III is monitored by both the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence. These two parliamentary committees must be informed, twice a year, about interceptions made under FISA in which intercepted information was used for law enforcement purposes. The Director of the Administrative Office is required to submit annual reports about interceptions made under Title III. The Attorney General is required

[6] The additional CALEA features are the capabilities to: (1) provide the content of subject-initiated conference calls supported by the subject's service, (2) identify the active parties of a multi-party call, (3) provide access to all dialing and signaling information available from the subject including a subject's use of features (e.g., the use of flash-hook and other feature keys), (4) notify the law enforcement agency when a subject's service sends a tone or other network message to the subject or associate (e.g. notification that a line is ringing or busy), (5) provide timing information to correlate call-identifying information with the call content of a communications interception, (6) and provide digits dialed by the subject after the initial call "cut-through" is completed to another carrier.

to submit annual reports on interceptions made under FISA and activities carried under the *Pen Register Act*.

Table 6 of the Annex provides a summary of the main lawful access legislation of the five countries that were discussed in this document.

ANNEX

Table 1: Main Lawful Access Tools (France)[lxxii]

	Authority	Fault Grounds	Length	Renewal
Security Interceptions	Prime Minister (section 3 of the *Act of 1991*)	•Terrorism •Organized Crime •National Security •Economic Security •Dissolved groups/organisations	4 Months	No limit
Judicial Interceptions	Investigative Judge (section 100 of the *Code of Criminal Proceedings*)	Criminal and correctional matters (potential sentence is equal or superior to 2 years of imprisonment)	4 Months	No limit
	Investigative Judge (section 80-4 of *the Code of Criminal Proceedings*)	Research the causes of death or disturbing disappearance	2 Months	No limit
	Public Department (Parquet) under the authority of a custodial judge (section 74-2, 695-36, and 696-21 of the *Code of Criminal Proceedings*)	Search for fugitives	2 Months	Renewable 3 times for correctional matters and no limit for criminal matters
	Public Department (Parquet) under the authority of a custodial judge (section 706-95 of the *Code of Criminal Proceedings*)	Organized Crime	15 Days	Renewable once

Table 2: Data Retention Obligations for Internet Service Providers (France)
(Decree No. 2011-219 of February 2011)

	Type of Technical Data
ISPs must retain:	•Identifier of the connection (e.g. IP address) •Identifier assigned to the subscriber (e.g. login name) •Identifier of the terminal used to access the Internet (e.g. the Media Access Control Address) •Dates and times of the beginning and end of the connection •Characteristics of the subscriber's line (e.g. call through the public switched network)
Service providers that provide public online communications, store information, writings, images, sounds or messages must retain:	•The identifier of the origin of the communication (originating IP address, or other relevant information such as the mobile phone number or the International Mobile Subscriber Identity (IMSI) number of the subscriber) •The identifier that the system assigns to the information content (uniform resource locator or location on a website's tree structure) •Types of protocols that are used to connect to the service (file transfer protocol, MMS, SMS) •Nature of the operation (e.g. creation, modification, deletion) •Date and time of the transaction •The identifier that the author used when creating or transmitting the content
Service providers must retain customer information provided for the creation of an account or the subscription to a contract (if they normally collect such information).	•The identifier of the connection used to create the account •Last name and first name •Postal addresses used •Pseudonym used •Associated e-mail addresses or accounts •Telephone numbers •Password as well as data allowing verifying or modifying it
When the subscription to a contract or an account requires a payment, service providers must retain for each payment operation contract (if they normally collect such information):	•Method of payment used •The amount •Date and time of the transaction

Table 3: RIPA Powers (UK)[lxxiii]

Power/Section of RIPA	When can this power be used?	Who can use the power?	Who authorises use of this power?	Who is responsible for Oversight
Interception of a person's communications (e.g. emails)/ Pt.1 Chapter 1	•National Security •Prevention and detection of serious crime •Safeguarding the economic well-being of the UK	•Intelligence Services: -Government Communications Headquarters (GCHQ) -Security Service (MI5) -Secret Intelligence Service (SIS) •Serious Organised Crime Agency (SOCA) •Scottish Crime and Drugs Enforcement Agency (SCDEA) •Metropolitan Police (Met) •Police Service for Northern Ireland (PSNI) •Scottish Police forces •HM Revenue and Customs (HMRC) •Defence Intelligence Staff (DIS)	Any of the Secretaries of State, but in practice the Secretary with responsibility for the investigating body will sign their respective warrants.	The Interceptions of Communications Commissioner.
The acquisition of telecommunications data (the who, when, and where of a communication) /Pt. 1 Chapter II	•In the interest of national security •Prevention / detection of crime •Safeguarding the economic well-being of the UK •In the interests of public safety •For the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department.	A wider group of public authorities can use the powers provided under Chapter 2 of the act than those under Chapter 1, including police forces, intelligence agencies, other enforcement agencies and local authorities. The full list of public authorities and their respective authorising personnel can be found in the Statutory Instrument (SI) at http://www.legislation.gov.uk/ukpga/2000/23/contents Although the list of bodies	A senior official in that public authority	The Interceptions of Communications Commissioner through a team of inspectors.

	•For the purpose, in an emergency, of preventing death or injury or damage to a person's physical or mental health. •For any additional purpose specified by an order from the Secretary of State.	is long, they have not all been given the same powers. The bodies are restricted in both the statutory purposes for which they may acquire data under Section 22(2) and the type of data they may acquire under Section 21(4).		
The investigation of electronic data protected by encryption/ Pt. III	•Interest of national security. •Prevention/ detection of crime. •Interests of economic well-being of the UK •For the purpose of securing the effective exercise or proper performance by any public authority of any identified statutory power or statutory duty.	Any public authority.	Authorisation is most frequently by a judge.	The Interception of Communications, Intelligence Services and Surveillance Commissioners, except when authorised by a judge.

Table 4: Types of Telecommunications Data (UK)[lxxiv]

Traffic Data
•Any data identifying, or purporting to identify, any person, apparatus or location to or from which the communication is or may be transmitted; •Any data identifying or selecting, or purporting to identify or select, apparatus through which, or by means of which, the communication is or may be transmitted; •Any data comprising signals for the activation of apparatus used for the purposes of a telecommunication system for effecting (in whole or in part) the transmission of any communication and; •Any data identifying the data or other data as data comprised in or attached to a particular communication, but that expression includes data identifying a computer file or computer program access to which is obtained, or which is run, by means of the communication to the extent only that the file or program is identified by reference to the apparatus in which it is stored.
Service Use Data
•Any data relating to the use made by any person of a communication service (e.g. itemized telephone call records showing the date, time and duration of calls made and the number dialled).
Subscriber Data
•Any data relating to information held or obtained by a TSP in relation to a customer (e.g. name and address of account holder or an email address).

Table 5: Summary of CALEA Statutory Responsibilities (US)[lxxv]

ENTITY	RESPONSIBILITY
FBI	•Ensures industry-wide implementation of the assistance capability requirements. •Consults with state and local law enforcement agencies. •Provides estimates to the telecommunications industry on the number of interceptions that government agencies may need to conduct. •Establishes rules to facilitate carrier reimbursements. •Allocates appropriated funds to carriers in a manner consistent with law enforcement priorities. •Annually reports to Congress the amount of carrier payments during the preceding year and the projected payments for the current year.
FCC	•Determines which entities are telecommunication carriers and may exempt any entity from compliance with CALEA by rulemaking and consulting with the FBI. •Establishes technical standards for compliance with assistance capability requirements if industry associations fail to issue technical standards, or if a government agency or any other person believes that industry-adopted standards are deficient. •Reviews and grants or denies petitions for extensions.
Telecommunications Carriers and Other Service Providers	•Ensure that equipment, facilities, or services that provide customers the ability to originate, terminate, or direct communications meet the CALEA assistance capability requirements.
Equipment Manufacturers	•Make available all features or modifications necessary to meet assistance capability requirements, including consulting with carriers over current and planned equipment.
OIG	•Reports to Congress biennially on the type of equipment, facilities, and services brought into compliance with CALEA and whether costs paid to each carrier for CALEA-required modifications were reasonable and cost effective.

Table 6: Main Lawful Access Legislation of Australia, France, New Zealand, the United Kingdom and the United States

	Main Lawful Access Powers for Law Enforcement and National Security Agencies	TSP's Intercept capability requirements
Australia	•*Telecommunications (Interception and Access) Act* 1979 (TIA Act)	•*Telecommunications Act* 1997 •TIA Act
France	•*Telecommunications Correspondence Secrecy Act of 1991* •*Code of Criminal Proceedings*	•*Posts and Telecommunications Code*
New Zealand	•*Search and Surveillance Act* 2012 (SASA) •*New Zealand Intelligence Service Act* 1969 •*Government Communications Security Bureau Act* 2003 •*Government Communications Security Bureau and related Legislation Amendment Bill**	•*Telecommunications (Interception Capability) Act* 2004 (TICA) •*Telecommunications (Interception Capability and Security) Bill* 2013*
United Kingdom	•*Regulation of Investigatory Powers Act* 2000 (RIPA)	•RIPA •The *Regulation of Investigatory Powers (Maintenance of Interception Capability) Order* 2002
United States	•*Omnibus Crime Control and Safe Streets Act of 1968* (Title III, for criminal investigations) •*Electronic Communications Privacy Act* (ECPA) •*Foreign Intelligence Surveillance Act* (FISA) •*USA PATRIOT Act*	•*Communications Assistance for Law Enforcement Act* 1994 (CALEA)

*Not yet enacted

[i] Telecommunications (Interception and Access) Act 1979, Report for the year ending 30 June 2012.

[ii]Telecommunications (Interception and Access) Act 1979, Report for the year ending 30 June 2012.

[iii]Telecommunications (Interception and Access) Act 1979, Report for the year ending 30 June 2012.

[iv] Telecommunications (Interception and Access) Act 1979, Report for the year ending 30 June 2012. p.70

[v] Australian Government, Attorney-General's Department, Equipping Australia Against Emerging and Evolving Threats, July 2012.

[vi] Australian Government, Attorney-General's Department, Interception Capability Obligations, Guidelines for Carriers and Carriage Service Providers, December 2010.

[vii] Australian Government, Attorney-General's Department, Interception Capability Obligations, Guidelines for Carriers and Carriage Service Providers, December 2010.

[viii] Australian Government, Attorney-General's Department, Interception Capability Obligations, Guidelines for Carriers and Carriage Service Providers, December 2010.

[ix] Australian Government, Attorney-General's Department, Equipping Australia Against Emerging and Evolving Threats, July 2012.

[x] Australian Government, Attorney-General's Department, Equipping Australia Against Emerging and Evolving Threats, July 2012.

[xi] ILETS Australian Paper 2010.

[xii] Code de procédure pénale, Article 100, http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=90DC590C3F611FFFB92234AD383340A4.tpdjo14v_3?cidTexte=LEGITEXT000006071154&idArticle=LEGIARTI000006575246&dateTexte=&categorieLien=cid and Code de procédure pénale, Article 706-95, http://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006071154&idArticle=LEGIARTI000006577810&dateTexte=&categorieLien=cid

[xiii] Fessard, Louise, ''Écoutes : ce que la police peut obtenir des opérateurs,''Mediapart, March 2012, http://blogs.mediapart.fr/blog/louise-fessard/260312/ecoutes-ce-que-la-police-peut-obtenir-des-operateurs

[xiv] http://www.lesinrocks.com/2011/09/buzzodrome/les-ecoutes-administratives-ont-progresse-de-19-en-2010/

[xv] Commission nationale de contrôle des interceptions de sécurité. 18e rapport d'activité, 2009 p.54-59.

[xvi] Fessard, Louise, ''Écoutes : ce que la police peut obtenir des opérateurs,''Mediapart, March 2012, http://blogs.mediapart.fr/blog/louise-fessard/260312/ecoutes-ce-que-la-police-peut-obtenir-des-operateurs

[xvii] http://www.lesinrocks.com/2011/09/buzzodrome/les-ecoutes-administratives-ont-progresse-de-19-en-2010/

[xviii] http://www.lepoint.fr/actualites-societe/2009-07-28/les-interceptions-de-communications-en-forte-hausse-en-france/920/0/365081

[xix] Sénat, ''Projet de loi de finances pour 2012 : Justice judiciaire et accès au droit,'' http://www.senat.fr/rap/a11-112-13/a11-112-1311.html#toc94
Sénat, ''Projet de loi de finances pour 2010 : Justice et accès au droit, B. D'importantes difficultés de gestion des frais de Justice,'' http://www.senat.fr/rap/a09-106-4/a09-106-46.html

[xx] http://lexpansion.lexpress.fr/high-tech/internet-sms-comment-thales-va-mettre-les-reseaux-francais-sur-ecoute_383757.html#Ds8I1vMX5jMD46ec.99

[xxi] http://lexpansion.lexpress.fr/high-tech/internet-sms-comment-thales-va-mettre-les-reseaux-francais-sur-ecoute_383757.html

[xxii] http://lexpansion.lexpress.fr/high-tech/internet-sms-comment-thales-va-mettre-les-reseaux-francais-sur-ecoute_383757.html

[xxiii] New Zealand Police, Annual Report 2011/2012, http://www.police.govt.nz/about-us/publications/corporate/annual-report

[xxiv]New Zealand Security Intelligence Service http://www.security.govt.nz/assets/media/annual-reports/nzsis-ar12.pdf, p.16.

[xxv] ILETS, June 2011, Legal Telecommunications Interception in New Zealand, STC/LPWG Meetings

[xxvi] Parliamentary Library, Bill Digest No. 2046, Government Communications Security Bureau and Related Amendment Bill (2013 No 109-1), http://www.parliament.nz/resource/0000262182

[xxvii] Parliamentary Counsel Office, Government Communications Security Bureau and Related Legislation Amendment Bill, Explanatory note

[xxviii] http://www.legislation.govt.nz/act/public/2004/0019/latest/DLM242336.html

[xxix] http://www.legislation.govt.nz/act/public/2004/0019/latest/DLM242336.html

[xxx] TFC Telecommunications Carriers Forum, Guideline for Interception Capability, August 2009.

[xxxi] ILETS, Legal Telecommunications Interception in New Zealand, June 2011

[xxxii] http://www.legislation.govt.nz/act/public/2004/0019/latest/DLM242336.html

[xxxiii] Telecommunications (Interception Capability) Bill, Government Bill, As reported from the Law and Order Committee, Commentary, p.5-6. http://legislation.knowledge-basket.co.nz/gpprint/docs/bills/20030152.txt

[xxxiv] http://www.legislation.govt.nz/act/public/2004/0019/latest/DLM242336.html

[xxxv] Telecommunications (Interception Capability and Security) Bill, Explanatory Note, http://www.legislation.govt.nz/bill/government/2013/0108/5.0/DLM5177901.html

[xxxvi] Telecommunications (Interception Capability and Security) Bill, Explanatory Note, http://www.legislation.govt.nz/bill/government/2013/0108/5.0/DLM5177901.html

[xxxvii] Telecommunications (Interception Capability and Security) Bill, Explanatory Note, http://www.legislation.govt.nz/bill/government/2013/0108/5.0/DLM5177901.html

[xxxviii] Telecommunications (Interception Capability and Security) Bill, Explanatory Note, http://www.legislation.govt.nz/bill/government/2013/0108/5.0/DLM5177901.html

[xxxix] Telecommunications (Interception Capability and Security) Bill, Explanatory Note, http://www.legislation.govt.nz/bill/government/2013/0108/5.0/DLM5177901.html

[xl] Telecommunications (Interception Capability and Security) Bill, Explanatory Note, http://www.legislation.govt.nz/bill/government/2013/0108/5.0/DLM5177901.html

[xli] Telecommunications (Interception Capability and Security) Bill, Explanatory Note, http://www.legislation.govt.nz/bill/government/2013/0108/5.0/DLM5177901.html

[xlii] Parliamentary Library, Bill Digest No. 2046, Government Communications Security Bureau and Related Amendment Bill (2013 No 109-1), http://www.parliament.nz/resource/0000262182

[xliii] RIPA http://www.legislation.gov.uk/ukpga/2000/23

[xliv] 2011 Annual Report of the Interception of Communications Commissioner, 2011, http://www.intelligencecommissioners.com/docs/0496.pdf, p. 16.

[xlv] 2003 Annual Report of the Interception of Communications Commissioner http://www.statewatch.org/news/2004/jul/uk-tel-tap-surv-2003.pdf
2004 Annual Report of the Interception of Communications Commissioner http://www.statewatch.org/news/2005/nov/teltap-2004.pdf

[xlvi] 2011 Annual Report of the Interception of Communications Commissioner, 2011, p.28.http://www.intelligencecommissioners.com/docs/0496.pdf,

[xlvii] Home Office, ''Communications Data Bill published,'' June 2012, http://www.homeoffice.gov.uk/media-centre/news/communications-data-bill and https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97987/key-background.pdf

[xlviii] The Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002, http://www.legislation.gov.uk/uksi/2002/1931/made

[xlix] The Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002, http://www.legislation.gov.uk/uksi/2002/1931/made

[l] The Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002, http://www.legislation.gov.uk/uksi/2002/1931/made

[li] The Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002, http://www.legislation.gov.uk/uksi/2002/1931/made

[lii] RIPA, http://www.legislation.gov.uk/ukpga/2000/23

[liii] Industry Canada Documents on Lawful Access, 2006, http://www.scribd.com/doc/79972705/Industry-Canada-documents-on-Lawful-Access-c-2006

[liv] TAB annual report 2011/2012, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/143753/tab-report-2011-12.pdf

[lv] http://www.cyber-rights.org/documents/ntac.htm

[lvi] RIPA, Part IV, http://www.legislation.gov.uk/ukpga/2000/23

[lvii] The Intelligence and Security Committee of Parliament, http://isc.independent.gov.uk/

[lviii] Intelligence Services Commissionner, https://www.gov.uk/government/organisations/intelligence-services-commissioner

[lix] Soghoian, Christopher, ''The Law Enforcement Surveillance Reporting Gap,'' 2012, p. 17-18; Parsons, Christopher, ''Lawful Access and Data Preservation/Retention: Present Practices, Ongoing Harm, and Future Canadian Policies,'' February 7, 2012, p. 10-11; Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications. http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2011/2011WireTap.pdf7.

[lx] Soghoian, Christopher, ''The Law Enforcement Surveillance Reporting Gap''

[lxi] Soghoian, Christopher, ''The Law Enforcement Surveillance Reporting Gap,'' 2012, p. 15-16; Parsons, Christopher, Lawful Access and Data Preservation/Retention: Present Practices, Ongoing Harm, and Future Canadian Policies, February 7, 2012, p. 11.

[lxii] Doyle, Charles ''National Security Letters in Foreign Intelligence Investigations: Legal Background and Recent Amendments,'' Congressional Research Service, September 8, 2009, 1-2.

[lxiii] Federal Communications Commission, CALEA, http://transition.fcc.gov/calea/

[lxiv] FCC Encyclopedia, http://www.fcc.gov/encyclopedia/communications-assistance-law-enforcement-act#CCSBI

[lxv] Implementation of the Communications Assistance for Law Enforcement Act by the Federal Bureau of Investigation, March 2006, http://www.justice.gov/oig/reports/FBI/a0613/findings.htm

[lxvi]FCC Encyclopedia, http://www.fcc.gov/encyclopedia/communications-assistance-law-enforcement-act#CCSBI

[lxvii] http://transition.fcc.gov/pshs/services/calea/

[lxviii] Federal Communications Commission, CALEA, http://transition.fcc.gov/calea/

[lxix] Federal Communications Commission, CALEA, http://transition.fcc.gov/calea/

[lxx] The Implementation of the Communications Assistance for Law Enforcement Act, March 2006, http://www.justice.gov/oig/reports/FBI/a0613/findings.htm

[lxxi] The Implementation of the Communications Assistance for Law Enforcement Act, Punch List, March 2006, http://www.justice.gov/oig/reports/FBI/a0613/app9.htm

[lxxii] Commission nationale de contrôle des interceptions de sécurité. 18e rapport d'activité, 2009 p. 54.

[lxxiii] 2011 Annual Report of the Interception of Communications Commissioner, 2011, http://www.intelligencecommissioners.com/docs/0496.pdf, p. 5-6.

[lxxiv] RIPA, Part 1, Chapter II, http://www.legislation.gov.uk/ukpga/2000/23

[lxxv] Implementation of the Communications Assistance for Law Enforcement Act by the Federal Bureau of Investigation, March 2008, http://www.crypto.com/papers/doj-08-20-redacted.pdf

26/07/2013

Foiled Terrorist Plots Associated with the Disclosure of National Security Agency Surveillance Programs

The Two Authorities Involved in the disclosed Surveillance Programs[1]

•Section 215 of the PATRIOT Act – this business records provision allows the government to collect metadata: the number that was dialed from, the number that was dialed to, the date and the length of time. Section 215 does not allow getting the identity of any parties to the phone call, nor does it allow getting the content of the communication and any cell site or location information as to where any of these phones were located.

•Section 702 of the FISA Amendment Act – this statute allows the government to collect the content of emails and phone calls of foreigners – not Americans – located outside the United States. In order to target a person, they have to be neither a US citizen nor a permanent US resident, and they need to be outside of the United States while they are targeted. If the target makes a call to inside the US, that can be collected, because the target of that call initiated the call from outside the US. This statute prohibits reverse-targeting, which is where one targets somebody who is out of the US, but the real goal is to capture the conversations with somebody who is inside the US.

General Info about the Foiled Plots mentioned by the NSA Director[2]

Of the 54 cases turned over to Congress in June 2013:

•12 involved cases of material support to terrorists;
•50 lead to arrests or detentions;
•25 occurred in Europe;
•11 were in Asia;
•5 were in Africa;
•13 had a homeland nexus;
•50 will remain classified.

<u>Cases Released by the US Government on June 2013</u>[3]

NYC Attack Plot 2009

In early September of 2009, while monitoring the activities of Al Qaeda terrorists in Pakistan, NSA noted contact from an individual in the US that the FBI subsequently identified as Colorado-based Najibullah Zazi. The US Intelligence Community, including the FBI and NSA, worked in concert to determine his relationship with Al Qaeda, as well as identify any foreign or domestic terrorist links.

The FBI tracked Zazi as he traveled to New York to meet with co-conspirators, where they were planning to conduct a terrorist attack. Zazi and his co-conspirators were subsequently arrested. Zazi, upon indictment, pled guilty to conspiring to bomb the NYC subway system.

Compelled collection (authorized under FISA Section 702) against foreign terrorists was critical to the discovery and disruption of this threat against the US.

[1] http://westmoreland.house.gov/images/6-19-13%20Intel%20Hearing%20Transcript%20NSA%20Leaks.pdf
[2] http://westmoreland.house.gov/images/6-19-13%20Intel%20Hearing%20Transcript%20NSA%20Leaks.pdf
[3] http://westmoreland.house.gov/index.php?option=com_content&view=article&id=854&Itemid=363

Chicago Terror Investigation

In October 2009, David Coleman Headley, a Chicago businessman and dual US and Pakistani citizen, was arrested by the FBI as he tried to depart from Chicago O' Hare airport on a trip to Europe. Headley was charged with support to terrorism based on his involvement in the planning and reconnaissance of the hotel attack in Mumbai 2008.

At the time of his arrest, Headley and his colleagues were plotting to attack the Danish newspaper that published the unflattering cartoons of the Prophet Mohammed, at the behest of Al Qaeda.

Compelled collection (authorized under FISA Section 702) against foreign terrorists and metadata analysis (authorized under the business records provision of FISA) were utilized in complement with the FBI law enforcement authorities to investigate Headley's overseas associates and their involvement in Headley's activities.

Bosaaly Moalin

In October 2007, NSA provided the FBI with information obtained from querying the metadata obtained under Section 215. This information established a connection between a phone known to be used by an extremist overseas with ties to Al Qaeda's East Africa network, and an unknown San Diego-based number running on the Verizon network.

That tip ultimately led to the FBI's opening of a full investigation that resulted in a February 2013 conviction of Basaaly Moalin and three others for conspiring to provide material support to al Shabaab, a State Department-designated terrorist group in Somalia that engages in suicide bombings, targets civilians for assassination, and uses improvised explosive devices.

Operation WI-FI

In January 2009, using authorized collection under Section 702 to monitor the communications of an extremist overseas with ties to Al Qaeda, NSA discovered a connection with an individual based in Kansas City. NSA tipped the information to FBI, which during the course of its investigation uncovered a plot to attack the New York Stock Exchange.

NSA queried metadata obtained under Section 215 to ensure that we identified all potential connections to the plot, assisting the FBI in running down leads.

Additional Cases mentioned in the Media

Foiled plots in Germany

German officials stressed that the NSA contributed in stopping terror plots in Germany, and mentioned that tips from American source had foiled a 2007 plot to attack U.S. troops and citizens in Germany. This case is known as the Sauerland cell plot: four Islamist extremists were convicted of terrorism charges, including planning a massive car bombing near a U.S. Air Force base in Germany.[4] Some news articles suggest that NSA's involvement in this case was minimal or remains unverified.[5]

[4] http://articles.washingtonpost.com/2013-06-27/world/40231068_1_alexander-collection-program-plots and http://www.mcclatchydc.com/2013/07/18/197051/germany-backs-away-from-claims.html

[5] http://www.scmp.com/news/world/article/1287842/germany-backs-down-over-number-terror-attacks-foiled-us-programme

Emmett, Jamie

From:	Durand, Mathieu
Sent:	July-22-13 3:30 PM
To:	Plunkett, Shawn
Subject:	Lawful interception and countermeasures

Shawn,

I just found that on Google. It might be of some interest.

http://kth.diva-portal.org/smash/get/diva2:511012/FULLTEXT01.pdf

M

Lawful Interception and Countermeasures

In the era of Internet Telephony

ROMANIDIS EVRIPIDIS

KTH Information and
Communication Technology

Master of Science Thesis
Stockholm, Sweden 2008

COS/CCS 2008-20

LAWFUL INTERCEPTION AND COUNTERMEASURES: IN THE ERA OF INTERNET TELEPHONY

BY

Romanidis Evripidis

Examiner: Gerald Q. Maguire Jr.

Supervisor: Gerald Q. Maguire Jr.

2008-09-22

Thesis submitted in partial fulfillment of the requirements for a Master's of Science Degree.

School of Information and Communication Technology
Royal Institute of Technology
Stockholm, Sweden

Abstract

Lawful interception and the way it is performed have played a significant role in the effectiveness of this type of communication monitoring. Although the secrecy of interception and the related equipment are supposed to provide correct information to a law enforcement agency, there are some countermeasures that can be taken by the subject that can seriously undermine the collection of correct and accurate data.

This thesis project attempts to identify the problems that exist for interception of telephony (be it fixed, mobile, or via the Internet). Moreover, there are some suggestions for improvements how lawful interception should be performed in order to avoid possible attacks that could decrease the credibility of the intercepted data.

Numerous publications (in print or distributed on the Internet) have described weaknesses in the current state of the art lawful interception when using equipment that can be purchased in the market. This thesis presents improvements in how LI can be conducted in order to avoid these vulnerabilities. Additionally, there is a description of the key escrow systems and the possibility of avoiding one of their most significant vulnerabilities.

The main problem of the lawful interception is the rapid changes in telecommunications and the complicated architecture of the telecommunication networks, as both make monitoring vulnerable to specific countermeasures. An analysis of how lawful interception can take place and current countermeasures for lawful interception of Internet telephony are vital in order to identify the problems in carrying out such intercepts today and to make suggestions for improvements.

This topic is especially relevant given the current Swedish "FRA lagen" regarding interception of electronic communication going into, out of, and through Sweden. Not only is it important to understand how lawful interception can be performed or prevented, but it is also important to understand how information obtained from lawful interception could be purposely misleading or falsified.

Acknowledgements

I would like to thank my supervisor, Professor Gerald Maguire, for his excellent guidance during the whole thesis. Even if we had to communicate through emails – because of our long distance – our communication did not confront any problems. His answers to my questions were very helpful and his proposals very illuminating. I really want to thank him for not having a problem of letting me working by distance.

Table of Contents

Table of Figures

List of Acronyms and Abbreviations

ADMF	Administrator Function
ANSI	American National Standards Institute
ATA	Analog Telephone Adaptor
CALEA	Communication Assistance for Law Enforcement Act
CC	Contents of Communications
CCC	Call Contact Channels
CD	Call Data
CDC	Call Data Channel
CDR	Call Detail Records
CNID	Calling-number ID
CO	Central Office
DHCP	Dynamic Host Configuration Protocol
DNR	Dialed Number Recorder
DOJ	(U.S.) Department of Justice
DTMF	Dual-tone Multi Frequency
ETSI	European Telecommunication Standard Institute
E.U.	European Union
FBI	(U.S.) Federal Bureau of Investigation
FISA	(U.S.) Foreign Intelligence Surveillance Act
GUI	Graphical User Interface
HI	Handover Interfaces
IETF	Internet Engineering Task Force
IIF	Internal Intercept Function
IMS	Interception Management System

INI	Internal Network Interface
IP	Internet Protocol
IRI	Intercept Related Information
ISP	Internet Service Provider
KRC	Key Recovery Center
LEA	Law Enforcement Agencies
LEAF	Law Enforcement Access Field
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
MAC	Media Access Control
MF	Mediation Function
MIKEY	Multimedia Internet KEYing
MKI	Master Key Identifier
NSA	(U.S.) National Security Agency
PAS	Priority Access Service
PKI	Public Key Infrastructure
POTS	Plain Old Telephone Service
PSK	Pre-shared key
PSTN	Public Switched Telephone Network
PTN	Public Telecommunication Network
RES	Remote-control Equipment Subsystem
RFC	Request For Command
RTP	Real-time Transport Protocol
SMS	Short Message Service
SRTP	Secure Real-time Transport Protocol

TTP	Trusted Third Party
U.S.A.	United States of America
VoIP	Voice over IP

1 Introduction

1.1 A brief introduction to lawful intercept

Governments always desire the ability to monitor people (inside or outside their own nation) in order to control these people and to formulate their policies. Even though there were several illegal means to achieve this, within the scope of democracy, the respect of human rights and the existence of different types of telecommunications many different legal ways of monitoring have been employed. The result of this trend was the introduction of the term of **lawful intercept (LI),** which is used to describe both the **means** and **mechanisms** for law enforcement agencies (LEAs) and other government agencies to have *the technical ability and the authorization to perform* a lawful interception of the communication of persons that are believed to have committed illegal actions (or in some case to have the *intention* of committing serious crimes). However, as in most facet of human life, even though lawful intercept may often times provide useful information concerning illicit actions (i.e., terrorism or kidnapping) there have been several instances where interception has also been used for *illegal monitoring* of persons who were simply political adversaries or persons that had different opinion from the current government. As a consequence, many people mistrust lawful interception (even if it is legal under certain circumstances); as they believe that it violates one of their fundamental human rights – the right of privacy in communication and that the statutes governing lawful interception may potentially be misused to conduct *illegal* interception.

1.2 Methods to analyze LI and countermeasures against LI

Lawful intercept is not stable, as it must always adapt to new ways and patterns of communication. When LI was first used only the traditional telephone was used (although prior to this telegraph messages could also be intercepted). However, with the advent of mobile communication system and the Internet and their rapid & widespread adoption, governments and their agencies have begun to consider how these methods of communication can be included in their lawful monitoring (which includes how to modify and adapt earlier laws designed for telephony, telegraphy, and radio communication to address these new communication technologies).

In fixed and mobile telephony, interception can be considered quite easy as the communication passes through a small number of networks that belong to public or private companies. It is easy for these companies to control their networks and to define where agencies can easily connect their monitoring devices. In most cases this is particularly easy as these networks have very centralized control and there are relatively speaking few connections from one network to another. Interception is especially easy for fixed and mobile telephony operators as the agencies do not have to setup any devices as the operators have generally already installed the appropriate software for interception (in some cases this was a legal requirement for them as an operator in a given country). However, for Internet and particularly in Voice over IP (VoIP) interception there appears to be very weak control by government agencies. In part this happens due to the nature of the Internet. As the Internet is a global network that has many different routes to send information to the same destination and lacks centralized control. There has also been no economic reason for Internet service providers (ISPs) to maintain detailed records of packet traffic, but rather to simply keep statistics (for example, total number of packets per month or total number of gigabytes sent or received in a billing cycle). Additionally, keeping more detailed traces of traffic would only increase the operator's cost and would neither improve service for the customer nor generate additional revenue. This means that it is not so easy to track the route of a conversation or to intercept all of a conversation of a possible criminal activity.

However, monitoring of traditional telephony & telegraph communications is not always successful. Target users can use several countermeasures in order to avoid interception, depending on the medium of communication they use (i.e. Internet, fixed, or mobile telephony). Additionally, these countermeasures may also result in false or misleading information being recorded.

1.3 Problem to be addressed by this thesis project

As countermeasures often spoil lawful interception, governments have tried (and still try) to circumvent these countermeasures. One of the ways to surpass the threat (to LI) of increasing use of encryption was the use key escrow systems. With these systems, trusted organizations maintain a depository of the master keys of all the conversations in order for a LEA to be able to intercept later of someone who is a "target" of an LEA. These key escrow systems were thought to give the government absolute control for their monitoring as key escrow eliminates the problems of the LEA being unable to access the plain text of either the signaling or the communication - when faced with encryption and no-cooperation of companies that provide a communication service or in some cases even the end users themselves. In order to be certain success, the use of a key escrow system must include the majority – if not all – of the products and services that provide encrypted communication.

However, many doubts exist as to the potential for success of a large scale key escrow system. Many people including individual cryptographers and individuals point to severe security flaws and violation of privacy (respectively) as reason not to pursue key escrow system. The analysis of the opponents of the key escrow systems successfully raised serious doubts as to the possibility of a successful implementation of a key escrow system.

1.4 Importance of this problem

There is no doubt that today many governments conduct LI. The exact number of intercepts which are conducted is not always clear, but a clear statistic is that the number of LIs in recent years is substantial [48]. Additionally the growing use of voice over IP is introducing new problems both for the regulations for LI of this means of communication and the technical abilities of the LEAs [49].

Many people in government agencies still believe that a key escrow system can be implemented and would definitely help them in intercept the communication of terrorists and other criminals. Even if it is considered difficult to implement a key recovery system which would include all the communication products that provide encryption, there are thoughts that it could be used at least in some of the products that are used by millions of users worldwide (i.e. Skype or other VoIP hardware/software) [39]. This belief becomes more apropos as the pressure from governments to control communications increases every year, highlighted by global terrorism and the perceived need to eliminate it. Could key escrow systems yet be the answer for the interception of communications that were previously difficult to be intercepted? Still many people (cryptographers, human rights organizations, and individuals) do not agree that key escrow is the solution. More details of this are presented in Chapter 5.

1.5 Thesis overview

This thesis project's main focus is to examine if a key escrow system could be viable when utilized with VoIP software. As many different types of VoIP software are used by millions of users around the world and many provide encryption between the parties in a conversation it is considered important by many government agencies to find a way that will provide them with easy and continuous access to these encrypted communications sessions. One of the solutions has been proposed several times are key escrow systems. However, there are strong indications that these kinds of systems cannot be considered a wise solution, as they suffer from security flaws and human rights violation. This thesis will examine key escrow in the context of a software VoIP system from a technical point of view in order to determine if there are also technical reasons why such a solution will not be feasible or successful in achieving the aims of many governments.

The objective of the overall thesis is to provide the reader with a general understanding of what lawful interception is and some of the problems that law enforcement agencies are facing. Chapter 2 gives a description of what lawful interception is and why is it desired so much by many governments. Chapter 3 describes how lawful interception can be performed in fixed and mobile telephony and enumerates some of the problems that LEAs can face due to specific countermeasures that targeted users can currently employ. Chapter 4 introduced VoIP communication and the problems that arise when attempting to monitor this communication. Chapter 5 presents an analysis of key escrow systems and the advantages and disadvantages of using them in communication products and software that encrypts the signaling and/or session content. Chapter 6 describes a way to avoid the problem of insider misuse of a key escrow system through the use of digital signatures. Finally, chapters 7 and 8 presents conclusions and future work (respectively).

2 Lawful Interception

2.1 What is lawful Interception?

Lawful Interception (LI) is not something new in our lives. During the last 50-60 years governments around the world have evaluated and used systems that are able to trace and intercept telecommunications in an attempt to prevent possible social hazards that might arise or to gather evidence for criminal prosecution of individuals for serious crimes. In the beginning the interception of the public telecommunications were done without any legal authorization. However, this situation has changed; over the years various legislatures have created and introduced laws defining the legal framework and authority for the government to perform interception.

One definition of Lawful Interception (LI) is "the acquisition of call identifying information and the interception of communications contents" by law enforcement agencies (LEAs) after receiving proper authorization from competent authorities [1]. The competent authorities are the mediator organizations that stand between the agency that wants to perform the interception and the network operator(s). Lawful interception can be performed in all modern systems -- including the Public Switched Telephone Network (PSTN), wide area wireless networks (e.g., mobile telephony), cable television systems, and the Internet. Although the monitoring of the fixed lines is a well- known procedure of law enforcement and intelligence services, in recent years challenging new obstacles have arisen. One such problem is tracking an end-user that uses a mobile phone or Voice over IP (VoIP); as both of these technologies allow the user to easily change their physical location (hence both offer *mobile communications*). Such mobile communications is significantly more difficult to intercept than traditional fixed telephony. Hence, users of such mobile communications are becoming much harder to track.

Although the details of LI differ between the different types of interceptions, there are some basic requirements that every interception has. A LI system must provide transparent interception of only the specified traffic, and the subject must **not** be aware of the interception. Moreover, during an interception other telephone users must **not** be affected in any way by degrading their provisioned service. Furthermore, in every interception there are some minimum data that must be collected and recorded in order for the intercept to be used later as evidences in a legal proceeding. So, in every type of interception there is a need to determine the presence, identity, and location of the parties of the specified communication.

Due to the increasing number of the terrorist attacks all over the world, governments and their intelligence services have re-examined the importance of legally monitoring telecommunications. Furthermore, in most countries these authorities assert that LI can be used in all cases of *wireless emergency calling* and *priority access calling* [2]. As far as the wireless emergency service is concerned, LI can be used for tracking and prosecution of the persons who intentionally make **false** emergency calls (i.e., calls to '911' in Unites States and '112' in Europe). Making false emergency calls is an illegal act, because it ties up resources that might be needed by someone who actually has an emergency. Moreover, LI can be used to enable a Priority Access Service (PAS). PAS can provide the necessary access to the authorities and governmental officials to make priority calls *despite* the telecommunication networks being congested or otherwise lacking resources. Again there is a need to ensure that PAS is only used for proper purposes and that abuses can be prosecuted [7].

Nevertheless, there are many organizations and people that do not believe that the usefulness of interception in preventing, detecting, deterring, and prosecuting criminal or terrorist acts is worth the risk of the violation of individual's rights, privacy, and personal integrity. Thus in most jurisdictions there are a need for balance between interception and privacy.

2.2 Architecture of LI elements

Even though there are some differences in the details of how interception is performed, the main architecture of LI all around the world is basically the same. The primary LI requirements and standards have been developed by the European Telecommunications Standard Institute (ETSI) in Europe and by ANSI in the United States of America (U.S.A.). In the USA, the regulations concerning LI are spelled out in the Communications Assistance for Law Enforcement Act (CALEA) [3]. In both Europe and the U.S.A., a dominant theme was to design LI systems such that information concerning an interception is communicated *only* to those persons in the telecommunication operator's network that *must* be involved in a given intercept, in order to reduce the possibility that someone might compromise an investigation; while simultaneously ensuring that *only* the legally authorized type of interception is applied and that it is *only* applied *to the specified targets of the investigation* (i.e., to avoid intercepting traffic which is not the target of a legal intercept).

The organization that primarily defined the architecture of LI systems (not only in Europe but also worldwide) is ETSI. Figure 1 gives a generalized overview of the proposed ETSI LI systems architecture.

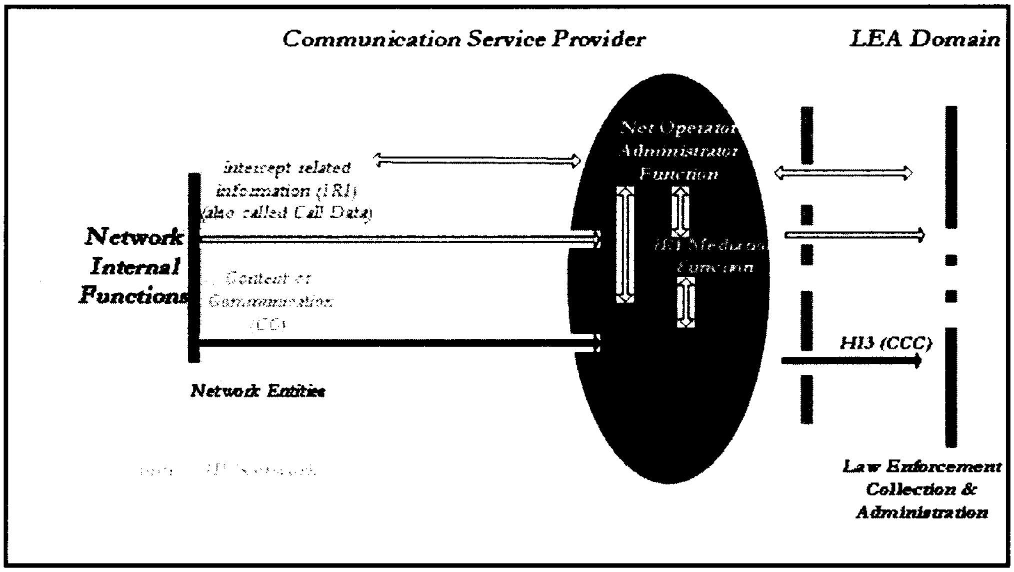

Communication Service Provider
LEA Domain
Net Operator Administrator Function
intercept related information (IRI) (also called Call Data)
Network Internal Functions
IRI Mediation Function
Content of Communication (CC)
HI3 (CCC)
Network Entities
Law Enforcement Collection & Administration

Figure 1: General Network Arrangements for Interception as proposed by ETSI (Adapted from [18])

This architecture describes how network operators and law enforcement agencies (LEAs) interact; even as networks expand and as these networks provide new services. This general architecture can be applied to all types of intercepts, e.g., to fixed lines, mobile calls, instant messaging, email, and VoIP. In the U.S.A., after the enactment of CALEA, the PacketCable surveillance model [3] is being used (See Figure 2). This approach has many similarities with the ETSI LI model and primarily differs in the terminology used.

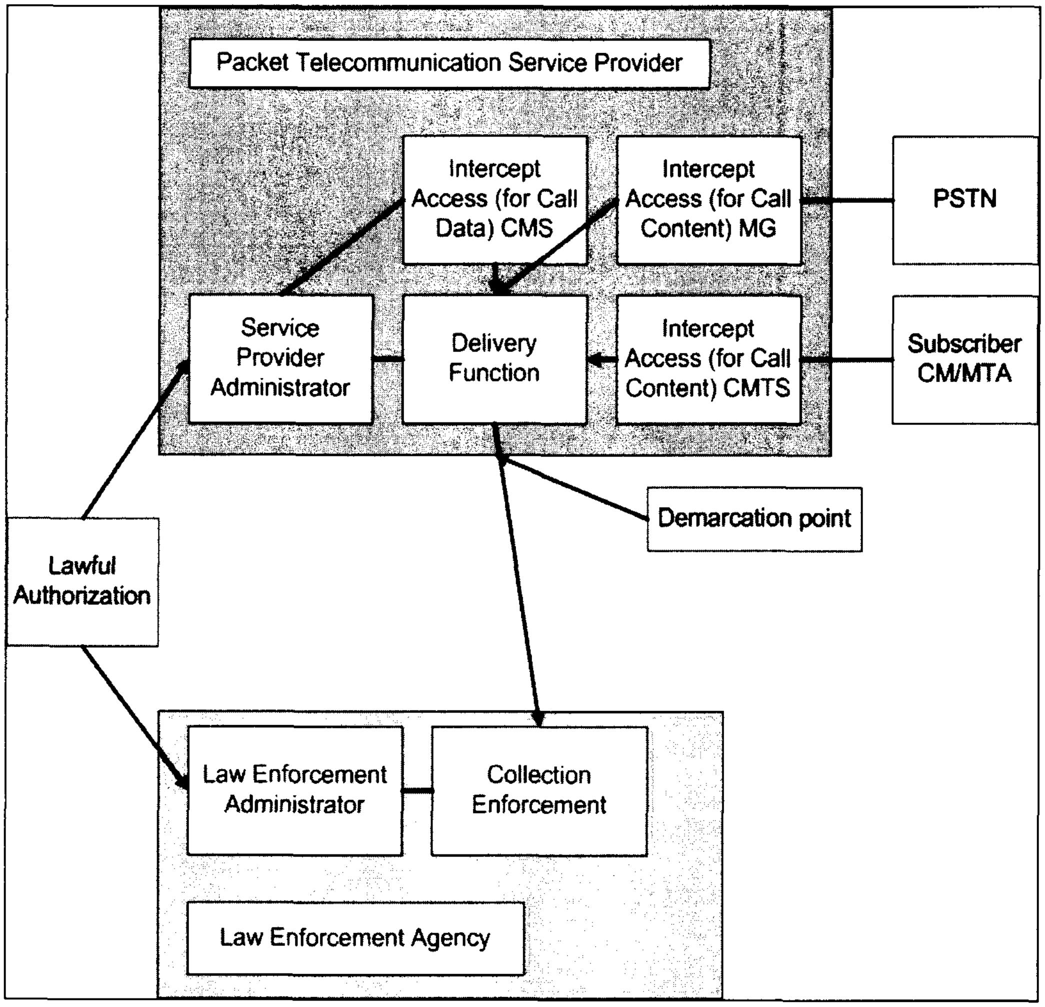

Packet Telecommunication Service Provider
Intercept Access (for Call Data) CMS
Intercept Access (for Call Content) MG
PSTN
Service Provider Administrator
Delivery Function
Intercept Access (for Call Content) CMTS
Subscriber CM/MTA
Demarcation point
Lawful Authorization
Law Enforcement Administrator
Collection Enforcement
Law Enforcement Agency

Figure 2: PacketCable Surveillance Model (Adapted from [3])

The call data can be separated into two broad categories: Intercept Related Information (IRI) {Europe} or Call Data (CD) {U.S.A.} and the Contents of Communications (CC). IRI/CD includes specific signaling information about the calling parties, such as the destination of a call (the called party), the source of a call (the caller), the time of the call,

call duration, etc. The CC includes the actual content of the communication, such as the message, video, voice, or other contents.

Figure 3 illustrates the distinct separation between the Public Telecommunication Network (PTN) and the networks which are used for the processing and distribution of the intercepted information. Generally, there are three basic elements in this architectural model [3]:

- An Internal Intercept Function (IIF) which is located in the PSTN operator's network nodes is responsible for collecting the targeted data – both the Intercept Related Information (IRI) and the Contents of Communication (CC) according to the specific LI request [3].
- The Administration Function (ADMF) is located inside the PTN and communicates with the IIFs and Mediation Function through an Internal Network Interface (INI). The Administrative Function (ADMF) is responsible for managing the orders that specify interceptions [3]. The ADMF is accessed through a web based graphical user interface (GUI) that is only accessible to authorized users. ADMF organizes all the tasks necessary for the interception. For each instance of an intercept order, a Warrant ID and Case ID are assigned by the LEA. For each of these intercept orders a starting and ending date is specified – this defines the exact duration of the interception. The intercept order also specifies the kind of the intercepted data that is to be collected (IRI, CC, or both).
- A Mediation Function (MF) is located inside the PTN which communicates with IIFs using INIs and the Handover Interfaces (HI2 and HI3) to communicate with the Law Enforcement Monitoring Facility (LEMF). Before transmitting data of these interfaces, the intercepted data (IRI and/or CC data) – which comes from the IIFs – are formatted properly. After validating that this data is to be provided to a specific LEMF, based upon the ADMF target details, the specified data is sent to the specified LEMF through HI2 (IRI) and/or HI3 (CC) [3].

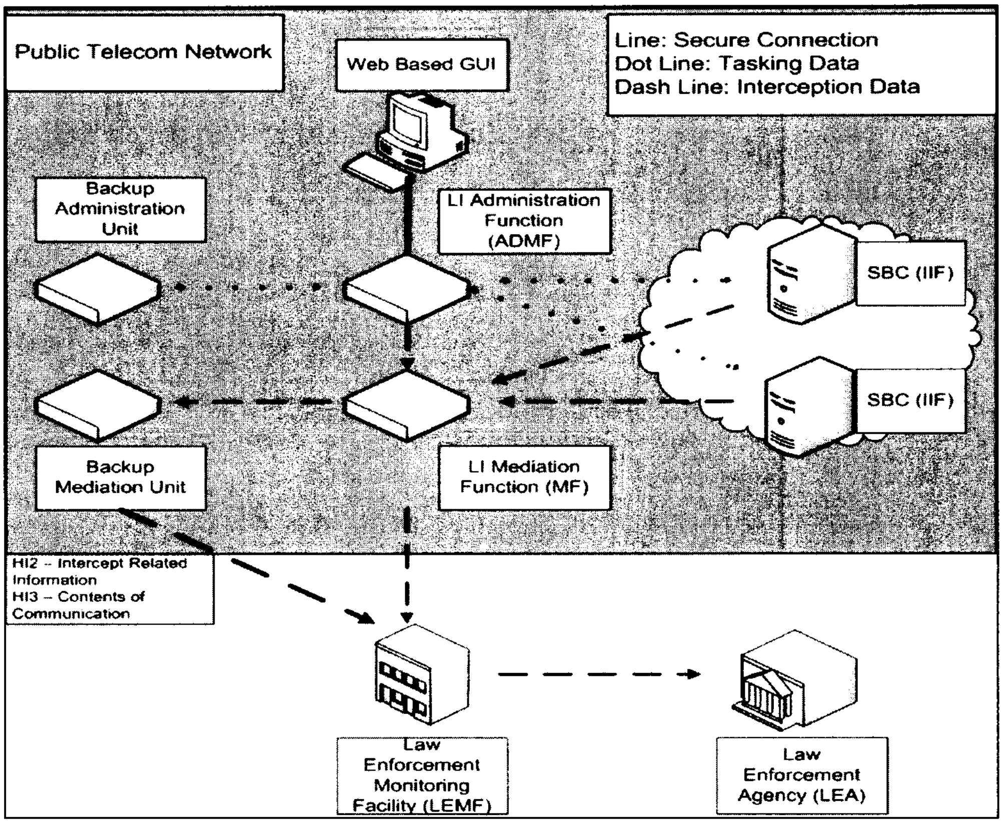

Public Telecom Network
Web Based GUI
Line: Secure Connection
Dot Line: Tasking Data
Dash Line: Interception Data
Backup Administration Unit
LI Administration Function (ADMF)
SBC (IIF)
SBC (IIF)
Backup Mediation Unit
LI Mediation Function (MF)
HI2 – Intercept Related Information
HI3 – Contents of Communication
Law Enforcement Monitoring Facility (LEMF)
Law Enforcement Agency (LEA)

Figure 3: Basic Elements in LI (Adapted from [3])

2.3 Laws

A majority of the countries around the world have enacted laws that enable government agencies (including their intelligence services) to monitor telecommunications networks. This legislation attempts to protect the private lives of citizens against possible abuse of power, based upon unwarranted interception. The pioneer among the countries that established a legal framework for lawful interception was U.S.A. Other countries have imitated the United States in this field, but there are some important differences in the details of LI according to each country's perception of their own needs.

2.3.1 United States of America

As U.S.A. faced the problem of LI very early, their government passed a wiretapping law under Title III of the Omnibus Safe Streets and Crime Act of 1968 [19]. This law defined the wiretapping procedures for criminal investigations. Later when "national security" was viewed as being at stake, another federal law was enacted to allow the lawful electronic monitoring of communications regarded as "foreign intelligence information" [4]. This legislation specified how these intercepts were to be conducted within territory that was controlled by the United States. This law is widely known as the Foreign Intelligence Surveillance Act (FISA) [4] and it permitted surveillance with warrants in three basic cases [4]:

- Any person in the United States that communicates through wire
- A U.S. person [1] in the United States that communicates through wire or radio
- Anyone inside the U.S.A. that communicates through radio with people - all of whom are in the United States

However, FISA included an important clear exception: There was no need for a warrant to intercept radio communications between people outside of and people inside the U.S.A. *unless the intelligence services were monitored a specific U.S. person that was inside the United States*. Although this was initially considered a temporary exception, there has been no amendment of this point of the law; hence this type of warrantless interception exception continues to exist. In February 2008, the U.S. Congress tried to pass a bill that would amend the FISA law [15], by granting new authorities for conducting electronic surveillance against foreign people. But the promised retroactive immunity for the telecommunication companies that helped the national agencies to perform such intercepts is still an open issue, as the House of the Representatives passed the bill *without* this retroactive immunity.

The increasing use of fiber optics has changed how international communications are performed; specifically the percentage of communications that is carried by radio communications links has decreased very significantly. As a direct consequence, the warrantless interception exception that existed under FISA became less applicable. There was a major need for an update to FISA; in response to this demand, the U.S. Congress enacted the Communications Assistance for Law Enforcement Act (CALEA) in 1994. The main intention of this law was to require "the telecommunications carriers ensure that their equipment, facilities, or services provided the necessary capabilities" [1] in order to assist the government in its electronic surveillance. Therefore, every telephone company in the U.S.A. had to create the necessary infrastructure that would allow the law enforcement agencies to monitor a phone call as transmitted over its network, and also make available Call Detail Records (CDR). In addition, the law requires that telephone companies provide a secure method of telephone surveillance that is not traceable by the target person. Finally, the data intercepted by a CALEA device is to be delivered to the premises of the LEA simultaneously with its capture.

After the terrorist attacks in the City of New York on the 11th of September 2001, the U.S. Congress enacted another law that enhanced both CALEA and FISA. This law is known as the USA Patriot Act. The main goal of this law is to extend the interception to include the publicly available broadband networks and VoIP services. Moreover, there was "no requirement of any warrant (in any medium) for communications of U.S. persons located in the United States with persons 'reasonably believed to be located outside the United States' " [5]. However, since modern telecommunication technology (e.g., Internet, mobile phones, VoIP, etc.) often supports mobility, it is not very easy to

[1] *U.S. citizens, permanent residents, and U.S. corporations*

determine the real location of a targeted person. So, surveillance may include traffic of people that are **not** supposed to be monitored -- as the intelligence services can simply claim that they did know the location of the parties. Additionally, several amendments to U.S. legislation have been enacted in order to broaden the powers of government surveillance to include more people (i.e. inclusion of financial transactions, particularly those involving foreign individuals and entities; broadening the definition of the terrorism to include "domestic terrorism" [8]).

2.3.2 Europe

The European Union (E.U.) issued a Directive (95/46/EC [9]) that defines the Lawful Interception of Telecommunications with the simultaneously protection of individuals. In general the directive defines the nature of the intercepted data and gives additional details on how the data may be used. Although many countries inside the E.U. were not pleased with this directive, all of the member countries finally accepted it as amended in Directive 2002/58/EC [10]. This acceptance occurred due to political pressure following the increase in terrorist attacks all over the world. Although Europeans are supposed to be more sensitive concerning privacy, their laws concerning data retention can be characterized as even more strict than those in the U.S.A. Finally, Directive (2006/24/EC [11]) specified "the retention of the data that is generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks" [11].

2.3.3 Telecommunication Data Retention

One of the major parameters in electronic surveillance is data retention (or preservation). Retention refers to "the storage of telephony and Internet traffic" by companies that provide these services. This data specifically includes Call Detail Records (CDRs) (as they provide details of the incoming and the outgoing calls), sent and received emails, visited web sites of the customers of ISPs, and also the location of the customers of telecommunications companies. The preservation of such data gives governments the ability to collect, analyze, and finally monitor the life of hundreds of millions of individuals - allowing in this way mass surveillance of almost the entire population.

The European Union issued a Directive (2006/24/EC [11]) that specifies in detail the period of data preservation and also the kinds of information to be stored. The period varies from 6 months to 2 years, according to the nature of the data. The content of the CDRs can include the following [11]:

- Trace and identify the source of a communication
- Trace and identify the destination of a communication
- Date, time, and duration of a communication
- Identity of the type of communication
- Communication device
- Location of mobile communication equipment

Although all the member-countries of the E.U. must adopt this directive as a national law, countries maintain the right to postpone the application of the directive in the fields of the Internet (visited web sites, sent and received emails, and VoIP) for more than 18 months. Furthermore, each country can extend the storage period of the CDRs according to its own needs, even though the initial proposal of the committee of Civil Liberties, Justice, and Home Affairs (LIBE) was to retain them for **maximum** period of 12 months.

As a consequence of the legislation of the above directive, many organizations and also individuals declared their opposition to the retention of this kind of data - as the investigation of terrorist attacks could be solved by keeping only the legally intercepted data. Moreover, CDRs can assist the police to find people that committed crimes *only after a terrorist attacks* and **not** before. Another point of the opponents to data retention is the excessive power that the state obtains to monitor and control the lives of individuals. As has been all too frequently observed, a common practice is that CDRs will be used by the police against any group or individual who opposes the government's plans or actions. Finally, opponents highlight the time frame of the preservation of the CDRs as excessive. As the retention time can be extended up to 2 years or more, this also causes a serious economical impact upon all the companies that are required to keep all these records, as in many countries they must pay the preservation costs (an exception to this is the country of Finland, where the government pays the storage costs).

2.4 Greek tapping

As described above, the main reason for lawful interception is supposed to be the identification of terrorists and the prevention of their attacks. However, the implementation of the required software and hardware for this legal interception can also be used for illegal monitoring of people (i.e., illegal tapping); even without the knowledge of the network operators or the LEAs that such interceptions are happening. One of the most recent incidents that perfectly illustrate this situation is the illegal interceptions that took place in Greece during the Olympic Games in 2004.

In March 2005 the largest mobile company in Greece – Vodafone Greece – announced that rogue software had activated the lawful interception mechanism implemented in the telephone switches used by the company. The result was that over 100 mobile phone numbers which belonged to a number of important Greek politicians (including the prime minister of Greece) and high ranking military staff had been tapped for at least one year without any warrant from a LEA. Many have asked: How could this happen? It is clear that some "really knowledgeable people managed to infiltrate the network of Vodafone from outside or subverted it from within" [6], as the perpetrators managed to implant the illegal software in four of Vodafone's mobile switching centers. These switches are located in the heart of their mobile phone network. This software took advantage of an upgrade to the switches that took place in 2003. This upgrade to Vodafone's network was to provide the ability to monitor its customers via a remote-control equipment subsystem (RES). The RES can copy a conversation (of a wiretapped phone) to a second stream and send this copy to the LEA. The rogue software activated the RES for specific phone numbers while simultaneously erasing any tracks that might reveal its presence. The key to the illegal interception was "to use the capabilities of the RES without using the dialog-box of the interception management system (IMS) that would have made auditable logs" [6].

The uncovering of this interception happened accidentally. The intruders upgraded their software in January 2005. However, this caused several problems in the delivery of text messages to other mobile phone companies. Due to this problem, Vodafone with the help of Ericsson's specialists started an extensive search for the cause of the SMS delivery problem and they finally discovered the existence of the rogue program.

As far as the identity of the intruder, many scenarios have been suggested, but none of them offers sufficient evidence. One of the dominant theories is that a Greek company, Intracom Telecom, which had taken over the programming evolution of a part of Ericsson's AXE, was involved. Moreover, one of the hacked Vodafone exchanges was located on the campus of the main Intracom facility. Another scenario that appeared in newspapers pointed toward United States agencies, which feared terrorist attacks during and on the Olympic Games in Athens. Moreover, the U.S.A. agencies were believed to have the knowledge necessary to perform the interception. Finally, the location of the monitored phones correlated with apartments and other property under the control of the U.S. Embassy in Athens.

However, the Greek state fined Vodafone €76 million and fined Ericsson €10 million for this interception and their mishandling of the situation (e.g., not preserving evidence). Still there is no final decision on the identity of the perpetrator(s) or the reason for the monitoring.

3 LI in telephony (fixed and mobile)

Both criminal investigations and national security concerns oblige governments and their law enforcement agencies (especially in the U.S.A. and in the E.U.) to utilize voice telephone interception systems in order to collect and analyze the information that was produced by telephone calls. Such interceptions have helped police agencies in the investigation of complex criminal affairs and in the prosecution of the culprits – despite frequent accusations of misuse of the interception technology.

However, after some research concerning the credibility of the telephone interception tools – with respect to legitimate security concerns – such interception was proved to be very susceptible to a plethora of countermeasures that a subject[2] can use in order to prevent the accurate tapping of the subject's calls. These countermeasures mainly exploit "the use of in-band signals between the telephone network and the law enforcement agency" [12]. The use of these countermeasures showed that they can "obscure not only the content of a call, but also the metadata that indicates the presence of a communication and also its endpoints in a way that is sometimes difficult to be detected" [12].

A serious consequence of the above is to undermine lawful interception to an extent that not only negatively impacts the accuracy of the tapped contents, but also to "the acceptability and weight of legal evidence derived from it" [12]. These weaknesses can be alleviated with the application of some recommendations that try to reduce the susceptibility of the lawful interceptions techniques to attacks. These recommendations are detailed in section 3.2.3.

3.1 How does LI work in a fixed telephony setting?

In the U.S.A. there are two federal laws that regulate how telephone wiretapping can be conducted; the Federal Wiretap Act (Title III) and the Foreign Intelligence Surveillance Act (FISA). These two laws specify three categories of wiretaps that law enforcement agencies can use.

The first category is called a pen register or dialed number recorder (DNR) [12] which is an electronic device that can record all the digits dialed from a particular telephone line and also other outgoing signaling information. A pen register tap is only allowed to provide traffic analysis of the targeted line and not the audio contents of calls. In order to be allowed to use this interception technique, a judicial authorization is needed; which is not very hard to acquire – basically the requirement is a suspicion of an illegal activity.

The second category is the "trap and trace device" [17] which is an electronic device that is used in order to show all the incoming calls for a specific targeted telephone number. This device is generally used in concert with a pen register (as the pen register deals with the outgoing calls of a targeted telephone number).

The third category is known as full audio interception. From the name it is clear that this intercept records not only the signaling and the dialed numbers, but also the actual audio (i.e., the call contents). Due to the addition of the audio the authorization for this

[2] "Subject" is a term for the person who is target of the LI

kind of interception is more judicially difficult than obtaining a pen register or trap trace authorization. Moreover, the expenses of a full audio interception are high, as it requires "continuous real-time monitoring" [12] by the law enforcement agency.

Apart from the above three categories of interception, law enforcement agencies are casually using telephone records (i.e. CDRs) as a source of information about subjects. The main disadvantages of the telephone records are that they (1) concern a "subject's past telephone activity" [12] instead of current or potential future activity and (2) they are not practically available to the law enforcement agency until sometime *after* the activity has occurred [12].

3.1.1 Wiretapping methods

As far as the above three categories of telephone intercepts (often referred to as *wiretaps*) are concerned, the same technological equipment can be used in order to implement them (in a pen register intercept the copying of the audio can be disabled). There are two widely known methods that can be used for wiretapping: the loop-extender and the CALEA taps.

A loop-extender (shown in Figure 4) is the oldest form of wiretapping technology. It is used exclusively for wire line (POTS) telephone lines. The main feature of this method is the use of a second line (called a "friendly line") that connects the subject's telephone line (called a "target line") directly with the law enforcement agency's premises. The friendly line can either be a dedicated leased line or a regular dial-up line that can be placed on the subject's premises or in the telephone switching center. In order to implement this tapping no special hardware is needed; where the loops are jointed, a small device – called a loop extender – is located in order to "ensure proper isolation and level equalization of the intercepted content" [12]. Note that loop extender is also used for some normal telephony local looks to increase the distance that the subscriber can be from the local exchange. The loop extender captures all the audio (and signaling) on the target's line and sends it via the friendly line to the premises of the law enforcement agency. At the end of this loop, the pen register equipment which is located in the law enforcement agency building decodes the dialed digits and the call activity signals. Moreover if authorized the equipment can also record the call contents. Note that when using a loop extended the telephony operator has no control over what information the law enforcement agency records for an outgoing call, since the LEA receives all of the signaling and call contents.

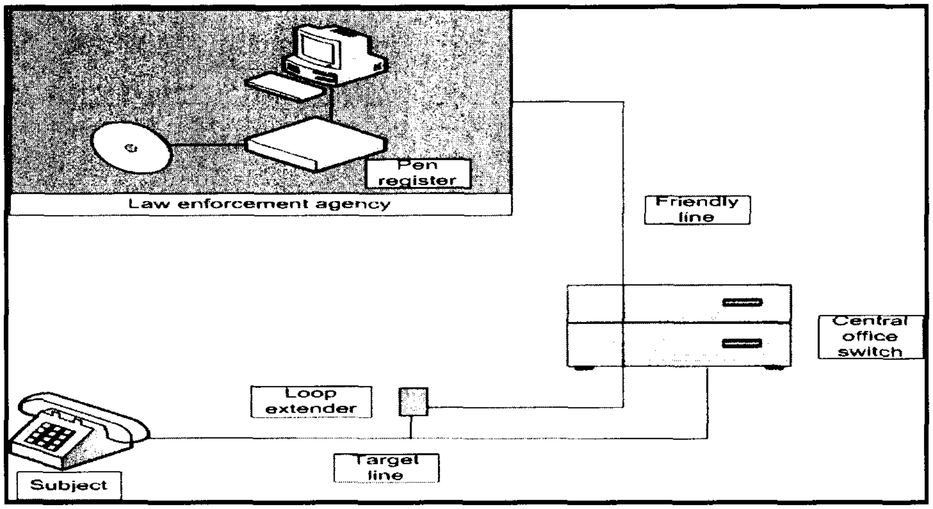


Figure 4: Loop-extender architecture (Adapted from [12]

Apart from the loop extender there is also a newer wiretap method – known as CALEA taps (see Figure 5) – which were designed to comply with CALEA requirements. The CALEA standards specify the existence of a standard interface between the law enforcement agencies and the telephone network providers (both wire line and cellular telephone companies). The main difference between CALEA taps and the loop extender is that the decoding of the signaling information is now performed by the telephone company, rather than the law enforcement agency. Instead, the law enforcement agency is connected to the telephone company through a standard interface (known as J-STD-025A [14] or the newer version J-STD-025B [15] which is used mainly in America). Another difference from the loop extender is that the J-STD-025A standard uses two categories of separate telephone lines: one for the signaling information (dialed digits, on-hook status, call times, line status, etc.) and the other for the call audio. The line that transmits the signaling information is known as a CDC (Call data channel) and is linked with all the telephone lines that the law enforcement agency is monitored. The lines of the second category are known as a CCC (Call content channel); this line transmits the voice content of all the active monitored lines. The CDC can carry information for more than one active interception at a time. In contrast, a particular CCC line can carry the audio information from only one tap at a time, but it can be time multiplexed to carry the call contents from different subjects at different times by dynamically assigning the line for the active targeted lines during a call.

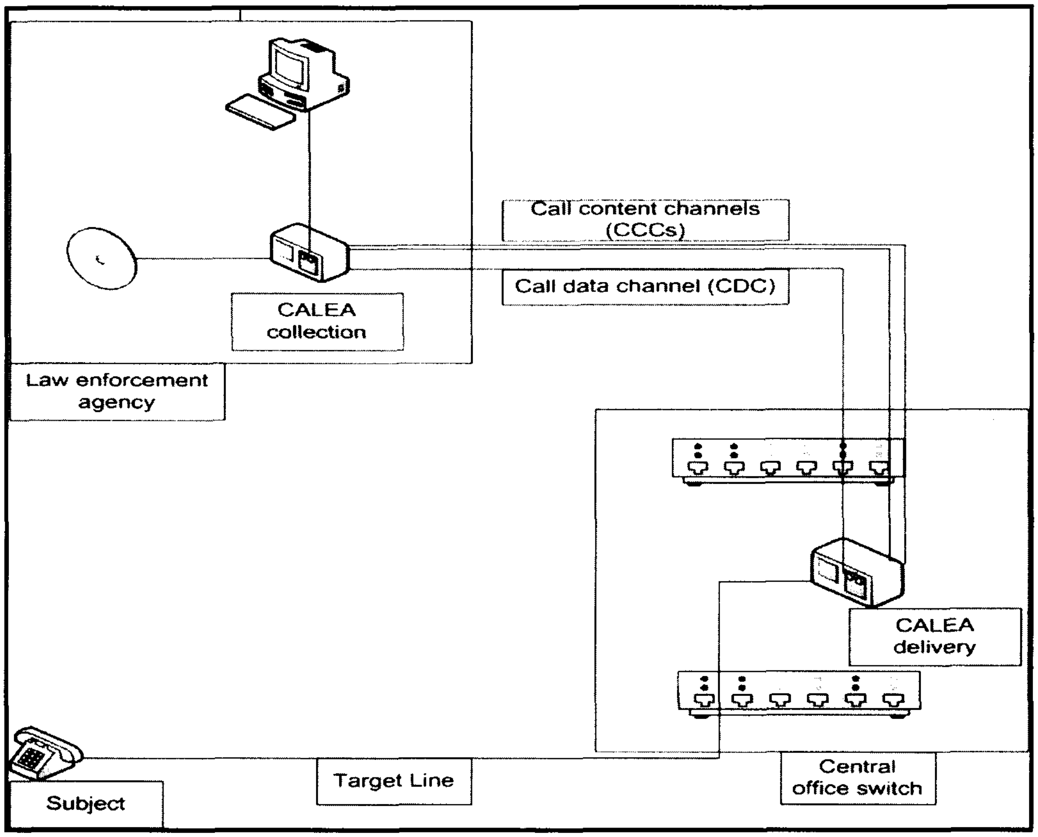


Figure 5: CALEA wiretap architecture (Adapted from [12])

3.2 Vulnerabilities in Wiretapping Systems

Even though there is little information (i.e., only limited public available) about the susceptibility of the wiretapping systems, an extensive survey by Sherr, et al. [12], a research team at the University of Pennsylvania, showed that there are a lot of threats that can negatively affect the accurate capturing of telecommunications data.

Apparently, the most prominent threat against a telecommunication tap is the detection of it. If the advantage of the secrecy is lost, then the whole wiretapping procedure is likely to be unproductive or counter-productive. Detection can be performed in many ways. First, if the tapping uses a loop-extender device which is placed near the subject's premises it can easily be detected by physical inspection. Moreover, it is known that taps that change the target's line transmission characteristics and this can sometimes be detected with "electronically means like sensitive loss measurements or time-domain reflectometry" [12]. Another threat is "the penetration of a telephone company's information systems by a computer compromise or physical burglar" [12]. While J-STD-025A specifies that taps should be performed in an undetectable way from the subject's point of view, it does **not** describe how to achieve this.

The most severe threat that a subject can unleash is the encryption of the voice and signaling, as this could lead to content and/or signaling obfuscation. The use of cryptographic techniques is often utilized to provide security between the communicating parties. However, as of today, voice encryption is not widely used by subjects [12] and digital voice systems for encryption of "analog telephones systems are not yet widely available in the market [12]. The major disadvantage of encryption is although it may protect the contents of a call, it generally does not protect the signaling information. However, by forwarding all call through an anonymizing third party, even the call signaling information can be moved to the call contents and hence also be encrypted.

Another public available countermeasure that can affect the CCCs (Call content channels) in CALEA taps is a denial of service attack against CALEA CCCs [12]. This countermeasure exploits the dynamic assignment of CCCs as "the number of different voice channels associated with a monitored line is potentially unbounded if the subject subscribes to a call-forwarding service" [12]. If the subject and their correspondents forward their calls elsewhere, there will be no CCCs available for the monitoring of important calls as every additional call needs a new CCC. It is not clear if the J-STD-025A standard specifies any defense against this countermeasure, as the published literature says little about this type of attack.

Finally, evasion and confusion are two additional countermeasures that a subject can use in order to avoid interception. Evasion means that the subject can prevent legitimate data from reaching the monitoring system. Confusion means that the subject sends additional false data along with the original data to the monitoring system. The result of either of these countermeasures is a serious degradation of the intercepted data's credibility. In order to avoid evasion or confusion there are some defenses that can be used (however, these lead to the eavesdropper's dilemma[3]) as by using one defense to avoid evasion the eavesdropping system is more susceptible to confusion and the reverse.

3.2.1 Countermeasures against loop-extender taps

As in-band [4] signaling is used mainly in the loop extender taps, it leads to vulnerabilities that make loop extender tapping very susceptible to attacks. Mainly, there are three kinds of countermeasures that a subject can utilize in order to avoid tapping by the law enforcement agencies: Dialed digit spoofing, incoming calling-number ID spoofing, and line status spoofing and recording suppression.

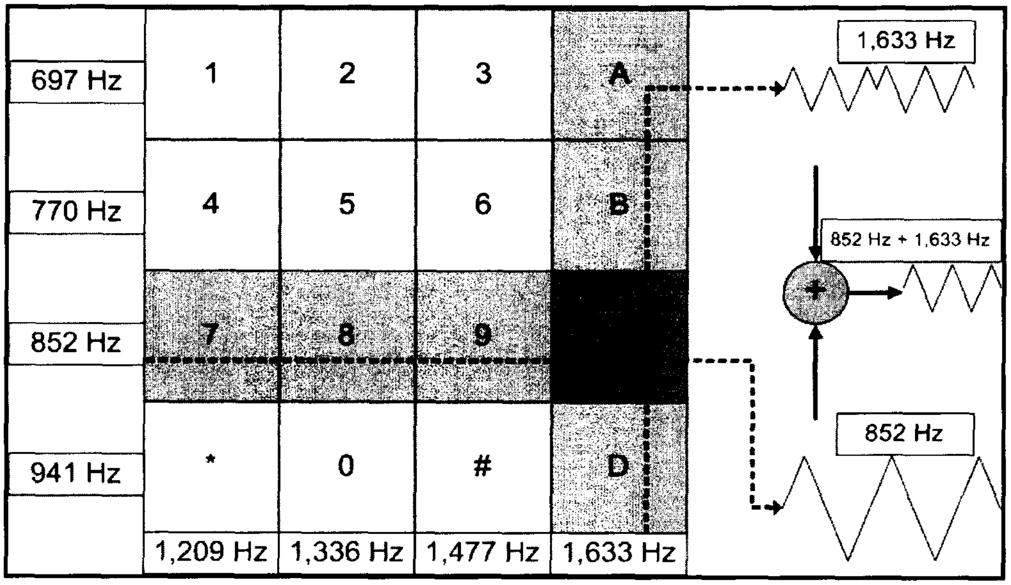
3.2.1.1 Dialed digit spoofing

Using this countermeasure the subject can mask the dialed numbers of an outgoing calling by exploiting the weakness of the way that tapping devices decode dialed numbers and audio signals. As the transmission (from the phone device to the call switching center) of a dialed phone number is done in analog form, the use of audio dual-tone multi frequency (DTMF) signals is obligatory.

[3] The eavesdropper's dilemma (See Appendix A) appears whenever the law enforcement agency lacks knowledge of how the network and receiver process traffic or if it destroys information processed at low layers of the protocol stack

[4] In band signaling is the exchange of signaling (call control) information within the same channel that the telephone call itself is using [13]

DTMF digit signals are the outcome of two audio frequency tones: "the 'low' tone" [12] which represents the horizontal row of the keypad of a telephone device and "the 'high' tone" [12] which represents the vertical column of the keypad. These two tones signals are combined when a telephone user presses a key on a phone device in order to generate a tone that will specify to the call switching center the pressed key. The DTMF standard specifies the existence of the numbers (0-9), characters (* and #), and a column with the letters (A, B, C, and D) on the keypad.



697 Hz	1	2	3	A
770 Hz	4	5	6	B
852 Hz	7	8	9	
941 Hz	*	0	#	D
	1,209 Hz	1,336 Hz	1,477 Hz	1,633 Hz

Figure 6: Dual-tone multi-frequency (DTMF) keypad and waveforms of generated tone
(Adapted from [12])

Even though in the majority of cases the generated tone signals are accepted by the DTMF decoders, there are times that a generated tone signal that is on the edge of the standard can be rejected by some DTMF (but not all) decoders as invalid. The parameters that specify if a generated tone is accepted or not by a DTMF decoder are: the precise frequency of the 'low' and the 'high' tones, their amplitude, the signal duration, waveform distortion, external noise, etc.

According to the experiments conducted by Sherr, et al. [12] analog telephone subscribers can discover the threshold of their switch's DTMF decoders, then later uses this knowledge to create signals that will be treated differently by other decoders. In a tap system that uses a loop extender device there are two different DTMF decoders, one at the telephone company's switch and the other at the law enforcement agency. Every dialed digit from the subject's line is processed independently by the two separate DTMF decoders. As a result a dialed digit may be accepted as valid by the telephone company's switch decoder and not the wire tapper or the opposite.

Sherr, et al.[12] showed that after discovering the threshold characteristics of a telephone switch's DTMF decoder with the help of a laptop, the subject can construct bogus digit encodings in order to be rejected as invalid by the switch's decoder. Despite these encodings being rejected it is very possible that they will be accepted by the law enforcement agency's decoder. The bogus signals are used to confuse the monitoring system. On the other hand, "non-standard digit encodings" [12] can be created that will be accepted by the telephone switch's DTMF decoder, but will be ignored by the law enforcement agency's tap. These signals attempt to evade such a tap.

From the above it can be seen that a wiretap can be either liberal or conservative. If a wiretap is liberal, it will accept signals that will be ignored by the switch, thus achieving its goal of confusing the tapping agency. If the wiretap is conservative, the digit signals will only be accepted by the switch and these digits will evade interception.

The effectiveness of this confusion and evasion is highly likely in every wiretapping system that uses its own DTMF decoder and interprets the dialed digits on its own. Even though a subject cannot be sure of how liberal or conservative a law enforcement agency's DTMF decoder is; the subject can unleash both of the threats in concert in a whole digit sequence. This means that "the subject sends n random noise digits" [12] that are dialed among the k 'real' digits in a random sequence. The 'real' numbers are sent using evasion and the noise numbers using confusion. With the above combined method, the real dialed number can be masked from the tapping. An important point is that the recording of **false** data will compromise the ability of a law enforcement agency to present this data as evidence during a trial.

3.2.1.2 Incoming calling-number ID spoofing

One of the extra options that a subscriber has is to screen the calling-number ID (CNID) when he or she receives a call via his or her phone device. Between the first and the second ring, with the help of in-band signaling, the calling-number and sometimes the related name are transmitted and can be presented on the screen of the phone or a special phone device belonging to the subscriber. When a subject has activated the CNID service it is clear that the law enforcement agency can also monitor this information.

However, if the subject uses some countermeasures lawful interception can lose valuable information. Sherr, et al. [12] showed experimentally that with the use of forged signals the subject can confuse the capturing of the real CNID. However, evasion cannot easily be performed as the central office (CO) is responsible for the transmission of the CNID. During their survey the researchers periodically replayed a counterfeit CNID – with the help of a sound card – whenever the subject's line was on-hook. The result was successful deception of all the tested DNR devices. Another countermeasure is to generate counter-signaling when the CNID is being set – since with suitable signal processing the signal can be received at the subject device, but corrupted for the loop-extender tap(s). Technically this has to do with the need for a given signal to noise ratio to properly receive the data, the likely longer path to the LEA decoder, and the three wire analog telephone circuit.

3.2.1.3 Line status spoofing and recording suppression

The main disadvantage of the loop extender taps is the use of the in-band signaling by the telephone, the central exchange, and spoofing devices used by the subject. Due to this, a subject can remotely unleash an 'attack' by spoofing the on-hook signal which is generated from the loop extender with a result of disabling the audio monitoring equipment.

It is known that in loop extender systems, the signaling data and the audio are transmitted to the law enforcement agency over the same channel – the friendly line – in the "analog voice-band domain" [12]. This is the characteristic that makes the loop extender susceptible to exploitation from the subject; but it is also the feature that makes such a loop-extender inexpensive and low complexity.

A monitoring system gathers many call-processing signals from the subject's line. These signals can be separated into two categories. In the first category, the signals (DTMF encoded dialed digits, CNIDs, dial tones, and ringing signal) are encoded in "the voice-band audio domain" [12]. So, these signals are simply passed to the friendly line through the loop extender and can be deciphered at the law enforcement agency. However, the second category of signals (including on/off-hook state and incoming-call ringing signals) are not encoded in the voice-band audio domain. Even so, the loop extender device can detect these signals on the subject's line, but cannot relay them in the same form over the friendly line (to be processed remotely by the law enforcement agency). To solve this problem these signals are encoded as "special audio tones superimposed on the friendly line audio" [12], in order to be recognized and decoded later by the law enforcement agency.

A signal that is very vital and is **not** included in the voice-band audio domain is the on/off-hook status. The on-hook status means that a line is idle, i.e., – no audio or other signals are transmitted at the moment. In order for the law enforcement agency to recognize that the subject's line status is on-hook, an idle tone is transmitted continuously on the friendly line. If there is a transmission of some signals over the target's line, then the idle tone is automatically removed from the friendly line. The representation of the idle tone is done using the DTMF C digit that produces a two-frequency audio signal (852Hz+1,633Hz). According to the survey [12] all the loop extenders in the market use the C tone to indicate that the subject's line is on-hook. As the on/off-hook status signal is sent through the same line, it is easy for the subject to send an "identical-sounding signal" [12] during a call in order to spoof the law enforcement agency's on-hook detector, thus avoid the call being recorded.

According to Sherr, et al. [12], some loop extenders devices have unexpected behaviors and can perform unexpectedly if a DTMF C idle signal is not followed by new call setup signals. If this happens, then the friendly line will be disconnected and will again try to reconnect. The reestablishing of the connection will take at least 30 seconds. During these 30 seconds no recording of audio can be performed. So, if every 30 seconds the subject sends a DTMF C signal, then no audio can be monitored by the LEA wiretap hardware!

Moreover, the use of the DTMF C idle tone can negatively affect full audio wiretaps. As loop extenders do not record audio when a DTMF C tone-pair is transmitted, it is easy for the subject to continuously send a low volume DTMF C tone-pair during a call in order to spoof the loop extender and avoid the recording of the call. While it might be assumed that only low quality call service can be established if a DTMF C tone-pair is transmitted continuously, however, this can be avoided if the DTMF C tone-pair is not sent at high amplitude. Sherr, et al. [12] showed that the loop extenders could be deceived and would stop recording even when the transmission of a low volume DTMF C tone-pair was present, yet this allowed an acceptable and comfortable conversation to be conducted. Additionally, using signal processing the DTMF C tone-pair could simply be recognized and subtracted from the received signal – as long as it has roughly constant amplitude and the sum of the amplitudes of the actual signal in the pass band for these two tones is within the range of the receiver.

The above countermeasure can be prevented only by filtering the DTMF C tone-pair signal from the point of the loop extender, in order to send the correct information over the friendly line. However, according to Sherr, et al. [12] no loop extenders in the market can perform such filtering.

3.2.2 Signaling countermeasures against CALEA taps

As the loop extender taps face serious problems with the credibility of the wiretapping due to the in-band signaling, the J-STD-025A standard tried to avoid this problem by separating the channels that deliver the subject's signaling (CDC and CCC) with a simultaneous decoding of the DTMF tones at the telephone company's switch instead of by a device at the law enforcement agency. The main idea was that by using a separate channel for the signaling (out-of-band), line status spoofing could be prevented. Moreover, as the DTMF decoding is now done in the telephone company switch's call processing system, it is more probable that the "reported digits" [12] to the law enforcement agency are more accurate than those that would be produced by the loop extender device and that these reported digits correspond to those used by the switching center.

Although CALEA taps are considered more robust than the loop extender taps, CALEA's taps face similar credibility threats. The J-STD-025A standard specified "only a standard interface between the telephone company and the law enforcement" [12]; the problem is that it did not specify any particular implementation of this interface. So, even though the telephone company's switches are supposed to report the real digits that were produced by the call processing system, there is no guarantee that they actually do. As a consequence, the law enforcement agency may gather false calling-numbers. Furthermore, Sherr, et al. [12] showed that 'post-cut-through' digits (for example, extra digits that could be used with a direct inward dialing exchange to reach a specific extension of the destination PBX) which are transmitted through the CDC can still be confused or evaded as they are processed by a "remote endpoint" [12] and not by the switch. Finally, in CALEA taps there is still the countermeasure of recording suppression that results in the evasion of call-conversation recording.

In some CALEA implementations the DTMF C tone-pair signal is used in order to declare that the CCC channel is idle. In many CALEA CCC systems this DTMF C tone-pair signal will disable recording. The continuing use of the DTMF C tone-pair signal may be motivated in order to achieve backward compatibility with the loop extender systems. Moreover, the U.S. Federal Bureau of Investigation (FBI) and the U. S. Department of Justice requested the use of a continuity tone (not necessarily the DTMF C tone-pair signal) in order to know when a CCC channel is idle or not. However, "the majority of the CALEA vendors" [12] are using the DTMF C tone-pair as an optional feature for the declaration of an idle CCC channel.

The result of the use of the DTMF C tone-pair signal is the same as in the loop extender taps. The subject can transmit a continuous DTMF C tone-pair at a volume that will discontinue monitoring, while allowing a good quality of call-conversation. As the same tone-pair signal is also used in the loop extender taps, the subject does not have to worry if the agency is using CALEA or loop extender methods for the recoding, as the countermeasure evades recording using both alternatives.

3.2.3 Suggestions for reducing vulnerabilities

The lack of diverse monitoring systems and the convenience of finding equivalent equipment in the market (by a simple search on the Internet) leads to a quite easy avoidance of lawful interception. In order to make the tapping systems more robust some improvements must be in order to alleviate the architectural and hardware vulnerabilities that make an interception susceptible.

As far as the analog loop extender interception systems are concerned there are not many improvements to be made due to the devices' inherent design limitations. The main disadvantage of loop extenders is the use of the in-band signaling which can easily be compromised by several different types of attacks.

On the other hand, CALEA systems can more easily be made less susceptible to some interception countermeasures. As one of the most serious problems is the use of the DTMF C tone-pair in order to specify the start or stop of recording, the CCC channel of the law enforcement equipment must be configured properly in order not to be shut off when a DTMF C tone-pair is present. Sherr, et al. [12] suggest the use of the CDC channel, instead of the CCC in order to determine when the recording will stop or start.

Moreover, all lawful wiretaps should be checked by investigators in order to check for signs of signaling countermeasures. This should be performed for both CALEA and loop extenders interceptions. Specifically, the CDRs of the telephone companies should be compared with the records of the dialed numbers and the call times that the law enforcement agency gathered from their monitoring in order to reveal recording discrepancies. Of course obtaining this data from the telephone operator will mean that either more people inside the operator's network will now be aware of who is the subject of a tap or that an automatic means must be made available for LEA to access the CDRs – without easily being detected.

Finally, all the interception standards (including the J-STD-025A) should be tested against a broad threat model designed to reveal all the weaknesses of these wiretapping models. If a weakness is detected, then the architecture of the monitoring systems should be redesigned by taking into consideration the possible countermeasures that a subject can unleash in order to avoid them. However, the introduction of a new standard will take a long time, which means the persistence of these vulnerabilities for some time.

4 LI in VoIP

With the prevalence of broadband Internet connections (generally fast Internet), another means of communication was added to the plethora of the means that people can use in order to make voice calls to each other. This technology, which has recently become popular, is widely known as Voice over IP (VoIP) and uses the Internet or other packet data network in order to establish a call to another workstation/PC/PDA/... that has the same software installed or via a gateway to mobile or fixed line phones.

Many people including specialists believe that sooner or later VoIP will replace fixed line telephony, as it has significant advantages compared with traditional telephony. Even though VoIP has not replaced telephony yet, millions of people use VoIP for their everyday calls, thus reducing their use of traditional telephony.

However, the spread of the VoIP technology caused serious headaches with regard to making lawful intercepts. The reason is that it is not easy to detect and record a VoIP call to/from a target because the Internet operates in a very different manner than fixed or mobile telephony. In the following sections, a description of the nature of VoIP is given; along with an explanation of why VoIP interception is problematic.

4.1 How VoIP works

VoIP can be characterized as a revolutionary technology as it can (and likely will) transform the global phone system. VoIP uses the Internet, which is an existing and widely available network, in order to make calls via a standard Internet connection.

VoIP transforms the analog audio signals into digital data, packetizes this data, and transmits it over the Internet. Today, there are three different ways for individuals to utilize VoIP:

- An analog telephone adapter (ATA) is a device that allows a user to connect a standard phone to his/her computer or router and make a call. The ATA performs the necessary analog-to-digital and digital-to-analog conversion of the signals, performs the signaling necessary to set up a call or to receive one, and provides power to the telephone handset. These devices enable a user to quickly and easily connect their existing telephones to the device and connect it to the Internet.
- IP phones are specialized digital phones that are equipped with a handset, buttons. The main difference from traditional phones is the use of a RJ-45 Ethernet connector instead of a RJ-11 telephone connector. This enables the IP phone to connect directly to an Ethernet hub, switch, or route. Versions exist that utilize IEEE 801.11b wireless local area networks (WLANs), thus the use can connect anywhere there is an IEEE 802.11 access point which will allow the user to connect to the Internet. Extensive networks of open or nearly open WLAN access points exist to facilitate this type of connectivity (see for example FON Wireless Ltd.[5]).

[5] http://www.fon.com/

- Computer-to-computer VoIP is the most widely known way of using VoIP. All that is needed is to download free or often very low-cost software, a soundcard, a microphone, speakers (or headset) and a fast Internet connection. The main advantage of this for many users is that they can call computer-to-computer without any additionally charges - no matter what the distance is. Of course the users have to have Internet connectivity, but this can be by any means (just as in the above cases).

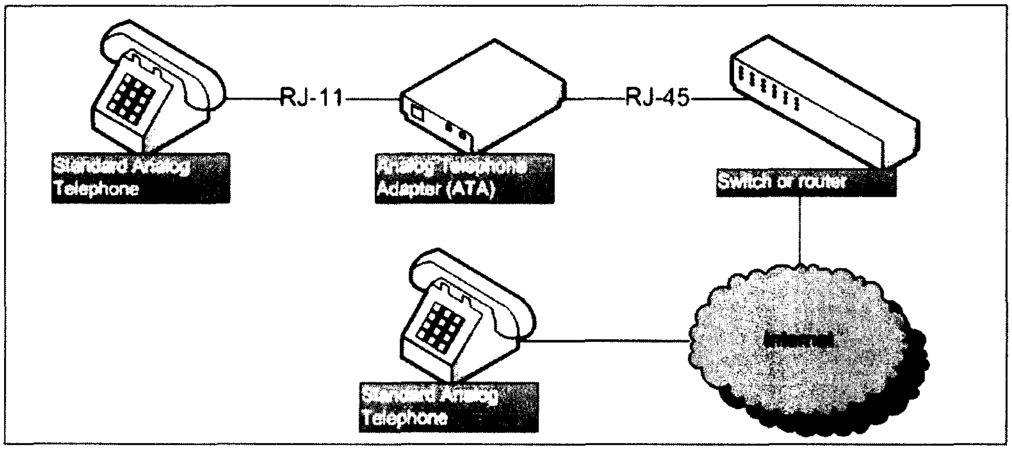

RJ-11
RJ-45
Standard Analog Telephone
Analog Telephone Adapter (ATA)
Switch or router
Standard Analog Telephone
Internet

Figure 7: VoIP service with the use of analog telephone adapter (ATA)

By using any of the above VoIP approaches, home & office users obtain two main advantages compared with the traditional phone system: low cost and increased flexibility. By having the ability to make a free (or nearly free) call to another VoIP terminal no matter how far away it is, enables VoIP users to save a lot of money. Moreover, the flexibility that VoIP gives users is almost unique - as they can call (and be called) from anywhere there is broadband connectivity. Furthermore, many extra services such as caller ID, call waiting, call transfer, repeat dial, return dial, return call, and three-way calling are provided by many vendors for free, while traditional telephone companies charge extra for these services. Finally, many advanced call-filtering options are available from many VoIP companies. Based upon the caller's ID the user can decide how he/she will accept/reject/ignore/forward to voicemail/... a call from a specific caller, at a specific time, in a specific place, ...

As VoIP operates over the Internet, it utilizes packets, in contrast with the circuit switching model which is used by the PSTN. The main difference between the two is that in the circuit-switch network there is a temporary (lasting only for the duration of the call) dedicated connection between the two parties. In a packet-switched network instead of using a dedicated line, each packet is routed over a packet network with thousands of possible paths to the final destination. While in circuit switching the connection is fixed until the parties hang up, in packet switched network a packet[6] is sent from one

[6] Packets are small chunks of data that contain the payload (a piece of clear information) and addresses (source and destination)

workstation to another via a series of switches and routers, thus the path through the network could be different for *each* packet.

The overall process of the sending data through the Internet can be summarized as [20]:

- The source-computer packetizes data, creating packets that contain a payload, source address, protocol, length, ... a **destination address** which the routers along the path utilize to decide where to forward the packet.
- The source-computer sends the packet to a nearby router, this router forwards the packet to another router that is closer to the destination-computer, and so on.
- Finally, the destination-computer may receive these packets (although the packets may have taken different network paths to this destination; some may even have been lost or duplicated) and reassembles the data in the order using sequence numbers contained in the packets (more precisely the sequence number is in the RTP header for the packets which contain the actual digitized audio samples).

The main reason why VoIP calls are cheaper than PSTN calls is that packet switching allows the digitized and encoded contents of multiple telephone calls to be carried the capacity that would be occupied by only a single call in a circuit switched network [20]. Despite the lower cost calls and the flexibility of making calls, why has VoIP not (yet) become the dominant means of making calls? One possible answer is the perception of a lack of reliability, as far as the service is concerned. The quality of a PSTN call generally very predictable; unlike a VoIP call which can vary in quality - as in the Internet, packet losses are quite common which can degrade the quality of a call. Moreover, the broadband connection can have serious delays that can negatively affect the quality of a call to such a point that it may be infeasible to for the called parties to communication via voice. However, today the quality is improving and VoIP is gaining acceptance. – thus it is likely to become **the** preferred means of voice communication for many users.

4.2 Similarities and differences in PSTN and Internet

Both PSTN and Internet are networks that people are using for their daily communication. Nevertheless, each operates in its own way, thus giving each some advantages and disadvantages.

Generally, the PSTN is considered a reliable, secure and moderately expensive network [22] for providing voice communications. One of the main characteristics of the PSTN architecture is that significant investments were made (earlier) in its infrastructure by the telephone companies, the result is a system that is "smart in the center and dumb at the edges" [22]. Moreover, due to the call establishment process and the maintenance of a connection until the parties hang up (due to its circuit switching nature), the call has a high *setup* cost.

On the other hand, because the Internet operates in a different way, the cost of transmission of small packets of data is very low (per packet). Moreover, the investments in the Internet are mainly at the edges with devices that are **computers**. As a consequence the Internet features a dumb infrastructure with routers and transmission channels (even if some of these devices are computationally powerful) connected to smart edge devices. While the Internet is considered less secure than the PSTN, it is possible to provide end-to-end security by using the appropriate protocols at various layers in the end devices.

Despite the differences between these networks and the different services they offer, there is an interaction between them that cause them to share some characteristics [22].

- Both networks use the same physical transmission medium (optical fibers, coaxial cables, and twisted pairs)
- Both networks are equipped in their central nodes with electronic routing/switching devices that direct bits through the network.
- Both networks serve large numbers of customers and operators try to provide services to these customers by efficiently utilizing their investment in equipment and transmission capacity.
- In both networks there are many companies that operate networks and these companies either provide interconnections between networks or to additional customers, hence the operators must cooperate in order to deliver the traffic that belongs to a user from network A to a user in network B.
- Today both network use digital transmission techniques.

Additionally, the PSTN and Internet differ in the principles upon which they operate [22]:

- Internet uses relatively inexpensive routers for its operation in an attempt to minimize the cost of transferring data. Most of the traffic is forwarded on a *best effort* basis, which does not provide any guarantee of data delivery. In contrast, the PSTN uses expensive switches in order to provide a reliable quality of service.
- Internet is a dumb network with smart edges. The PSTN is a smart network with dumb edges. This means that in the Internet the cost is the same no matter what type of application the user is using. Conversely, in the PSTN when new services are added there is often a high charge for using them – as the high cost of implementing the service via the network must be recovered by the operator.
- In the Internet evolution of services come from unexpected places. Anyone can create a new service and test it. On the other hand, in PSTN innovation was mainly the privilege of telephone vendors.

In conclusion, the architecture of these two networks represents the available technology of each epoch. Although digitization and fiber are bringing the two networks closer, there remain some clear differences.

4.3 SRTP in VoIP

The Secure Real-time Transport Protocol is considered the secure profile for the Real-time Transport Protocol. RTP is used to carry the digitized real-time audio (and other media) data over IP networks. SRTP was designed to provide security against the threats that RTP packets confronted. SRTP provides this by data encryption, message authentication and integrity, and replay protection of the RTP data.

As RTP packets carry audio and video data these packets are essential for providing conversational VoIP services. But the security problems that Internet bequeathed to VoIP made VoIP services vulnerable to several types of attacks (forged data, man-in-the middle attack, etc.). As a consequence SRTP was designed to fill this security gap. RFC 3711 [43] defines in detail the main objectives; the format; and the algorithms that are used for encryption, message authentication and integrity in SRTP. From analysis of this RFC and the proposal [44] & licentiate thesis [45] of Elisabetta Carrara, it is easily understood how SRTP has proved to be important for enabling secure communication over VoIP. Today a plethora of VoIP clients (i.e. minisip [50], Gizmo5 [51], Globe7[52], KPhone[53], etc.) implement SRTP in their software.

4.4 Security Problems in interception of VoIP calls

It is widely known that lawful interception is more successful in the PSTN than in the Internet. Why is this true? In fixed telephony callers use fixed phones which are always connected to the local telephone company's exchange. The switch at the local exchange **must** support wiretapping[7]. This means that the wiretapping hardware and software are quite well secured as only authorized employees have physical access to the interception system. Moreover, this interception is very effective as the switch that serves the target number directly supports wiretapping. So, even if the monitoring has to do with an incoming call that is going to be forwarded somewhere else, the interception can be done since the call first reaches the local switch (or at least the local operator) before being diverted.

What happens in the case of VoIP? Compared with traditional telephony, VoIP has two basic differences that render it problematic for interception. First of all, the target's computer is not owned by the carrier (unlike the switch - in the case of the fixed/mobile telephony). Second, a VoIP call is not associated with fixed location as is generally the case with the phone numbers in the PSTN. Even if some IP addresses that are used by computers are fixed, this is not the norm especially due to the widespread use of wireless networks, Internet cafes, and even home networks that dynamically assign computers new IP addresses every time they connect to the Internet. Dynamic IP address assignment is increasingly common compared with static IP addresses, especially with the increasing use of mobile communication devices. While the details of the dynamic IP address assignment might be recorded in a database or log file, these records are not centralized and easily accessible to law enforcement agencies. Additionally, any logs of calls (if they exist) are also distributed and not easily accessible to law enforcement agencies unlike the CDRs of calls through the PSTN[8].

[7] The requirement to support wiretapping is generally part of the regulations for lawful intercept in each country. In the case of CALEA the law stated the minimum capacity for intercepts as a function of the switch's capacity. Thus while a switch must provide facilities for LI, it may be bounded in the number of simultaneous intercepts which are possible.

[8] Note that with the increase in flat-rate calling plans for telephony, there is no business need for the operator to keep call detail records for these calls – since they do not need this information for billing purposes. Therefore, the availability of CDRs many decrease in the future – unless regulations compel operators to create and keep these records.

In addition, to the problems described above, there is also another problem that can make Internet LI more vulnerable to attacks. The current LI laws do not distinguish between the different types of electronic communications [22]. The U.S.A. is facing this problem with CALEA. There is a high risk to the security of the entire Internet as companies try to adopt a monitoring model that only has to deal with VoIP, while other ways of Internet communication may have security holes. This was the main concern of the IETF Network Working Group when they rejected taking into account wiretapping as part of IETF's standards [23]. Several attacks (man-in-the-middle, capturing of identity, and passwords) [22] can be done, because of the application of a one-dimensional wiretap law. Thus there is a need for a more thorough analysis of what is needed, what is desirable, what is feasible, what is required, ... in order to define laws & standards and to guide implementations.

As far as VoIP calls are concerned, a VoIP provider can help a law enforcement agent make an interception by guiding the target's call to a specified "point" where the tap is installed. However, even if this may work in some cases, the best way to intercept communication between Alice and Bob is to monitor the local router of one of the two persons or both of them. Unfortunately, this is not an easy task. In order to accomplish this, the routers must be under the control of an entity within the jurisdiction of a law enforcement agency. Every time an interception is needed an authenticated message must be sent to the network operators (in this case Internet service providers – ISPs) in order to start the monitoring. This causes a new problem, in the U.S.A. and in many other countries the majority of the ISPs are small companies who do not have "unlimited" resources. Unfortunately, compliance with the resource demanding wiretapping requirements may drive them out of business [22].

However, this is not the only problem that ISPs have to deal with. No matter what the size of a service provider is, VoIP introduces the problem of multiple identities. A VoIP user can very easily create multiple accounts in order to confuse a LEA that is attempting to monitor his or her traffic and/or identify him/her. Multiple identities are something very common in the Internet, but the recognition of the equivalence of these identities is not an easy task. As a consequence, a VoIP user with multiple identities cannot be easily identified by a pen register, since by changing accounts every log entry may have different caller identity information [22].

While the main problems with monitoring a VoIP call are VoIP mobility and multiple identities, there are other security issues that make VoIP interception problematic [22]:

- Physical security of the switching/routing equipment into which wiretap functions are inserted. Small ISPs may not have the expertise for securing their switching/routing equipment.[9]
- The ease of creating and using new VoIP identities on the Internet causes difficulties in identifying the *actual* target.

[9] In addition, due to use of co-location facilities the ISP may not have physical access control for this equipment. In co-location facilities many organizations share a physical site and all place equipment at this site. In some sites this equipment simply has a label on it indicating who is responsible for this piece of equipment, while in more secure co-location facilities each operator's equipment may be located in a physically secured cage within the facility. However, in nearly all such shared facilities it will be difficult to carry out operations which can not be observed by others.

- As the Internet is characterized as a dumb network with smart edges, it is easier for a target to discover that he/she is being wiretapped. In contrast the PSTN is not as vulnerable as the Internet because of the smart network and the dumb edges.
- For every interception, the surveillance must be concentrated only on the specified target. However, mobility and the multiple identities that a VoIP user can create both cause extra difficulty in isolating only the targeted VoIP communications. Intercepting untargeted subjects will cause many illegal problems.
- There is no agreement when is best to examine a packet. In a PSTN or in a mobile network telephony interception is generally based on a unique identifier, the phone number[10]. However, Internet packets do not include this kind of information. Instead of a phone number associated with a call (session) in the PSTN, each packet includes source and destination IP addresses. However, these addresses are usually not static and may change every time someone connects to the Internet [24]. As described earlier, to find the mapping between this IP address and a MAC address requires access to the DHCP logs (in the case of dynamic host configuration protocol based IP address assignment). Additionally, many network interfaces enable the user to change the MAC address which this interface uses, so this is not a guaranteed unique identifier for a device – let alone a user.
- Finally the call signaling and the call contents may be encrypted [24]]. There are two categories of VoIP companies. Those who do not encrypt their calls and those who encrypt them. Vonage is one of the most well-known VoIP companies in the first category, as it does not encrypt the packets used for setting up the calls **nor** do they perform encryption of the call contents (in fact they might never see the call contents - as they do not necessarily operate any of the networks over which these contents might be sent!). On the other hand, there are other companies that encrypt their VoIP calls (both call signaling and call contents), but due to their obligation to comply with interception laws, they are obliged to provide the decryption keys if a law enforcement agency asks them to do so. In addition to these two categories, there is a major VoIP company that constitutes an exception leading to headaches for law enforcement agencies. Skype is the world's most popular VoIP company with hundreds of millions users. Both Skype and SIP providers use peer-to-peer communication for the call contents between the callers. Thus Skype is not able to provide interception as the call traffic is not handled by it. Moreover, with strong encryption of packets [26] it is difficult to decrypt them even if the packets were captured at some point in the network. It is considered that only NSA [24] has the necessary computational power to decipher Skype's packets. However, Skype and some SIP operators might be subjected to law enforcement agency requests to (1) weaken the client which a given user uses, (2) disclose the information about the keys which a user is using (if known by

[10] Or in some cases an identifier for a specific mobile telephone.

the operator), and (3) disclose the information they do know about a given subscriber (this might include the subscriber's public key, what IP address they have logged in from, information about how the user pays for their service(s), etc.).

It is easily understood that all the above factors render lawful interception of VoIP calls both different and more difficult to perform than in traditional telephony. If a VoIP caller has a fixed location and a fixed IP address from an ISP, then monitoring the call can be performed relatively easily as it does not differ (substantially) from the existing methods of wiretapping in the PSTN. In fact, it may be much easier - since the data seen by the network and by the user's computer are the same (i.e., taking advantage of differences in thresholds for dialed number detection, etc. is much harder). However, if any of the above conditions occurs then the effectiveness of the interception can be substantially reduced.

4.5 Example of problematic VoIP interception

Suppose there are two VoIP users – Alice and Bob - who are connected to different ISPs. Moreover, both Alice and Bob have selected a VoIP service provider associated with another ISP (See Figure 8).

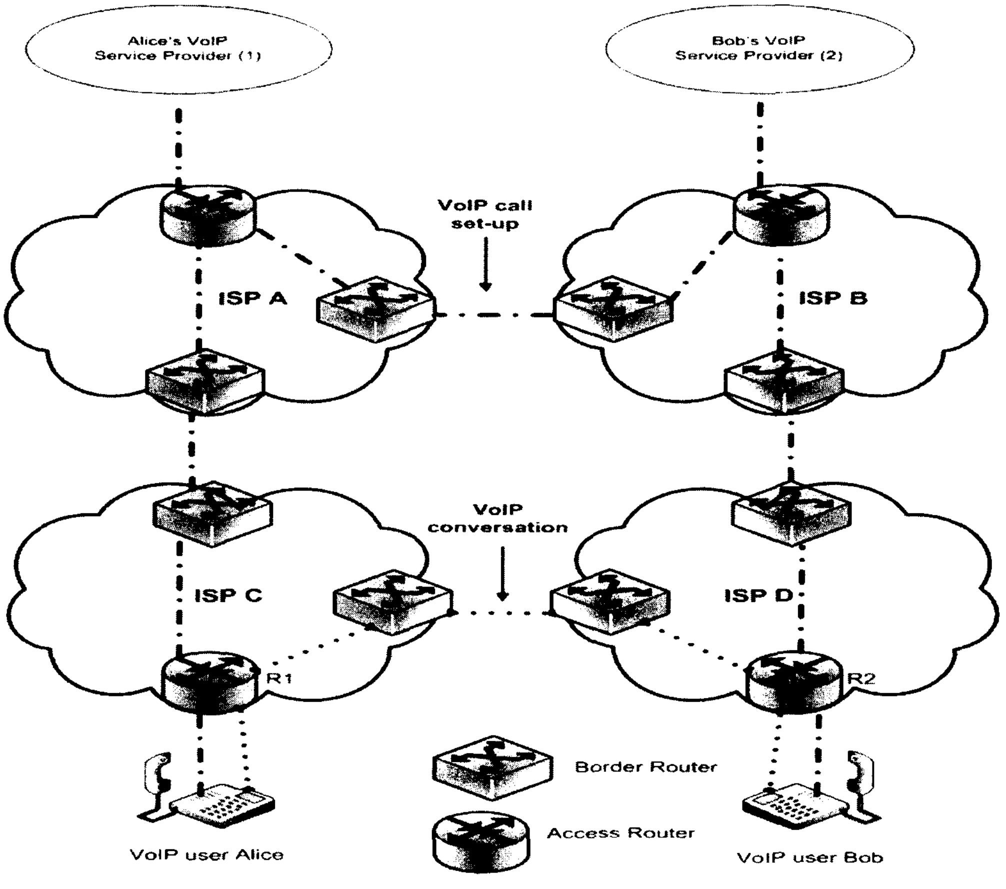


Figure 8: Problematic VoIP interception (Adapted from [22])

Suppose Alice wants to call Bob. Alice's VOIP phone uses the Internet to notify her VoIP provider which informs Bob's provider, which in turn notifies Bob's phone, thus a VoIP call can be set-up.

If an agency wants to start an interception that involves Alice, then the key routers are the access routers R1 and R2. These are the routers that are quite similar to the local exchange in the PSTN. However, routers R1 and R2 do not know the identity of the VoIP callers; hence the interception cannot start here. One of the VoIP providers must give the order to start the monitoring of its customer. Here is where the problems start. The VoIP providers can be located anywhere in the world and they are not obliged to have a "technical relationship" [22] with ISPs other than their own. Thus Alice's VoIP provider might not only have *no control over* router R1, but might not even have a business relationship with ISP C - hence ISP C would have no reason to process a request from Alice's VoIP provider to perform monitoring of Alice's call traffic.

The problem would be simpler if the VoIP provider is owned by the ISP that provides Internet connectivity to Alice (i.e. if ISP A and ISP C are the same). Even if this is feasible, it cannot be expected to be the norm. One of the best known examples is Skype which is not associated with any ISP [22]. As the VoIP provider is not associated with the ISP and the VoIP user can even move from one ISP's network to another (sometimes in the middle of a call), thus effective interception is not an easy task. Even more difficult is the case when the user does not use an external VoIP provider, but instead provide this service themselves - now it become impossible for a LEA to seek the cooperation of the VoIP provider without tipping off the user that their communication is the target of a legal intercept!

4.6 Solutions for VoIP interception

According to the above analysis, law enforcement agencies face serious problems in accomplishing effective monitoring of VoIP calls. They can easily miss a call, they might not have the ability to decrypt a conversation, and they may be unable to intercept targeted calls while avoiding intercepting non-targeted calls. However, some improvements can be made in the way a VoIP interception is performed.

4.6.1 A formal architecture for VoIP interception

One of the most significant causes for a VoIP call avoiding interception is that no IETF working group supports a standard for lawful interception [23]. However, a widely accepted interception architecture that would specify in detail what the functions are and where in the network they should be done might be successful. This architecture could be used as a base to which new functions can be added or deleted, if something does not work properly. Moreover, if such an architecture was widely known, then many organizations, companies, and individuals might evaluate it, test it, and address open problems. This evaluation could help further development of such architecture.

In recent years Cisco Systems has made a significant effort to support lawful interception of VoIP calls. In 2006, they described an architecture for LI known as Service Independent Intercept [27]. This architecture describes specific Cisco Systems tools that "can be used by the ISPs in order to construct an LI-compliant network" [27]. There is a document [28] that describes in detail how interception can be performed in

Cisco Systems' LI architecture. The main characteristic is that the interfaces and the functions are quite similar to those that exist in the ETSI standard for both traditional and mobile telephony [18]. The Cisco Systems approach shows that there can be an evolution in VoIP interception architectures as standards have been updated since 2003. By incorporating this architecture in products which they have introduced to the market, it has become one of the de-facto standards for VoIP lawful interception.

4.6.2 Use of a Trojan

As already stated, Skype (and a number of other clients) uses strong encryption of the media between the parties of a call. The result is that even if a lawful intercept agency managed to intercept these packets it would be difficult to decrypt them by brute force. To overcome this problem a new way of interception has been introduced by DigiTask [29], a German company. The main idea for intercepting Skype calls is the installation of a Skype-Capture-Unit on the target's computer. This unit (which consists of malware software) captures the voice and chat traffic directly and diverts it to an anonymous recording proxy which in turn can forward it to a final recording server. The intercepted data can then be accessed "via mobile evaluation stations" [29]. Also, the intercepted data is encrypted for security reasons and compressed to save bandwidth. The forwarding of the capture-unit's intercept can be done through email or via direct communication with the target's computer. Finally, the analysis of the intercepted data can be done following decryption and decompression using a media player - which can play voice and other forms of data back in real time.

Similar to the above surveillance technique is the use of a "key logger" system [30]. A key logger is surreptitiously installed in the target's computer and starts recording the keystrokes from the keyboard. This means that whatever the user of the computer enters via their keyboard it will be captured by the key logger system (even characters that were typed and then deleted). The captured keystroke data are sent to the law enforcement agency. Key loggers can be placed onto the target computer manually or by sending it remotely as a virus. With this technique encryption does not provide any protection, as the user's entry of a key is captured, hence the key can be entered to a copy of the same software at the LEA and the security circumvented. (note that there can still be inadequate information to decrypt the intercepted encrypted information – for example the user might use an external encryption unit which contains the actual key generation function – thus without access to this information the user entered phase phrase might not be sufficient)

4.6.3 Watermark technique

In 2005, a university team conducted a survey/experiment [31] about how feasible the tracking of VoIP calls through anonymizing networks would be. This team proved that even if a calling party uses a network that anonymities the traffic to make his/her VoIP calls that a call can be tracked. The main idea behind this tracking method is to embed a unique watermark into the encrypted VoIP packets. This watermark is based upon a timing adjustment that can be preserved even if the packet flows through an anonymous network [31]. A key to the success of the experiment was that the time interval for the addition of the watermark (i.e., the added delay) has to be less than 20ms or 30ms, as this is the usual inter-packet delay of a VoIP flow. Due to this constraint the team utilized

3ms adjustments in order to assign unique labels to VoIP packets. A larger watermark delay causes a greater distortion in the original inter-packet timing -- which can be detected by the target. Using this method (See Figure 9) someone who can intercept the traffic can track when two parties are communicating. Note that this interception can now be conducted by access to a very high speed backbone link – rather than being restricted to routers near the caller or callee. The watermark enables the intercept to select only the correctly marked traffic for further processing.

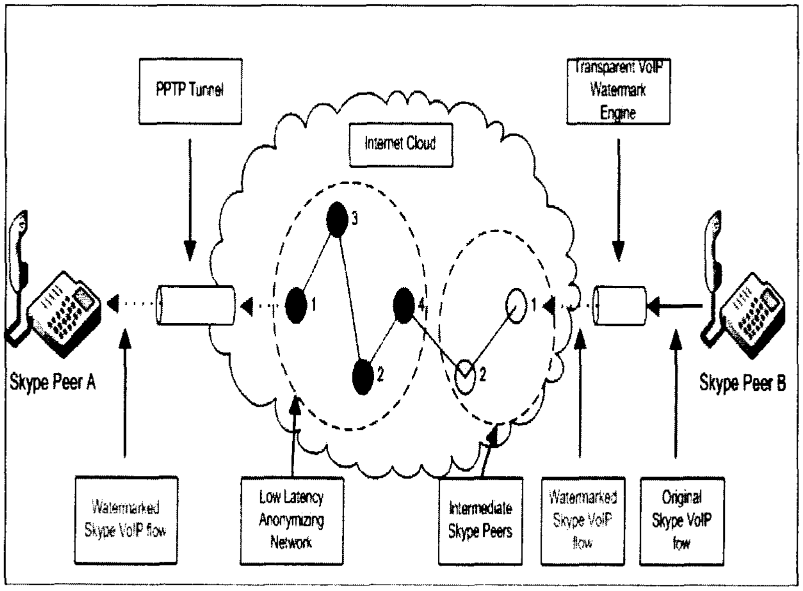

PPTP Tunnel
Internet Cloud
Transparent VoIP Watermark Engine
3
1
4
2
1
2
Skype Peer A
Skype Peer B
Watermarked Skype VoIP flow
Low Latency Anonymizing Network
Intermediate Skype Peers
Watermarked Skype VoIP flow
Original Skype VoIP flow

Figure 9: Experimental setup for real-time tracking of anonymous VoIP calls (Adapted from [31])

and key recovery encryption items" [34]. They cited the main specifications of global key recovery systems (which were based mainly upon law enforcement demands [35]) as:

- **Access of TTP or government without the notice to or consent of the user.** This also affects "self-escrow" systems where companies may deposit their own keys, but they must provide a mechanism that obscures the revealing of the decryption between the key owners and the recovery agents.
- **International adoption of key escrow systems.** In order to succeed and provide real help to law enforcement agencies, key recovery systems must be as widespread as possible. This means that for the majority of the encrypted data and communications a key escrow system must be used, *whether there is an end-user demand or not.*
- **Law enforcement agencies demand high availability to the decryption keys.** In the U.S.A. the time to obtain the keys was specified as two hours (i.e., near real time). Moreover, the recovery process should be available 24 hour per day 365 days of the year.
- **The system should provide access to encrypted communications as well as to encrypted stored data.** This explicit inclusion of encrypted communications was important, as industry only seemed be interested in accessing encrypted stored data as opposed to securing and recovering communication traffic.

The above specifications were widely seen as incompatible with the needs and requirements of commercial encryption users. Unfortunately, governments took into consideration only their own needs, although they tried to appear as if they also considered the requirements of industry and commercial users; but as they failed to convince the industry and commercial users that the government's needs were the same as or trumped the users' needs the government's argument was unsuccessful.

5.2 Clipper chip

Perhaps, the most widely known key escrow implementation was the Clipper chip [32]. The clipper chip was a cryptographic device which was designed to encrypt private communications while simultaneously making the conversation's key available using the keys held by TTPs. The concept behind Clipper was that the session key would be encrypted and transmitted along with the session, thus given access to the device's keys from the TTP the government agents could easily recover the contents of a telephone conversation – for example to introduce the call as evidence in court. The intention of the U.S. government was that all telecommunications companies would be forced to use this device.

The main idea behind the Clipper chip was that each telephone device would have an embedded Clipper chip which was responsible for the encryption of all data passing through the device. Each chip had a unique key. The government stored "a record of the serial number/encryption key correspondence for every chip manufactured" [32] in order to have the ability to use it later for monitoring/intercepting a conversation. In order to calm the fears that many people had against the government possessing these keys and the probability of undesired practices, the government decided not to keep the keys only in a single "safe" place. Instead, each key was broken in two quantities and these two parts were to be delivered for deposit and safekeeping with two different agencies. The reason for this was that it would be more difficult to misuse the keys for monitoring purposes as access to the keys would require the cooperation of two separate agencies. In order to enforce this status, the U.S. government claimed that voluntary cooperation *without a court order* to deliver the parts of the key among separate government agencies was improbable [32]. Another strong point of the key escrow system was that the pieces of each deposited key must be XORed in order to produce the actual key. Therefore knowledge of **only** one part of the key is completely useless for the retrieval of the complete key (or even the recovery of any bits of the key!).

For encryption the Clipper chip utilized a classified algorithm known as Skipjack, which was invented by NSA (note that the U.S. government declassified this algorithm in 1998). Furthermore, the Diffie-Hellman key-exchange algorithm was used for the agreement of a session key between the peers [32]. The information that agencies needed to decrypt the packet were included in a field known as the Law Enforcement Access Field (LEAF) which was transmitted during each communication session. An important aspect of the use of the Skipjack encryption algorithm was that the LEAF sent from a caller to a recipient must be valid; otherwise no communication would be permitted. This had the advantage that a strong encryption algorithm could be used, but the government could be ensured that since the LEAF was valid they would be able to decrypt it given the proper key.

Although the Clipper chip escrow system seemed very robust, in 1994 Matt Blaze demonstrated and described in a paper [33] a serious vulnerability in the security of the Clipper chip system. This vulnerability occurred because a 16-bit part of the (128-bit) LEAF contained a hash value that was used as a checksum to ensure the integrity of the LEAF data. If the receiver computes another checksum over the LEAF, then his/her Clipper chip would not decode the message. The problem was that 16 bits was a very small number, thus only 2^{15} random numbers had to be tested (in a brute force attack) before finding the correct checksum. In this case the Clipper chip could be used as an encryption device, but the LEAF field would be invalid and hence the government's key escrow capability could not yield the correct session key.

As a result of the above serious security defect, the Clipper chip was abandon in 1996. Although this key escrow system did work it was not adopted, hence the U.S. government continued to pressure manufacturers to adopt key escrow in order to reduce the difficulty of decrypting encrypted conversations.

5.3 Advantages of a key escrow system

The main (and perhaps only) supporters of the key escrow systems were and still are governments and theirs agencies that want an easily controlled method which would offer secure communication while also allowing lawful interception. In order to persuade others (i.e. companies, individual cryptographers, and the average person) they tried to point out the benefits that a key escrow system could offer in society even if the result was not as expected.

The main advantage of a key escrow system is that a government and its LEAs can provide better security for the public, because they can effectively control encrypted communications by knowing all the keys -- but only if every user is forced to deposit their master keys with one of TTPs. This means that a LEA can easily access a target's conversation even if it is encrypted, by using the master keys to decrypt it. Moreover, with the proper participation of the TTPs, they hoped to assured that no one could easily misuse their knowledge to improperly access the master keys and inappropriately gain access to an encrypted conversation. Because each master key would be broken into parts and delivered to different agencies (i.e. as was proposed for the Clipper chip), this was expected to prevent illicit wiretapping as the collaboration of different agencies in an illegal act (i.e., disclosing a key without proper authorization) was supposed to be extremely difficult [32]. The assumption was that separating the key into parts controlled by separate agencies offers a secure way to guarantee that there would not be any violation of human rights and freedom as illegal decryption of the conversation would require a lot of cooperative effort.

Another advantage of a key escrow system – in a company – is that it would allow a company to easily monitor all the communication of its employees. Why would a company need to do this? Basically, there are two reasons for a company to use key escrow system [32]. First, if the employees of a company know that their conversations (even if they are encrypted) can be easily decrypted and read/listened to; then they are more likely to conform to the company's policies. Second, the company can assure that no data will be lost if an employee forgets a password or leaves the company. An additional reason (in the post-Enron era) that a company might need access to a copy of an encrypted conversation is to comply with a legal search and discovery order from a court.

It is understood that in both cases (national and corporate level) a key escrow system's main advantage is the 24hour **availability** of access to encrypted data, thus giving the responsible authorities the ability to access this data. Unfortunately, this does not mean that they can control access to this data (as in the event of law enforcement actions the access to the data might be done without the knowledge or consent of the individuals or company).

5.4 Disadvantages of a key escrow system

Despite the government's attempt to persuade companies, independent cryptographers, and other people of the usefulness of the key escrow systems, the negative reaction was significant from all sides. From the very beginning key escrow systems were criticized due to the severe security flaws they suffered and the great potential for possible violation of human rights and individual privacy. There are a number of risks that make key escrow highly insecure [36]:

➢ Introduction of new vulnerabilities

- *Potential illegal access to data:* As the TTPs have the ability to use the master keys in order to intercept communication (even without a court order) it is possible for them to perform illegal acts. Moreover, because the companies or individuals will not know that the TTPs has used their master keys for monitoring them, the company or individual cannot protest this (potentially) illegal access to their communications. Access to such data may give a government or its agencies a strong advantage against targets, so there is an incentive to circumvent court orders and simply access the target's conversations. Examples of this type of potential abuse include the U.S. government's ability to persuade telecommunications companies to give them unrestricted access to international trunks [40], [41], and [42].

- *Insider misuse:* One of the most dangerous threats that a key escrow system introduces is insider misuse, for example to produce records that appear to be legitimate, but which in fact have been forged. As the employees of TTPs may not be as trustworthy as he/she should be, they might be "motivated by greed or ideology" [35] to compromise the secrets of individuals or companies (sometimes this has been part of a scheme to blackmail the individual or company). This has happened many times in the recent past; in these cases someone exploited his/her position in order violate others privacy for his/her own advantage. However, revealing secret information of companies or individuals is only one type of insider misuse. The other type of misuse is more severe, in this case a person who has the session keys of a conversation may "fabricate" contents [37] (i.e. counterfeit contents) that a user never sent in order to incriminate him/her. This practice has also been used a lot in the past. However, creating forged contents is a double sided sword at it may impair the ability to use wiretapped communications as evidence in the court.[37].

- *New targets for attack:* One of the main characteristics of key escrow systems is the depositing of the master keys in central databases. This feature makes these databases a high value target as "the theft of only one private key (or a small set of keys) which are held by a recovery agent may disclose all the data or part of them of an individual or a company" [35] or even worse from a "broader array of communication" [35]. This problem will be highlighted by the key escrow systems themselves, as for every encrypted communication a "pointer" must exist in order to direct the LEA how to retrieve the key information. Thus this "pointer" becomes a target upon which attackers can focus their efforts for intrusion. Even though, the risk may be decreased by splitting the keys and delivering them to different agencies, doing so will create several other problems (i.e. increased cost, longer response times in order to assemble the keys and provide the plaintext).

- *Destruction of Forward Secrecy:* As key escrow systems enable access to the session keys of every conversation encrypted by the device, forward secrecy is not available. Forward secrecy offers two characteristics. First of all, its design is simpler. Secondly, the system has enhanced security and lower cost. This happens because if a system uses forward secrecy, even if one key of a conversation is compromised there is no threat that other communications will be revealed. For example, in an encrypted telephone call the session key(s) exists only during the conversation. When the call ends the key(s) are destroyed (sometimes they are destroyed several times during the same call) so later decryption of this conversation is not possible - since the keys have not been retained. But with a key escrow system the ability to restore the original communication exists, as the keys which the TTPs have stored enable one to access the encrypted session keys which were transmitted as part of the original communication, hence later access to this encrypted communication is both feasible and simple for a possible subsequent use voiding any thought of forward secrecy – since all traffic which has been captured from this device in the past or in the future are accessible.

- *Storage of the keys in the Key Recovery Center (KRC):* Another problem that a key escrow system faces is what kinds of keys must be deposited for subsequent recovery. As there are many different kinds of encryption keys, it is difficult to decide which keys must be stored in the TTPs. For the purpose of key escrow systems, encryption keys can be divided into three categories. First there are the keys that are used for encrypting stored data. It is easy to understand that these keys must be available for the lifetime of the data, as the owner has an interest in access to his/her information. The second category of the keys includes those that "are used for the encryption of a real-time conversation" [38], such as calls. Here the interest in storing these keys is solely on the part of LEAs or someone else who wants to have access to this communication. Generally the communicating parties do not want recoverability of their conversation (although as noted above they may be compelled to provide this for regulatory or other legal or business purposes). During the call the keys may be destroyed and new ones can established without any loss of information between the communicating parties.; thus these keys are only used for a very limited period of time (the communication session duration or less). Lastly, there are the keys used for authentication and signatures which "insure that messages originated from a particular party" [38]. For these keys there is no need for anyone (either owner or LEAs) to recover them as they do not prevent lawful access to data, but rather protect the **integrity** of the data. If an owner looses a signature key, he/she can establish a new one very easily (although perhaps at some cost of time and money). Therefore there is no legitimate need for any of these key categories to be stored. However, as these keys are usually "indistinguishable from one another outside of the application in which they are used" [38] all of them might be stored and consequently they risk exposure in key escrow systems.

➢ Complexity

- *Design complexity:* According to many professional cryptographers there is a general admission that building a practical secure cryptographic system is extremely difficult. The introduction of new parameters in a cryptographic system may create several new security flaws. Even in non-key recovery systems which have fewer requirements, many exploitable flaws are still discovered [35]. Key escrow systems are considered more complex due to the necessity of key storage. This feature adds a lot of complexity in the overall design of the system. One of the best examples of the weaknesses (and subsequent failure) which can result is well illustrated by the Clipper chip.

Even though the Clipper chip was designed by NSA (an agency with a lot of experience in cryptography) – security deficiencies still existed. It is important to note that the weakness was not in the algorithms, but rather the implementation choice of a short checksum.

- *Scale factors:* Governments and their law enforcement agencies have envisaged a key recovery system that would extend worldwide. This means that a very large number of companies, LEAs, and TTPs must corporate in order to succeed in their "mission". However, considering only the numbers of the involved people and organizations it is easy to understand that a worldwide system is almost impossible (simply due to scaling issues). Nowadays, millions of users every day use encrypted communications (i.e. access secure pages via the Internet). Moreover, there are thousands of products in the worldwide market that provide encryption. There are several tens of thousands of TTPs and LEAs worldwide. It is hard to image the secure and successful depositing of hundreds of billions of recoverable session keys (for every encrypted telephone call, stored encrypted file, e-mail, web session) [35]. Finally, the infrastructure to support and manage the system will be vast. As a result of the overall magnitude of a worldwide key escrow system, it is clear that a system is not viable.
- *Operational complexity:* According to the U.S. government, a key escrow system in order to provide good services must operate on a worldwide scale. However, this requires a lot of complexity, not only due to the enormous number of the entities involved, but also due to the number of the key recovery requests - each of which requires a speedy response. The result is that the system could be vulnerable to fraudulent key requests and keys might be exposed to the wrong people. Consequently, there will be partial compromises of the system. While a well designed system, well trained staff, and technical controls can reduce the risks of a key escrow system (to some extent), "the operational vulnerabilities in the process of key recovery cannot be eliminated entirely" [35]. Thus there are going to be some leaks - which may have either little or major impact on individuals, companies, and governments. One only need to look at the leaks of confidential and secret personal information which already takes place today, with frequently several reports per week of disclosures of personal data (ranging from medical records to tax records).
- *Authorization for key recovery:* One of the requirements of a key escrow system is that only authorized people can request a session key. However, it is widely known that identity documents, such as passports and birth certificates can easily be forged. Using such forged identification, someone might be able to illegally obtain a key in order to eavesdrop or even forge conversations. It is possible that a key escrow system that would operate locally (i.e. inside a company) may not face this risk of forged personal identification. This is because the key administrator might personally know everyone who has "the rights to which keys" [35]. However, this "knowledge" is not readily available when the scale of the key escrow system exceeds a very small scale.

➢ Costs

- *Operational costs:* Even though "cryptography is an intrinsically inexpensive technology", the scale of a key escrow system that would extend beyond the national borders of U.S.A. would cost a lot for its operation. The reason for high operational costs is that government requires availability around the clock (365 days per year), which requires to a lot of employees. Moreover, staff should be well trained in order to perform their job properly. High-assurance hardware and software should be purchased in order that the government could be sure that the system will not have any bugs.
- *Product design costs:* For the operation of such a large scale key escrow system the products (software and hardware) should be designed to support user-level encryption. Doing so will increase the product's design costs as correctly adding encryption is not a simple job. The result could be poor implementations on the vendors' part, i.e. poorly design products. While the product might be designed well, if it is mis-configured by the user, then the security might be weak. In addition, if encryption is needed for older products, this might entail significantly greater costs.
- *Government oversight costs:* Finally there will be the expenses necessary for the government and its LEAs to "test and approve key recovery products" [35]. The plethora of key recovery products that will exist in the market should all be tested to see that they comply with the government's requirements and if they suffer from any security flaws. This can be a time-consuming and costly process. Moreover, government also needs to certify and audit the recovery agents and their ability to provide the services they are to perform. This also means extra cost as there must be an appropriate inspection mechanism to do so.

Based on the above analysis, it is clear that key escrow systems suffer from many vulnerabilities (i.e. security problems, cost, difficulties in their design and operation) that render key recovery unsuccessful, at least as far as it concerns large scale systems. However, a key escrow system implemented on a much smaller scale – such as inside a single organization or company – might eliminate many of these risks, this is not the intension of the U.S. government, as they want to have the ability to intercept the majority of communications and decrypt the majority of stored data.

6 SRTP/MIKEY and Key Escrow

According to chapter 5 analysis it is understood that key escrow systems suffer from a very serious flaw – forged data – that can undermine the whole credibility of the system. An authorized person that has access to the session keys of a conversation may forge traffic in order to create "evidence" that will incriminate one (or both) call parties. This is a very problematic situation, as a court cannot easily decide if the recording of a conversation is legitimate or not.

The idea of using digital signatures was suggested as a solution to this problem. The idea is that the signature can be used to verify the real source of the data. As many VoIP companies are using SRTP in order to transmit data in a secure way, one means to prove who the source of the data was is to compute signatures over groups of packets. The signature will be produced using the private key of the user – as this key is **not** stored in any key escrow system. This means that even if a malevolent employee of a TTP organization knows the session key that was used to encrypt the SRTP data, he/she may generate forged data, but will not be able to correctly fabricate the digital signatures. Hence with the help of digital signatures it can easily be proven (by anyone with access to the source's public key) that the contents were not produced by the alleged source.

6.1 Secure Real –time Transport Protocol

The secure real-time transport protocol (SRTP), defined in RFC 3711 [43], is a secure profile for RTP. SRTP adds confidentiality, message authentication, and integrity – through replay protection – to the RTP traffic and to the control traffic for RTP (Real-time Transport Control Protocol - RTCP). RFC 3711 defines the format of an SRTP packet, the algorithms that can be used in order to encrypt/decrypt RTP packets, and also the mechanism for key derivation. Generally, there are two types of keys in SRTP: session keys and master keys. Session keys are used for the encryption of the data or for message authentication. Master keys are random bit strings that are provided by a key management protocol, (i.e. Multimedia Internet KEYing, MIKEY) which are used for the production of the session keys in a cryptographically secure way.

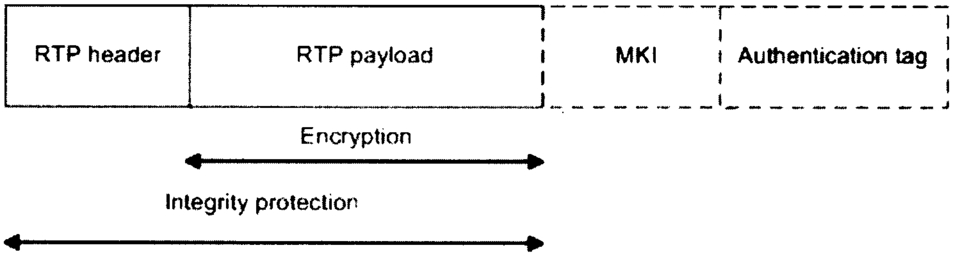


Figure 10: Format of SRTP packet (Adapted from [44])

Figure 10 shows the structure of an SRTP packet. Encryption is only applied to the RTP payload (to ensure confidentiality of the message). However, integrity protection includes both the RTP header and payload by adding an authentication tag to the end of each packet. There is also a Master Key Identifier (MKI) field in the SRTP packet which indicates to the receiver which master key was utilized for the derivation of the session key(s) that was/were used in this particular SRTP packet. Both the MKI and Authentication tag fields are optional.

SRTP needs six session keys to protect the media. The first triplet concerns the security of RTP packets (a session encryption key, a session authentication key, and a session salt key) and the second triplet the security of RTCP packets with the equivalent session keys. To generate all of these session keys, SRTP uses a key derivation function which needs only a single master key. The master key was exchanged via a key management protocol (i.e. MIKEY). The production of the six session keys is known as key splitting and it works with the help of a pseudo-random function (PRF), the master key, the derivation rate, the master salt (which is exchanged also via the management protocol) and a label. Different values of the label generate different the session keys.

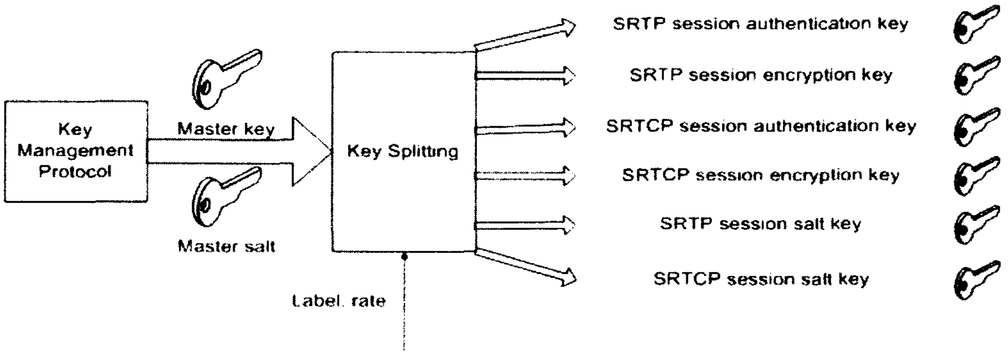

Key Management Protocol
Master key
Master salt
Key Splitting
Label, rate
SRTP session authentication key
SRTP session encryption key
SRTCP session authentication key
SRTCP session encryption key
SRTP session salt key
SRTCP session salt key

Figure 11: SRTP Key Splitting (Adapted from [44])

The previous description shows that SRTP is an independent protocol, as far as the generation of the sessions keys are concerned. With the embedded key splitting function SRTP only needs one key (the master key and its related parameters) for the derivation of all the other keys. However, SRTP must provide some mechanism(s) to change keys in order to provide better security:

- *Key refresh*: The key derivation function can also be used to regenerate session keys. This is very helpful as with the same software new keys can be produced. The use of new session keys can provide increased security as small pieces of data will be encrypted with the same session key. This means that if an attacker managed to compromise a session key, only the data that are encrypted under this specific key can be revealed. The other session keys do not have any relation with the compromised key as the derivation function prevents this from happening. By using multiple session keys, SRTP achieves perfect forward secrecy for all of the separate streams. The key derivation rate defines how often the key refresh will take place. However, key refresh is an optional feature in SRTP as although it works well in unicast sessions such a mechanism is not suitable for a multicast sessions -- as every participant would have to maintain a potentially large number of keys (6 times the number of participants) which could have a serious impact on performance – especially if these keys are refreshed frequently. However, if the key was only refreshed at a rate driven by the user's transmission; this mechanism might even be applicable to multicast sessions with a modest number of users.

- *Re-keying*: This mechanism concerns the change of the master key. Re-keying can be achieved with the execution of a key management protocol, which makes the whole procedure complicated and computationally expensive. Why is there a need for a new master key? Because compromising of the master key would reveal all the session keys, re-keying is obligatory for the following reasons [45]:

1. When the lifetime of the master key has expired.
2. When there is a compromise of the master key.
3. Depending upon the application policy (i.e. the application may trigger rekeying every time there is departure from a session or a new participant added to a session, or due to a conservative security policy that limits the amount of ciphertext encrypted with the *same* master key).

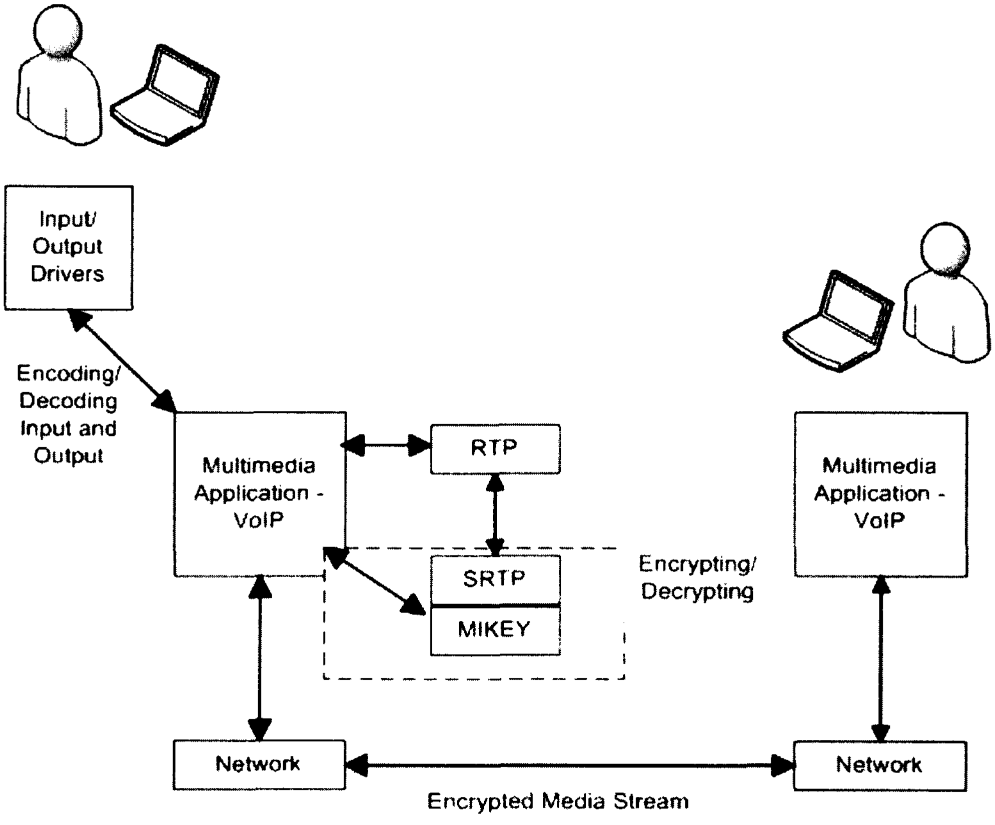

Input/ Output Drivers
Encoding/ Decoding Input and Output
Multimedia Application - VoIP
RTP
SRTP
MIKEY
Encrypting/ Decrypting
Multimedia Application - VoIP
Network
Network
Encrypted Media Stream

Figure 12: SRTP encoding/decoding process (Adapted from [46])

Figure 12 depicts the SRTP encoding/decoding process during a VoIP conversation. First the application "captures the input from a device (i.e. microphone) and encodes the signal" [46]. Then it creates the RTP packet payload which is encrypted by an encryption algorithm (i.e. AES). Before RTP packets are sent to the network they must be secured. SRTP converts the RTP packets to SRTP packets. Now, the SRTP packets are ready to be transmitted through the network. When the data arrives at the destination, then the multimedia application of the other party (i.e. calling party) decrypts the SRTP packets, producing RTP packets that are ready to present (heard or watched) by the other party.

6.2 Multimedia Internet KEYing (MIKEY)

Multimedia Internet KEYing is a key management protocol that has its main goal to efficiently generate and distribute keys and their related parameters. The keys can be use as master keys in other protocols (i.e. SRTP).

The MIKEY protocol supports three different variants of key agreement [47]:

- *Pre-shared key* (PSK): This method presumes that the peers share a pre-shared key which has been exchanged by some other means. In this variant, symmetric cryptography based upon the pre-shared key is used to derive keys for the encryption and the integrity of the MIKEY message. MIKEY is considered the best solution for key transport as it requires only half or one roundtrip, but it suffers from a lack of scalability as the key has to be shared with every other peer that a user wants to communicate with.
- *Public key*: This method is similar to the PSK method, but here the initiator chooses a pseudo-random key which will be used for encryption and integrity. This key is encrypted using the responder's public key and sent to the responder. Although this approach consumes greater resources than the PSK method, it can be scalable using a Public Key Infrastructure (PKI).
- *Diffie-Hellman*: This method provides perfect forward secrecy. The main difference from the other methods is that in this method the key is not sent to the recipient, but instead both parties contribute to the generation of the key. This method is considered the most resource consuming method and also requires the existence of a PKI.

6.3 Scenario: Minisip and Key Escrow

One of the most serious weaknesses that key escrow has is insider misuse. An authorized employee of the TTP who is motivated by greed or ideology might use his/her authorization in order to access the session keys of a conversation for malevolent reasons. This is a double threat in that he/she can reveal both the session contents and (even worse) he/she can forge the contents of a conversation.

This scenario is very frightening as it will destroy the reliability of evidence coming from systems which have made use of the key escrow systems. The threat of insider misuse is a real scenario, as this has happened several times. Thus this risk is a real threat to individuals or organizations making use of a key escrow system.

Many VoIP clients (i.e. Minisip) utilize MIKEY/SRTP in order to provide protection to the transmitted audio/video packets in a session. These protocols are used to give some protection to the contents of a conversation (as the exchange of the keys is secured and there is also encryption and integrity control). However, if key escrow is used, then all the master keys from which the session keys are derived will be automatically available to the authorized TTP's employees. This has as a consequence that an insider misuse (revealing or forging the contents of the conversation) is possible.

Therefore, the main problem when using key escrow is how a session participant can ensure that even if a key escrow system has stored the conversation's master keys, it is impossible for the session's contents to be forged. One possible solution utilizes digital signatures. Public key cryptography using public/private keys can ensure that when someone sends data he/she is the only possible owner send. Thus an insider can forge contents, but not forge the correct digital signatures – hence protecting the real source from fraudulent or misleading "*evidence*". One possible implementation of this solution is depicted in Figure 13.

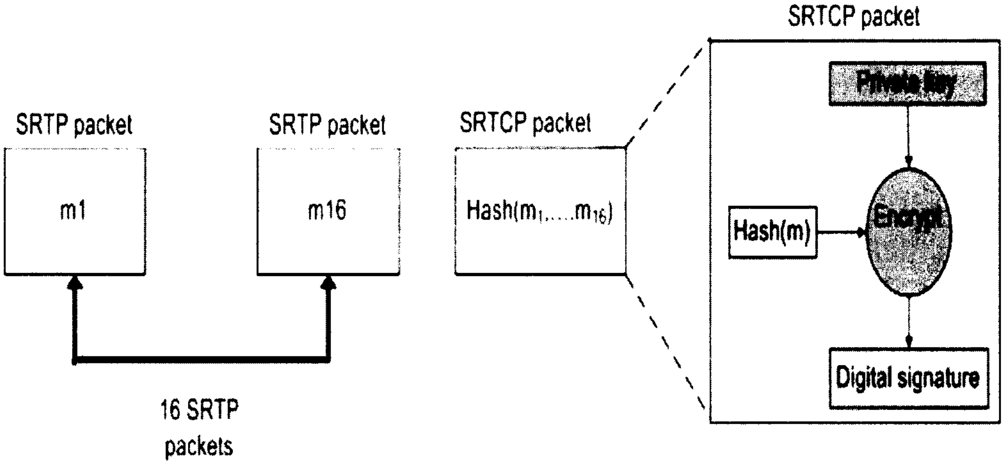


Figure 13: Digital signatures for SRTP packets

In this solution, digital signatures can be used for groups of SRTP packets (i.e. 16 SRTP packets). Every SRTP packet will be encrypted and integrity protected as defined by the SRTP protocol. Following the transmission of 16 SRTP packets an SRTCP packet will be sent which contain a hash of the payloads of the 16 SRTP packets (Hash (m_i)). As the sender of the SRTP packets is the only entity to know his/her private key, (i.e., the private key will **not** be stored by the key escrow system), thus the Hash (m_i) will be signed with this private key producing a digital signature over these packets. This means that anyone with knowledge of the sender's public key can easily verify if the contents came from the real owner of the data. Tampering with data is easily detected as only the owner of the private key can produce a valid signature. Each individual SRTP packet is also protected by encrypting it and with integrity protection. However, as the digital signatures are independent of the session keys (which were derived in a known way from the master keys - which a key escrow system will have stored), the private key (of the public-private key pair) is only known by the real owner. Hence only the owner can correctly sign the hash. Note that the number of SRTP packets which are grouped before the signed hash is an implementation matter – as this represents a tradeoff between increased computation and traffic and the security which this solution offers.

Digital signatures can provide **security and credibility** as to who is the real owner of the contents is, but it does not protect the contents from being revealed by a malevolent TTP's employee. The advantage is that anyone can detect this forgery.

6.4 Problems to consider

The solution with the digital signatures can provide the wanted security and credibility but in order to be implemented some possible problems must be taken into consideration. The main problem is the **rate** of computing the signature. If the signing of the SRTP packets is very often it will add extra traffic as more packets must be produced for the inclusion of the digital signatures. This may cause delay problems in the performance of a VoIP call. However, the delay problem can be mitigated as digital signatures will be transmitted through SRTCP packets which are sent **periodically** to control information of the SRTP flow.

Furthermore, there is the problem of a possible **leakage** of a private key. If for the production of the digital signatures the same private key is used several times, the possibility of someone to find the private key increases a lot. The continuous encryption of a text with the same key may reveal information of the identity of the key. One solution that can be used is the use of more than one private key. By using several private keys the can be confusion to the person who will try to find out the identity of the private key.

Both the above problems must be taken into consideration as they can affect negatively the implementation of the digital signatures.

7 Conclusions

Safe & secure communication is very critical nowadays. However, citizens' communications – at a worldwide level –not only face a threat of privacy violation from malevolent individuals but also from governments. In (nearly) every country, the government has decided to allow lawful intercept of the communications of their citizens (and often most especially non-citizens) for security reasons. Moreover, the tendency is to enact laws that broaden the range of interception by keeping the intercepted data for a longer period of time, by intercepting all the means of communication, and by trying to circumvent court orders in order to perform an interception without proper judicial review.

This thesis examined lawful interception in fixed and mobile telephony and Internet networks. It also presented some of the difficulties in lawful interception due to the specifics of the operation of the various communication networks. The thesis also discussed several countermeasures that a target can utilize in order to avoid (or minimize the value of) interception. Furthermore, an analysis of key escrow systems was given. In addition, there was an examination of a possible elimination of one of the key escrow's main disadvantages - tampering of the contents.

This analysis showed that even if many VoIP clients use SRTP and MIKEY protocols to provide security, a key escrow system that stores the master keys that are used for the production of the session keys might allow a TTP's employee to forge contents could be detected. The use of digital signatures to detect tampering with the data can be a very powerful technique for preventing the introduction of fabricated evidence. This means that evidence from a key escrow system could be reliable as it can be proved if a particular person is the real owner of the data or not. However, the possibility of forged data is only one of the problems that a key escrow system faces. Even if digital signatures can circumvent the problem of forgery, there remain many problems in implementing a successful & secure key escrow system.

8 Future work

This thesis tried to present how lawful interception is performed in fixed, mobile, and Internet telephony by government law enforcement agents. It also presented the difficulties that exist for the different means of interception as targets can utilize countermeasures to avoid being monitored or to create misleading evidence. Finally there was an analysis of a means of overcoming the problem of the insider misuse that exists in key escrow systems.

Even if key escrow systems are difficult to implement and some attempts in the past to create large scale key escrow systems failed, the idea of using a key escrow system to store master keys of all the kinds of communication still exists. This thesis proved that by using digital signatures it is very easy to detect if a conversation has been tampered with. However, as there remain many other problems for key escrow systems, such system should be further analyzed in order to be more effectively & securely implemented. A good start should be the analysis of each key escrow problem separately and the description/implementation of a possible solution for each one.

Moreover, as technology – in the field of telecommunication – is changing rapidly new threats may appear that reduce the effectiveness of lawful interception. Targets may find new countermeasures in order to avoid tracking and monitoring. Also, new documents may be published that present the existing or planned means of intercept or the difficulties that the existing mechanism confronts. So, there will be a need for a more extensive analysis of the new ways of interception and new countermeasures.

A clear need is to implement the method for using digital signatures that is proposed in this thesis in order to understand the practical performance of such a solution in terms of both computation resources needed and the additional traffic which is generated.

9 REFERENCES

[1] Office of the Inspector General, "The Implementation of the Communications Assistance For Law Enforcement Act, U.S. Department of Justice, Audit Division, Audit Report, 06-13 March 2006

[2] MobileIN.com, "Lawful Intercept", Mobile in a Minute mini-tutorials, MObileIN.com http://www.mobilein.com/LI.htm, 28/02/2008

[3] "White Paper – Lawful Intercept Overview", Newport Networks, http://www.newport-networks.com/whitepapers/lawful-intercept1.html , 28/02/2008

[4] U.S. House of Representatives, "50 U.S.C. Chapter 36 – Foreign Intelligence Surveillance" - amendments, Jan. 2, 2006 – Aug. 1, 2008 http://www.law.cornell.edu/uscode/html/uscode50/usc_sup_01_50_10_36.html, 07/04/2008

[5] Steven M Bellovin, Matt Blaze, Whitfield Diffie, Susan Landau, Peter G. Neumann, and Jennifer Rexford, "Risking Communications Security: Potential Hazards of the "Protect America Act"", Security & Privacy, IEEE Computer Society, Jan./Feb 2008, October 22, 2007

[6] Vassilis Prevelakis and Diomidis Spinellis, "The Athens Affairs", Spectrum, http://www.spectrum.ieee.org/print/5280 , 28/02/2008

[7] "Public Safety and Homeland Security", Mobile in a Minute, http://www.mobilein.com/public_safety_homeland_security.htm , 28/02/2008

[8] "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act Of 2001", U.S.A. Congress, Public Law 107-56-OCT. 26, 2001. 115 STATUTORY 272, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf, 31/03/2008

[9] "Directive 95/46/EC Of The European Parliament And Of The Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data", Official Journal of the European Union, 23/11/1995

[10]"Directive 2002/58/EC Of The European Parliament And Of The Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)", Official Journal of the European Union, 31/7/2002

[11]"Directive 2006/24/EC Of The European Parliament And Of The Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC", Official Journal of the European Union, 13/4/2006

[12]Micah Sherr, Eric Cronin, Sandy Clark, and Matt Blaze, "Signaling Vulnerabilities in Wiretapping Systems", Security & Privacy, IEEE Computer Society, Nov./Dec. 2005, pp.13-25.

[13]Denis Howe, "In-band signalling", The Free On-line Dictionary of Computing http://dictionary.reference.com/browse/in-band%20signalling, 07/04/2008

[14]"TR-45 J-STD-025 Rev. A Lawfully Authorized Electronic Surveillance", Telecommunication Industry Association, May 31, 2000

[15]Scott W. Coleman, "DoJ Files Deficiency Petition with FCC over J-STD-025B", TMCnet, June 7,2007, http://blog.tmcnet.com/lawful-intercept/doj-files-deficiency-petition-with-fcc-over-jstd025b.asp, 02/04/2008

[16]U.S. Congress, Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, 3 January - 2008 http://thomas.loc.gov/cgi-bin/query/z?c110:H.R.6304

[17]Jim X. Dempsey, "CDT's Analysis of S. 2092: Amending the Pen Register and Trap and Trace Statute in Response to Recent Internet Denial of Service Attacks and to Establish Meaningful Privacy Protections", Center for Democracy & Technology, Security & Privacy, Wahsington, DC, April 4, 2000, http://www.cdt.org/security/000404amending.shtml, 07/04/2008 – see also The "Carnivore" Controversy: Electronic Surveillance and Privacy in the Digital Age, Hearing before the Committee on the Judiciary United States Senate, Committee on the Judiciary, September 6, 2000, Serial No. J-106-105, U.S. Government Printing Office Washington, 2001, pages 47-61. http://www.loc.gov/law/find/hearings/pdf/00089583263.pdf

[18]Aqsacom, "Lawful Interception For 3G Networks", Document No. 040450, v .4, November, 2005, Aqsacom Inc. Washington, DC

[19]Shana K. Rahavy, "The Federal Wiretap Act: the Permissible Scope of Eavesdropping in the Family Home", The Journal of High Technology Law, vol. II, No 1, 2003, pages 95.-98.

[20]Eric Cronin, Micah Sherr, and Matt Blaze. "The eavesdropper's dilemma", University of Pennsylvania Technical Report, number MS-CIS-05-24. August 2005. http://www.crypto.com/papers/internet-tap.pdf

[21]Robert Valdes and Dave Roos, "How VoIP Works", 09/05/2001, HowStuffWorks.com http://communication.howstuffworks.com/ip-telephony.htm, 15/05/2008

[22]Steven Bellovin, Matt Blaze, Ernest Brickell, Clinton Brooks, Vinton Cerf, Whitfield Diffie, Susan Landau, Jon Peterson, and John Treichler, "Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP", Information Technology Association of America, June 13,2006

[23]Fred Baker, Brian E. Carpenter, NWG, "RFC 2804 – IETF Policy on Wiretapping", May 2000

[24]P. Branch, "Lawful Interception of IP Traffic," Australian Telecommunications, Networks and Applications Conference (ATNAC), Melbourne, December 8-10, 2003

[25]The Economist, "Bugging the cloud", March 6th 2008, http://www.economist.com/printedition/displaystory.cfm?story_id=10789393, last access 22/05/2008

[26]Berson Tom, "Skype Security Evaluation", Anagram Laboratories, 18 October 2005

[27]Cisco Systems, "Lawful Intercept Architecture", http://www.cisco.com/en/US/docs/ios/12_2sb/feature/guide/ht_ssi.html, 29/05/2008

[28]Cisco Systems, "Cisco Service Independent Intercept Architecture Version 1.0", version 2, 15 March 2006, http://www.cisco.com/technologies/SII/SII.pdf

[29]WikiLeaks, "Bavarian trojan for non-germans", http://wikileaks.org/wiki/Bavarian_trojan_for_non-germans, last modified 28 April 2008, last accessed 29/05/2008

[30]Privacy International, "PHR2006 – Privacy Topics – Surveillance of Communications/ Internet Surveillance: Black Boxes and Key Loggers", 18/12/2007, http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559085, 07/08/2008

[31]Xinyuan Wang, Shiping Chen, and Sushil Jajodia, "Tracking Anonymous Peer-to-Peer VoIP Calls on the Internet", 7-11 November 2005, Alexandra, Virginia, USA

[32]Charlie Kaufman, Radia Perlman, Mike Speciner, "Network Security Private Communication in a Public World", Prentice Hall PTR, 2002

[33]Matt Blaze, "Protocol Failure in the Escrowed Encryption Standard", Proceedings of Second ACM Conference on Computer and Communications Security, Fairfax, VA, November 1994.

[34]Dept. of Commerce, "Interim Rule on Encryption Items," Federal Register, Vol. 61, p. 68572 December 30, 1996

[35]Hal Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, "The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption", Sun Microsystems, Menlo Park, 27 May 1997

[36]Erland Jonsson, "KEY ESCROW – a System for Law-Enforced Covert Surveillance and its Risks", Department of Computer Engineering, Chalmers University of Technology, 01 December 2004

[37] Martin Rex, "RE: [TLS] draft-housley-evidence-extns-00 worse than key escrow", IETF-TLS, 8 January 2007

[38]Matthew Blaze, "Testimony Of Dr. Matthew Blaze Before The Senate Committee On Commerce, Science, And Transportation, Subcommittee On Science, Technology, And Space", Congressional Hearings Intelligence and Security, June 26 1996, http://www.globalsecurity.org/intell/library/congress/1996_hr/960626_blaze_test.htm, 04/06/2008

[39]Simson L. Garfinkel, "VoIP and Skype Security", Creative Commons, 3/12/2005

[40]Mark Klein, "Wiretap Whistle-Blower's Account", Wired News, April 6, 2006, http://www.wired.com/science/discoveries/news/2006/04/70621, 08/08/2008

[41]Ryan Singel, "NSA Must Examine All Internet Traffic to Prevent Cyber Nine-Eleven, Top Spy Says", Wired News, January 15, 2008, http://blog.wired.com/27bstroke6/2008/01/feds-must-exami.html, 08/08/2008

[42]Ryan Singel, "NSA's Lucky Break: How the U.S. Became Switchboard to the World", Wired News, October 10, 2007, http://www.wired.com/politics/security/news/2007/10/domestic_taps, 08/08/2008

[43]M. Baugher, D. McGrew, M. Näslund, E. Carrara, and K. Norrman, "The Secure Real-time Transport Protocol", IETF RFC 3711, March 2004

[44]Elisabetta Carrara, "Security for IP Multimedia Applications over Heterogeneous Networks", Licentiate thesis, Royal Institute of Technology (KTH), Stockholm, Sweden, August 31 2004, http://web.it.kth.se/~carrara/licproposal.pdf

[45]Elisabetta Carrara, Security for IP Multimedia Applications over Heterogeneous Networks, Licentiate thesis, Royal Institute of Technology (KTH), Stockholm, Sweden, May 2005, http://web.it.kth.se/~carrara/lic.pdf

[46]Peter Thermos, Ari Takanen, "Securing VoIP Networks Threats, Vulnerabilities, and Countermeasures", Addison-Wesley Professional, August 01,2007

[47]J. Arkko, E. Carrara, F. Lindholm, M. Naslund, and K. Norrman, "MIKEY: Multimedia Internet KEYing", IETF RFC 3830, August 2004

[48]John Leyden, "Italy tops global wiretap league: State of the surveillance nation", The Register, Wednesday 7th March 2007 18:15 GMT http://www.theregister.co.uk/2007/03/07/wiretap_trends_ss8/

[49]Lewis Page, "VOIP and the web baffle Brit spook wiretappers: MI5, GCHQ bemoan 'biggest change since telephones', The Register, Wednesday 30th January 2008 15:27 GMT http://www.theregister.co.uk/2008/01/30/gchq_mi5_baffled_by_ip_wiretapping/

[50]Erik Eliasson, et al., Minisip, http://www.minisip.org/, last accessed 2008.09.07.

[51]SIPphone.com, Gizmo5, http://gizmo5.com, last accessed 2008.09.07.

[52]Axill Europe Ltd., Globe7, http://www.globe7.com/, last accessed 2008.09.07.

[53]Billy Biggs, Wirlab, and others, KPhone, http://sourceforge.net/projects/kphone, last accessed 2008.09.07.

10 Appendix A

Eavesdropper's dilemma

Generally, it is considered that in order for a tap to be effective the recording must have 'fidelity'. Here, fidelity means that the recording is free from all the factors (like excessive noise or distortion) that can decrease the quality of the reproduced call contents. For an interception system in order to achieve fidelity it must be free from some serious threats that can seriously undermine its performance. The above threats are known as: obfuscation[11], confusion[12], and evasion[13].

The main problem that faces an eavesdropper is how sensitive[14] and selective[15] a recording has to be. The above two characteristics are in collision. If the eavesdropper is very sensitive and so captures all the messages in order to avoid the attack of evasion, the interception system is vulnerable in confusion as it may record a lot of noise that will decrease the quality of the intercepted contents. On the other hand, if the eavesdropper is very selective in order to avoid the attack of confusion, many of the transmitted messages can elude from the tapping as they can be ignored as insignificant messages.

The above problem exists also in POTS especially when the analog signal is converted to digital (i.e. the signaling between the subscriber and the switch). In order to perform, POTS uses a touch-tone system which "is an international standard known as DTMF" [20] that all the manufacturers of telephone equipment accepted in order to exist a global compatibility. The DTMF's specification "lists acceptable ranges for tone duration, spacing, frequency, amplitude, and twist" [20].

However, in reality the production of a DTMF decoder that can precisely follows the above specifications proved to be harder and more expensive than it was expected. The majority of the decoders are tolerant in some of the standard's specifications. As a result every type of decoder has a unique range of accepted tones that leads to production of out-of-specification tones and in the rejection of them by some other decoders. The negative consequence of the above is the exploitation of this knowledge by a subject with the performing of the attacks of evasion and confusion.

The above dilemma remains in every effort to intercept. The solution for on how selective or sensitive a tap has to be is not an easy task. However, suggestions and decisions can be taken according to the specific characteristics of each individual interception.

[11] When an interception system cannot correctly interpret a message (the message's contents, its headers, or both) [20].

[12] When an interception system records messages that are sent on purpose from one party in order to confuse the law enforcement agency as the second telephone party knows to reject them [20].

[13] When an interception system cannot capture and record all the messages which are sent between two telephone parties [20].

[14] When an eavesdropper considers all the messages as important and records them [20].

[15] When an eavesdropper must recognize the real call contents [20].

5 Key escrow

During the early of 1990s a new idea for monitoring telephone communications was introduced in the U.S.A. The primary people responsible for this concept were at the U.S. National Security Agency (NSA). This concept is widely known in cryptography as key escrow. The main characteristic of this approach is that the keys needed to decrypt encrypted data were stored by a Trusted Third Party (TTP) which can provide the key to a LEA after a court order or an official warrant. By storing the private keys with a TTP, the government and its LEAs could gain access to all the encrypted conversations because they could decrypt them *after* getting the stored keys, without the knowledge of the target. Of course, storing of the key used to encrypt every encrypted conversation regards everyone as a potential "criminal" whose communication might need to be monitored. One of the important questions is who should be the TTP? The main attributes of the TTP are its widespread trustworthiness and the lack of dependence upon the other TTPs.

In 1993, the U.S.A. government with the assistance of NSA created an encryption device that was supposed to be adopted by telecommunications companies for voice transmissions to implement the key escrow concept. The whole project was widely known as "Clipper chip". This project was abandoned in 1996.

Despite the attempts that U.S. government and its agencies made to promote key escrow as a solution-system that would help nations avoid terrorism and for organizations to avoid losing encrypted information the reactions of independent cryptographers, companies, and civil-rights organizations were tenacious and negative. This made key escrow systems highly controversial and revealed that establishing a suitable trusted party (or trusted parties) did not result in a feasible solution.

5.1 Government's key escrow goal

As governments know when cryptosystems are well designed it is very difficult to recover encrypted data without the correct keys, thus they understand that they need a widespread system that would provide them easy access to all encrypted data. In order to achieve this, the idea of key recovery systems arose. These systems would be built in such a way that they would provide 24 hour accessibility to the master keys enabling the decryption of encrypted data. However, this availability frightened many people due to a potential (or inevitable) violation of their privacy, hence governments promoted the use of key escrow systems by stating that such systems were also very important for industry which needs a guarantee that it can access its **own** encrypted data to avoid a possible loss (for example, following the death of an employee, a physical disaster or other incident that could destroy the keys or render the keys inaccessible to the lawful owner of the data). However, the real needs of industry are different from those of governments, as far as availability of encrypted data is concerned – thus the government's argument was not very successful.

As the U.S. government was the global promoter of key recovery systems we will examine what the officials stated as their goal for key escrow systems. In 1996 there was a statement in the U.S. Department of Commerce's encryption regulations, stating their goal: "envisions a worldwide key management infrastructure with the use of key escrow

COS/CCS 2008-20

www.kth.se

Communications Applications and the Use of Encryption to Protect Telecommunications

Lines for Memo

Encryption is used by default or by choice for each of the world's top 12 communications applications (see Table 2 below for a listing), which have a combined 3.9 billion active users (note – each user likely subscribes to more than one service). While complete Canadian figures for each of the applications are not available, the number of Facebook users in Canada, for example, is around 17.8 million. This means that each time Canadian authorities seek a warrant to intercept communications, they will more than likely encounter the additional obstacle of decrypting those communications.

Background Information

Today, about 80% of Canadians households are connected to the Internet and their general Internet usage include using communications applications such as email, cloud computing, instant message and social networks services (e.g. Gmail, SkyDrive, Skype and Facebook, respectively). Such applications allow Canadians to benefit from easy-to-use and diverse communication tools. An increasing number of these applications include some kind of encryption (either by default or as an option that can be enabled) and support third-party plug-ins that allow adding further layers of encryption. Encryption, which refers to any cryptographic process used to make data more secure and more difficult to be intercepted by third-parties, is no longer a privilege of the State and widely available to the general public and business.

Encryption technology has legitimate and important uses for private citizens and business for the protection of personal information and commerce. However, encryption technology also benefits to criminals and terrorists who use encrypted communications services to shield further their activities from detection, and to facilitate the commission of serious offences. Undeniably, police and national security agencies' ability to lawfully intercept the communications of specific individuals related to specific offenses is diminished by the increasing availability, ease of use and sophistication of encryption technology. Besides, the general trend regarding encryption technology suggests that communications applications are likely to continue to benefit from stronger encryption to ensure the security of users' communications.

Among the likely top 12 communications applications used by Canadians, four are social networks (Facebook, Google+, Twitter, and LinkedIn), three are email services (Gmail, Outlook and Yahoo mail), three are instant communications services (Skype, iMessage and WhatsApp) and two are cloud computing services (iCloud and SkyDrive). These categories of services are not mutually exclusive – for example, the social network Facebook can be used to send instant messages. Although the exact encryption technology used may vary from an application to another, the 12 of them either provide some kind of encryption by default or support additional encryption options for some of their features.

Even though data about Canadians users for each aforementioned application were not available, some partial and related data allows validating the prime importance of these applications with regard to their use by Canadians. Currently, about half of Canadians have a social media profile, 17,863,080 Canadians are on Facebook, 6,514,327 Canadians are on LinkedIn, and the five most visited social media websites by Canadians are Facebook, LinkedIn, Twitter, YouTube and Google+). Table 1 lists the likely top 12 communications applications used by Canadians and provides the number of worldwide active users (which includes Canadian users) for each application.

Table 1: Likely Top 12 Communications Applications Used by Canadians Featuring Encryption Technology or Supporting Encryption Plug-ins, and Number of Worldwide Active Users (AU)

f 665M AU	GM il 425M AU	Outlook 400M AU	g+ 359M AU
twitter 297M AU	YAHOO! MAIL 282M AU	skype 282M AU	iMessage 240 M Users*
iCloud 250 M Users*	SkyDrive 250M AU	WhatsApp 250M AU	Linkedin 225M Users *

Total Estimated Worldwide AU = 3.90 Billion

*= no data on active users

Table 2: Main Application Services Widely Available to Canadians

Service	Encryption Information	Type of Services	Number of Users
1-Facebook	Option to always enable HTTPS secure encrypted browsing.	IM, File sharing, Social network, Geo-location	1.11 billion users (2013) 665 million active users (2013)
2-Gmail	By default, Gmail is set to use HTTPS.	Email	425 million active users worldwide (2012)
3-Outlook	Option to enable 3DES for encrypting messages.	Email	400 million active users worldwide (2013)
4-Google+	Uses HTTPS (Hangouts App needed for IM, Video calls and pics sharing)	Social network, Video calls, IM, File sharing, Geo-location	359 million active users (2013)
5-Twitter	Option to always enable HTTPS secure encrypted browsing.	Social network and Microblog	297 million active users (2013)
6-Yahoo Mail	Option to always enable HTTPS secure, encrypted browsing for all Mail activities.	Email	282 million active users (2012)
7-Skype	Encryption cannot be disabled, and is invisible to the user. RSA for key negotiation and the Advanced Encryption Standard (AES) to encrypt conversations.	IM, VoIP, Video calls, File Sharing	280 million active users (2012)
8-iMessage	All messages are encrypted.	IM, File Sharing	250 million users (2012) (no data on active users) Estimate: 175 million active users
9-iCloud	ICloud data is kept encrypted in transit and on Apple servers (except emails, which are only encrypted in transit). ICloud account includes an email account. http://support.apple.com/kb/HT4865	Storage, File sharing, E-mail	250 million users (2013) (no data on active users) Estimate: 125 active users
10-SkyDrive	SkyDrive doesn't natively support encrypting files, but there are a number of 3rd-party file/folder encryption tools available.	Storage, File Sharing	250 million active SkyDrive users (2013)
11-WhatsApp	In 2012, WhatsApp introduced encryption to its communications (type not specified).	IM, Video/pics, Geo-location	250 million active users (2013)
12-LinkedIn	Emails are not encrypted. SSL for login.	Social Network	225 million (2013) (no data on active users) Estimate: 115 million active users

GLOSSARY

AES: Advanced Encryption Standard (AES) is a symmetric-key block cipher algorithm and a U.S. government standard for secure and classified data encryption and decryption. It supersedes the Data Encryption Standard (DES). The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data (block size: 128 bits/key sizes: 128, 192 or 256 bits). (Wiki)

Block Size: In modern cryptography, symmetric key ciphers are generally divided into stream ciphers and block ciphers. Block ciphers operate on a fixed length string of bits. The length of this bit string is the block size. (Wiki)

DES: Data Encryption Standard is a previously predominant algorithm for the encryption of electronic data. It was highly influential in the advancement of modern cryptography in the academic world and was published in 1977 (block size: 64 bits/ key size: 56 bits). (Wiki)

Encryption: Refers to any cryptographic process used to make data more secure and more difficult to be intercepted by third-parties.

HTTPS: Hypertext Transfer Protocol Secure (HTTPS) is a communications protocol for secure communication over a computer network, with especially wide deployment on the Internet. Technically, it is not a protocol in and of itself; rather, it is the result of simply layering the Hypertext Transfer Protocol (HTTP) on top of the SSL/TLS protocol, thus adding the security capabilities of SSL/TLS to standard HTTP communications. In its popular deployment on the internet, HTTPS provides authentication of the web site and associated web server that one is communicating with, which protects against man-in-the-middle attacks. Additionally, it provides bidirectional encryption of communications between a client and server, which protects against eavesdropping and tampering with and/or forging the contents of the communication. (Wiki)

Key size (or key length): Size measured in bits of the key used in a cryptographic algorithm (Wiki).

RSA: RSA is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large integers, the factoring problem. A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message. Whether breaking RSA encryption is as hard as factoring is an open question known as the RSA problem (key sizes: 1,023 to 4,096 bits). (Wiki)

3DES: An encryption algorithm based on the Data Encryption Standard (DES). Triple DES (3DES) repeats DES three times. Consequently, 3DES runs slower than standard DES. However, it is more secure (block sizes: 64 bits/key sizes: 168, 112 or 56 bits). (Wiki)

Hawrylak, Maciek

From:	Chayer, Marie-Helene
Sent:	July-08-13 2:21 PM
To:	Chartrand, Francine
Cc:	Hattem, Tina; Dyer, Lara; Hawrylak, Maciek
Subject:	RE: Lawful Access Initiative - Grade assessment template

Merci Mme Chartrand. Vos commentaires sont dument notés.

Bonne semaine.

Marie-Hélène

Marie-Hélène Chayer
Director – Investigative Technology and Telecommunications Policy /
Directrice – Politique sur les technologies d'enquête et les télécommunications
National Security Operations Division / Division des Opérations de sécurité nationale
Public Safety Canada / Sécurité Publique Canada
(613)949-3181

From: Chartrand, Francine [mailto:Francine.Chartrand@ppsc-sppc.gc.ca]
Sent: July-08-13 11:55 AM
To: Chayer, Marie-Helene
Cc: Hattem, Tina; Dyer, Lara; Hawrylak, Maciek
Subject: RE: Lawful Access Initiative - Grade assessment template

You will find attached the PPSC's completed template. Note that we've numbered the areas being assessed for ease of reference.

Areas 4 and 5 have been rated under Production/Volume and Efficiency, but cannot be rated for Impact given that we are not in a position to determine the level of impact.

As we discussed previously, area 15 should be modified to remove the mention of prosecutions since we do not see the validity or relevance for linking the emergence of new technologies with prosecutions.

Area 17 might apply to the PPSC, but it is not possible to provide an assessment for any of the three criteria as we are not in a position to confirm or estimate any assessment.

We would like to reiterate our concern with the fact that there is no mechanism to ensure that the subjective ratings are based on the same criteria from department to department – affecting the comparability, reliability and validity of the ratings. As such, we continue to question the value of providing any subjective assessment.

Thank you.

Francine Chartrand
Directrice, Planification stratégique et gestion du rendement /
Director, Strategic Planning and Performance Management
Direction générale des poursuites réglementaires et économiques, et de la gestion / Regulatory and Economic Prosecutions and Management Branch
Service des poursuites pénales du Canada / Public Prosecution Service of Canada
2258-284 rue Wellington Street
Ottawa, Ontario K1A 0H8
Tél. / Tel. 613-946-7991 Télec / Fax 613-946-9977
Courriel / E-mail Francine.Chartrand@ppsc-sppc.gc.ca
Gouvernement du Canada / Government of Canada

From: Chayer, Marie-Helene [mailto:Marie-Helene.Chayer@ps-sp.gc.ca]
Sent: June 28, 2013 11:51 AM
To: Chartrand, Francine
Cc: Hattem, Tina; Dyer, Lara; Hawrylak, Maciek
Subject: Lawful Access Initiative - Grade assessment template

Bonjour,

Tel que convenu, je vous fais parvenir le document à remplir.

Thank you again very much for agreeing to fill out the form – it is much appreciated.

Please don't hesitate to call me if you have any questions.

Bonne fin de semaine

Marie-Hélène

Marie-Hélène Chayer
Director – Investigative Technology and Telecommunications Policy /
Directrice – Politique sur les technologies d'enquête et les télécommunications
National Security Operations Division / Division des Opérations de sécurité nationale
Public Safety Canada / Sécurité Publique Canada
(613)949-3181

Dyer, Lara

From:	Dyer, Lara
Sent:	July-08-13 12:06 PM
To:	Chayer, Marie-Helene
Subject:	RE: Lawful Access Initiative - Grade assessment template

Perfect

From: Chayer, Marie-Helene
Sent: Monday, July 08, 2013 12:05 PM
To: Dyer, Lara
Subject: RE: Lawful Access Initiative - Grade assessment template

Let`s say 1:00.

thanks

Marie-Hélène Chayer
Director – Investigative Technology and Telecommunications Policy /
Directrice – Politique sur les technologies d'enquête et les télécommunications
National Security Operations Division / Division des Opérations de sécurité nationale
Public Safety Canada / Sécurité Publique Canada
(613)949-3181

From: Dyer, Lara
Sent: July-08-13 12:04 PM
To: Chayer, Marie-Helene
Subject: RE: Lawful Access Initiative - Grade assessment template

Or even earlier… I'm on page 15.

From: Chayer, Marie-Helene
Sent: Monday, July 08, 2013 12:02 PM
To: Dyer, Lara
Subject: RE: Lawful Access Initiative - Grade assessment template

Yes because I'm also reviewing it. Would you be available at 1:30 to discuss?

Marie-Hélène Chayer
Director – Investigative Technology and Telecommunications Policy /
Directrice – Politique sur les technologies d'enquête et les télécommunications
National Security Operations Division / Division des Opérations de sécurité nationale
Public Safety Canada / Sécurité Publique Canada
(613)949-3181

From: Dyer, Lara
Sent: July-08-13 11:58 AM
To: Chayer, Marie-Helene
Subject: RE: Lawful Access Initiative - Grade assessment template

Merci – I'm almost done reviewing the Intro… would you like to see my changes before I make them?

From: Chayer, Marie-Helene
Sent: Monday, July 08, 2013 11:56 AM
To: Dyer, Lara
Subject: FW: Lawful Access Initiative - Grade assessment template

Marie-Hélène Chayer
Director – Investigative Technology and Telecommunications Policy /
Directrice – Politique sur les technologies d'enquête et les télécommunications
National Security Operations Division / Division des Opérations de sécurité nationale
Public Safety Canada / Sécurité Publique Canada
(613)949-3181

From: Chartrand, Francine [mailto:Francine.Chartrand@ppsc-sppc.gc.ca]
Sent: July-08-13 11:55 AM
To: Chayer, Marie-Helene
Cc: Hattem, Tina; Dyer, Lara; Hawrylak, Maciek
Subject: RE: Lawful Access Initiative - Grade assessment template

You will find attached the PPSC's completed template. Note that we've numbered the areas being assessed for ease of reference.

Areas 4 and 5 have been rated under Production/Volume and Efficiency, but cannot be rated for Impact given that we are not in a position to determine the level of impact.

As we discussed previously, area 15 should be modified to remove the mention of prosecutions since we do not see the validity or relevance for linking the emergence of new technologies with prosecutions.

Area 17 might apply to the PPSC, but it is not possible to provide an assessment for any of the three criteria as we are not in a position to confirm or estimate any assessment.

We would like to reiterate our concern with the fact that there is no mechanism to ensure that the subjective ratings are based on the same criteria from department to department – affecting the comparability, reliability and validity of the ratings. As such, we continue to question the value of providing any subjective assessment.

Thank you.

Francine Chartrand
Directrice, Planification stratégique et gestion du rendement /
Director, Strategic Planning and Performance Management
Direction générale des poursuites réglementaires et économiques, et de la gestion / Regulatory and Economic Prosecutions and Management Branch
Service des poursuites pénales du Canada / Public Prosecution Service of Canada
2258-284 rue Wellington Street
Ottawa, Ontario K1A 0H8
Tél. / Tel. 613-946-7991   Télec / Fax 613-946-9977
Courriel / E-mail Francine.Chartrand@ppsc-sppc.gc.ca
Gouvernement du Canada / Government of Canada

From: Chayer, Marie-Helene [mailto:Marie-Helene.Chayer@ps-sp.gc.ca]
Sent: June 28, 2013 11:51 AM
To: Chartrand, Francine
Cc: Hattem, Tina; Dyer, Lara; Hawrylak, Maciek
Subject: Lawful Access Initiative - Grade assessment template

Bonjour,

Tel que convenu, je vous fais parvenir le document à remplir.

Thank you again very much for agreeing to fill out the form – it is much appreciated.

Please don't hesitate to call me if you have any questions.

Bonne fin de semaine

Marie-Hélène

Marie-Hélène Chayer
Director – Investigative Technology and Telecommunications Policy /
Directrice – Politique sur les technologies d'enquête et les télécommunications
National Security Operations Division / Division des Opérations de sécurité nationale
Public Safety Canada / Sécurité Publique Canada
(613)949-3181

s.16(2)

s.19(1)

Dyer, Lara

From: Hawrylak, Maciek
Sent: June-28-13 3:41 PM
To: Bill Beiersdorfer (William.Beiersdorfer@rcmp-grc.gc.ca); [redacted] Cameron, Frank; Farley, Manon
Cc: Dyer, Lara; Chayer, Marie-Helene
Subject: Lawful access reprofiling - 2013 exercise

Colleagues,

Please note that I have sent you emails on the secure system (Dragon for PS Finance, the interdepartmental secure system for RCMP and CSIS) launching the 2013 Reprofiling process for lawful access. Further details are found in those emails.

[redacted] but please feel free to contact Lara Dyer (copied, and at 613-991-2938) with any questions.

Best,
Maciek

Maciek Hawrylak
National Security Operations Directorate | Direction des Operations de Sécurité Nationale
Public Safety Canada | Sécurité Publique Canada
Tel | Tél : 613-991-6036
Fax | Téléc : 613-991-4669
Maciek.Hawrylak@ps-sp.gc.ca

Chayer, Marie-Helene

From: Chayer, Marie-Helene
Sent: June-28-13 12:59 PM
To: 'Jeff Beaulac'
Subject: RE: Lawful Access Inisitative

Merci . Toi aussi.

M

From: Jeff Beaulac [mailto:Jeff.Beaulac@rcmp-grc.gc.ca]
Sent: June-28-13 12:40 PM
To: Chayer, Marie-Helene
Subject: Re: Lawful Access Inisitative

We will have someone there. Enjoy your long weekend. Jeff

>>> Chayer, Marie-Helene 6/28/2013 12:01 PM >>>
Bonjour,

As discussed earlier this week, I would like to have a quick meeting on this year's LAI Performance Measurement Report. Specifically, I'd like to discuss the attached assessment chart that we asked your teams to fill out. Please let me know if you can make it.

Many thanks and have a nice weekend.

Marie-Hélène

Marie-Hélène Chayer

Dyer, Lara

From:	Hawrylak, Maciek
Sent:	June-25-13 12:14 PM
To:	Chayer, Marie-Helene; Plunkett, Shawn; Durand, Mathieu; Dyer, Lara
Subject:	FW: Australia postponing its 'lawful access' data retention bill

In reality, we knew they weren't going to move forward with it until after the September elections anyway.

Maciek

From: Audcent, Karen [mailto:Karen.Audcent@justice.gc.ca]
Sent: June-25-13 12:12 PM
To: Angers, Lucie; Sansom, Gareth; Wong, Normand; Nguyen, Trang Dai; Belanger, Pierre-Gilles; Hawrylak, Maciek
Subject: FW: Australia postponing its 'lawful access' data retention bill

From: Scrivens, Mark
Sent: 2013-Jun-25 9:36 AM
To: Therrien, Daniel; Audcent, Karen
Cc: Sugunasiri, Shalin (PS)
Subject: Australia postponing its 'lawful access' data retention bill

http://www.reuters.com/article/2013/06/24/australia-security-idUSL3N0F01T120130624

Mark Scrivens
Senior Counsel | Avocat-conseil
Office of the Assistant Deputy Attorney General | Bureau du Sous-Procureur Général Adjoint
Public Safety, Defence, and Immigration Portfolio | Portefeuille de la Sécurité Publique, de la Défense, et de l'Immigration
Justice Canada
Jean Edmonds, Tower South | Tour Sud
365 Laurier Avenue West | 365 Avenue Laurier Ouest 15th Floor | 15e étage, OTTAWA, ON
K1A 1L1
mailto:mscriven@justice.gc.ca
Telephone | Téléphone (613) 954-1248
Facsimile | Télécopieur (613) 957-7840

» Print

Australia shelves plans to store phone, Internet metadata

Mon, Jun 24 2013

CANBERRA, June 24 (Reuters) - Australia's government on Monday shelved plans to force phone and Internet companies to hold two years of phone call and email data following concerns raised by a parliamentary inquiry into telecommunications interception laws.

The move follows long-running criticism by privacy advocates in Australia, and comes in the aftermath of revelations in the United States, where spy agency contractor Edward Snowden exposed secret U.S. surveillance of vast amounts of Internet data under a programe known as Prism.

The government had wanted phone and Internet companies to hold metadata for two years to help fight criminal activity, but lawmakers on the telecommunications inquiry called for changes.

They said Internet browsing data should be excluded from the plans, and called for greater oversight of government agency access to telecommunications data by the ombudsmen and the Inspector-General of Intelligence and Security.

Attorney-General Mark Dreyfus responded to the inquiry findings by delaying any changes until after the September 14 parliamentary election and only after further consultations.

"The government will not pursue a mandatory data retention regime at this time and will await further advice," Dreyfus said in a statement after the report was tabled.

Conservative opposition lawmakers, who are expected to win power in September, have raised concerns about surveillance of cloud server data stored in the United States, but are still likely to support the new laws in Australia if they take office.

The influential Australian Greens Party, which holds the balance of power in the upper house, said the security and intelligence committee report reflected political and privacy concerns first raised last year about plans to collect and store the telephone and email data of all Australians.

"This report refused to endorse data retention and condemned Government's secretive approach," said Greens communications spokesman Scott Ludlum.

The report did not specifically mention the Prism programme, as its hearings were completed before the Snowden revelations about Prism.

But the inquiry's report did raise concerns about the wide number of Australian government agencies able to access private data, with 293,501 requests made in 2011-12 to access communications data without a warrant. (Reporting by James Grubel; Editing by Ron Popeski)

Thomson Reuters journalists are subject to an Editorial Handbook which requires fair presentation and disclosure of relevant interests.

Emmett, Jamie

s.21(1)(a)
s.21(1)(b)

From: Plunkett, Shawn
Sent: May-31-13 2:21 PM
To: Grigsby, Alexandre
Subject: RE: Paper on lawful access

Thanks. [redacted]

On another note, [redacted]

From: Grigsby, Alexandre
Sent: May-30-13 3:21 PM
To: Cameron, Bud; Plunkett, Shawn; Hamilton, Sharon; Bonvie, Jeff; Dvorkin, Corey; Bradley, Kees
Cc: Hatfield, Adam
Subject: RE: Paper on lawful access

Here's more -- an open letter penned by a number to tech experts in response to the WaPo and NYTimes stories about the FBI's proposed changes to CALEA. Some pretty big names have signed on, including Schneier and Zimmermann.

https://www.cdt.org/files/pdfs/CALEAII-techreport.pdf

From: Cameron, Bud
Sent: Thursday, May 30, 2013 10:19 AM
To: Grigsby, Alexandre; Plunkett, Shawn; Hamilton, Sharon; Bonvie, Jeff; Dvorkin, Corey; Bradley, Kees
Cc: Hatfield, Adam
Subject: RE: Paper on lawful access

[redacted]

From: Grigsby, Alexandre
Sent: May 28, 2013 11:33 AM
To: Plunkett, Shawn; Hamilton, Sharon; Cameron, Bud; Bonvie, Jeff; Dvorkin, Corey; Bradley, Kees
Cc: Hatfield, Adam
Subject: Paper on lawful access

Hi all,

Came across this paper that might be of interest. It's authored by some engineers concerned that mandating backdoors in software for lawful intercept purposes introduces new vulnerabilities into software that will be exploited by non-authorized purposes. Their solution seems to be: "all software has vulnerabilities – just have law enforcement exploit existing vulnerabilities as opposed to creating new ones"

https://www.cs.columbia.edu/~smb/papers/GoingBright.pdf alex

Alexandre Grigsby
Analyst | Analyste
National Cyber Security Directorate | Direction générale de la cybersécurité nationale
Public Safety Canada | Sécurité publique Canada
tel. 613.949.4243
www.publicsafety.gc.ca | www.securitepublique.gc.ca

CALEA II: Risks of Wiretap Modifications to Endpoints

Ben Adida
Collin Anderson
***Annie I. Anton** (Georgia Institute of Technology)*
***Matt Blaze** (University of Pennsylvania)*
***Roger Dingledine** (The Tor Project)*
***Edward W. Felten** (Princeton University)*
***Matthew D. Green** (Johns Hopkins University)*
***J. Alex Halderman** (University of Michigan)*
***David R. Jefferson** (Lawrence Livermore National Laboratory)*
Cullen Jennings
***Susan Landau** (privacyink.org)*
Navroop Mitter
***Peter G. Neumann** (SRI International)*
***Eric Rescorla** (RTFM, Inc.)*
***Fred B. Schneider** (Cornell University)*
***Bruce Schneier** (BT)*
***Hovav Shacham** (University of California, San Diego)*
***Micah Sherr** (Georgetown University)*
***David Wagner** (University of California, Berkeley)*
***Philip Zimmermann** (Silent Circle, LLC)*[1]

17 May 2013

Abstract: The U.S. government is proposing to expand wiretap design laws broadly to Internet services, including voice over Internet protocol (VoIP) services and other peer-to-peer tools that allow communications in real-time directly between individuals. This report explains how mandating wiretap capabilities in endpoints poses serious security risks. Requiring software vendors to build intercept functionality into their products is unwise and will be ineffective, with the result being serious consequences for the economic well-being and national security of the United States.

[1] Affiliations are for identification purposes only. The authors thank the Center for Democracy & Technology for coordinating this effort.

1 Introduction: "Going Dark" and CALEA II

The Washington Post and the New York Times have reported that the U.S. government is considering extending wiretap design laws to cover Internet communications services and software.[2] The Federal Bureau of Investigation argues that ongoing changes in the communications environment are making government electronic surveillance harder, so hard, in fact, that government agents are at risk of "going dark."[3] On technical details, the government is not specific; the FBI has described various aspects of the problem and it appears that its concerns include a variety of Internet-based services that allow voice, video, or text communications in real-time or near real-time. It is clear that the FBI would like policymakers to adopt new legislation requiring some products to be born wiretap-ready or to be modified upon government demand to be wiretap-ready.[4]

This could encompass a wide range of products and services, from instant messaging and chat to Skype to Google Hangouts to Xbox Live. It could include services offered through a variety of means, from stand-alone services to features built into web browser software and social networking sites. The most recent media accounts of the still-secret proposal lack information about the scope of services or companies that would be covered.[5] These stories report that the government seeks 1) authority to fine "companies" that do not comply with wiretap orders,[6] and 2) to expand wiretap obligations to peer-to-peer VoIP services.[7] It is this second aspect of the proposal that is the focus of this report: mandated wiretap modifications to endpoint software and services that allow direct, peer-to-peer communication.[8]

In contrast to the view that the government is going dark, there is a contrary view that technological changes have made available to the government vastly more information than ever before.[9] However, in our analysis we have not attempted to assess the merits of the FBI's characterization of the problem. Instead, we have chosen to focus entirely on the technical issues associated with one aspect of the proposed solution: the mandating of wiretap capabilities in endpoint systems. This report examines the properties of wiretapping mandates on endpoint systems and outlines the technical risks and implications of deploying endpoint systems that provide surreptitious access to communications in real-time or near real-time. We conclude that deployment of an intercept capability in endpoint communications services, systems and applications poses serious security risks.

[2] Ellen Nakashima, "Panel seeks to fine tech companies for noncompliance with wiretap orders," Washington Post, (April 28, 2013), *available at:* http://articles.washingtonpost.com/2013-04-28/world/38885216_1_wiretap-proposal-companies; Charlie Savage, "U.S. Is Weighing Wide Overhaul of Wiretap Laws," New York Times, (May 8, 2013), *available at:* http://www.nytimes.com/2013/05/08/us/politics/obama-may-back-fbi-plan-to-wiretap-web-users.html.

[3] Valerie Caproni, Statement before the House Judiciary Committee, Subcommittee on Crime, Terrorism, and Homeland Security, (February 17, 2011), *available at:* https://www.fbi.gov/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies. The FBI testimony and other government materials — see: http://info.publicintelligence.net/FBI-GoingDark.pdf (FBI Situational Information Report on technical mechanisms that frustrate surveillance efforts) and https://www.eff.org/document/ice-documents-released-response-calea-foia (Customs and Border Protection FOIA response detailing instances where surveillance has been frustrated) — make it clear that "going dark" encompasses a variety of issues, including disputes about the wording of government orders, isolated failures of otherwise sufficient interception systems, dissatisfaction with government-developed industry standards, and government claims that some companies already covered by interception design mandates have not complied.

[4] *See:* Declan McCullagh, "FBI: We need wiretap-ready Web sites – now," CNET, (May 4, 2012) *available at:* http://news.cnet.com/8301-1009_3-57428067-83/fbi-we-need-wiretap-ready-web-sites-now/.

[5] *See:* Nakashima and Savage, fn. 2.

[6] Under current law, wiretap orders can be issued not only to any provider of wire or electronic communications service but also to any "landlord, custodian, or other person." 18 U.S.C. § 2518(4). The FBI apparently has in mind some subcategory of these entities.

[7] *See:* Savage, fn. 2 ("The 1994 law would be expanded to cover peer-to-peer voice-over-Internet protocol.")

[8] We also expect to have technical objections to the proposal that would enhance penalties for inadequate response to wiretap orders, but the specifics of that part of the proposal remain vague.

[9] *See*, e.g., Peter Swire, Kenesa Ahmad, "'Going Dark' Versus a 'Golden Age for Surveillance'" (Nov. 28, 2011) (arguing that we live in a "golden age of surveillance" as both the overall volume of information available to the government has greatly expanded and entire new categories of electronic data are being generated) https://www.cdt.org/blogs/2811going-dark-versus-golden-age-surveillance.

2 Technical Background: Monitoring Communications

In the United States, the Communications Assistance for Law Enforcement Act (CALEA) currently requires telecommunications service providers to design their networks to ensure that law enforcement and national security officials can perform lawfully authorized electronic surveillance at service provider premises.[10] In 2005 the Federal Communications Commission (FCC) adopted a rule extending CALEA obligations to facilities-based broadband Internet-service providers (such as cable companies) and interconnected VoIP services — that is, VoIP that can send or receive calls into the public switched telephone network (PSTN).

Traditional telecommunications involved a limited number of service providers offering access services through a limited number of switches. On the public telephone network, the customer had a relatively dumb handset that was connected to a "central switch." This switch controlled call setup and all content flowed through the switch to the recipient. In classical analog phone systems as well as in modern mobile systems, tapping can be performed at the switch without any interaction with the endpoint.

Even as the telephone network transitioned to digital carriage, and as companies began offering broadband Internet access that carried a wide range of services, including voice, all the call setup information and all the content from a subscriber using a particular access point (DSL, cable, wireless) was fed through a facility serving a limited geographical area (a switch or, in the case of cable, the headend or CMTS) that allowed access to the full communications stream. The government, when tapping a particular person's data stream, increasingly had to sort through an array of services (real-time voice calls, email, chat, web browsing, attachments to email), but it could still access these at the "last mile" facility (although some may be encrypted).

Now, however, users are increasingly mobile and use services from a variety of service providers at an increasingly large number of access points, making it more challenging to predict how a user will be connected at a given moment. As we understand the government's problem, the geographically-limited routing facilities that had previously been the focal point of interception no longer provide access to all a target's communications.

In response, it seems the government has two options:

- To wiretap at points where communications can be accessed in a centralized manner; or,
- To access communications at the end-points, by controlling the software or hardware of the endpoints.

Sometimes, there is no centralized point where content is accessible. For example, most VoIP systems have centralized call setup but do not centralize carriage of content. For instance, in a typical VoIP system using the protocol known as SIP,[11] while a centralized system controls call setup, the communications content flows directly between the endpoints ("peer-to-peer"). If an individual is using a fixed access point (such as residential broadband), the content can still be captured at the local switch (the "headend" in the case of cable broadband). However, once a person moves, for example using different Wi-Fi hotspots, it becomes harder for government wiretappers to keep up (though it may be possible to gather pen register information — call routing metadata — at the service provider's central facility).

2.1 Monitoring at the Center

With some Internet services, there is a centralized point where communications are aggregated or controlled. For example, in some VoIP services, the service provider operates a central signaling service that provides:

- Access to pen register information (i.e., who is calling whom).
- The ability to redirect or duplicate the content stream to a location where it can be monitored.

[10] Throughout the remainder of this report, we use "CALEA I" to refer to existing CALEA obligations and "CALEA II" for what we believe to be currently proposed changes.

[11] Rosenberg, J., Schulzrinne, H., Camarillo, G., *et al.*, "SIP: Session Initiation Protocol," IETF, RFC 3261, June 2002, *available at:* https://www.ietf.org/rfc/rfc3261.txt.

Of course, if the traffic is end-to-end encrypted, access to the call content is of limited utility. With older VoIP systems,[12] the signaling server generally had access to the keying material, but modern systems[13] are designed to prevent centralization of keying material for security reasons.[14] With such systems, any effort to substitute the keying material of the intercept service in place of the users' keying material would be detectable by the user and, depending on the system results in the call not connecting. This is to say that only in relatively outdated VoIP systems will central monitoring be feasible. Modern peer-to-peer services don't have such central points at which content can be monitored; to mandate that they do so would require substantial re-engineering that would fundamentally change the service and be expensive to implement, maintain and operate.

2.2 Monitoring at the Endpoint

These technical limitations of centralized monitoring have led to suggestions that instead monitoring should be provided at the endpoints. That is, end-user software should be modified to support monitoring. When monitoring is desired, the feature is activated and the software starts delivering copies of its keys, traffic, or both to some monitoring point. This may or may not be achievable in a way that is undetectable to the user. For example, a Chinese-localized version of the Skype software, called TOM-Skype, used by over 90 million Chinese people has clearly been modified such that when a user sends certain terms during chat sessions, those chat messages are censored (i.e., never delivered to the intended recipient) and/or subject to surveillance (i.e., delivered to a TOM-Skype server, and possibly to the Chinese government).[15]

3 A Wiretap Mandate on Endpoints Will Present Serious Security Risks

Security is a fundamental requirement of communications systems. Commerce, government and interpersonal relationships all rely upon secure communications. However, we know that our communications systems today are under attack, with a particular focus on endpoint systems. Government information and communications systems, including law enforcement and national security systems, have been targeted,[16] as have corporate systems, including the systems of communications service providers.[17] It is in this context that we raise our concern: A wiretap design mandate on communications tools is, plainly put, an opportunity for increased exploitation. As we explain below, extending CALEA to endpoint software and devices will make communications systems, products and services even more vulnerable.

3.1 Vulnerabilities That Are Hidden in Design and Operation Pose Serious Security Risks

All networks, software, and communication tools that support "lawful intercept" include features that are designed to breach the confidentiality of communications without detection by any party involved in the communication. When parties communicate using services with such features, there is an increased likelihood that an unauthorized and/or malicious adversary with the right technical knowledge and access to the system

[12] For example, those that use SDP Security Descriptions. *See:* Andreasen, F., Baugher, M., Wing, D., "Session Description Protocol (SDP) Security Descriptions for Media Streams," IETF, RFC 4568, July 2006, *available at:* https://tools.ietf.org/rfc/rfc4568.txt.

[13] For example, ZRTP and DTLS-SRTP. *See:* Zimmermann, P., Johnston, A., Callas, J., "ZRTP: Media Path Key Agreement for Unicast Secure RTP," IETF, RFC 6189, April 2011, *available at:* https://tools.ietf.org/rfc/rfc6189.txt; McGrew, D., Rescorla, E., "Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)," IETF, RFC 5764, May 2010, *available at:* https://tools.ietf.org/rfc/rfc5764.txt.

[14] The "signaling server" is the directory server that handles call setup between the two endpoints. "Keying material" refers to the encryption keys needed to render the call content.

[15] Vernon Silver, "Cracking China's Skype Surveillance Software," Bloomberg BusinessWeek (March 8, 2013), *available at:* http://www.businessweek.com/articles/2013-03-08/skypes-been-hijacked-in-china-and-microsoft-is-o-dot-k-dot-with-it; Jeffrey Knockel, Greg Wiseman, "Chat Program Censorship and Surveillance in China: Tracking TOM-Skype and Sina UC," Boston Freedom in Online Communications Day (BFOC 2013), Boston, Massachusetts (March 2013), *available at:* http://cs.unm.edu/~jeffk/publications/bfoc2013censorship-slides.pdf.

[16] James Andrew Lewis, "Significant Cyber Incidents Since 2006," Center for Strategic and International Studies (November 20, 2012), *available at:* http://csis.org/publication/cyber-events-2006.

[17] David Drummond, "A new approach to China," Official Google Blog (January 12, 2010), *available at:* http://googleblog.blogspot.com/2010/01/new-approach-to-china.html (describing a sophisticated and targeted attack against Google).

could capture communications contents without detection. The general nature of CALEA-style mandates and the necessarily clandestine nature of intercept mechanisms increase security risks further.

The cleverest and most dangerous cyber-attackers are those who are able to not only compromise a system but also to evade detection. That is also precisely the objective of a government surveillance solution: to compromise communications without detection. We know that communications networks and services are increasingly the subject of exploitation, often because of unintended and not very well-hidden vulnerabilities. Wiretap capabilities can be uniquely dangerous precisely because they are developed to be hidden, both in design and in application. Wiretaps are designed to be kept secret from both the parties involved in the communication and also from anyone else that does not have a "need to know" in order to execute the tap (including employees of the service provider who are on the alert for system compromises).[18] This requirement for obscurity increases the security risks further because it increases the possibility that a malicious communications intercept could be effectuated with low risk of discovery.[19]

3.2 There Is a High Risk That Wiretap-Modified Endpoints Will Be Vulnerable

3.2.1 Building Wiretap Capability in Endpoint Software Is Dangerous

In a traditional CALEA monitoring setting, the *vendor* builds CALEA access into key network components used by a network operator and the *network operator* performs the wiretap. That is, the access only occurs with the operators' cooperation, and the operators are ultimately in control of their own systems. Further, CALEA I mandates focused on a relative handful of telecommunications network operators who have a long history of cooperating with the government to provide access and have substantial experience and capabilities for monitoring and securing their networks. These service providers have procedures in place that allow trusted and carefully supervised employees to initiate wiretaps inside their networks, and they maintain security operations that are constantly monitoring for unauthorized access.

By contrast, in a system where the endpoints facilitate lawful intercept, the software developer builds the wiretap capability into end user software but the network operator does not control access. (Nor, of course, does the end user.)

The government and the developer have two choices:

- The developer designs the software, product or service so that the developer itself controls the access feature and individually responds to each governmental request for access, making a case-by-case decision about the legal validity of each such request.
- The developer provides the government or some intermediary with the requisite capabilities to access user communications without any further cooperation from the developer.

Neither of these solutions is satisfactory. In the first case, the developer not only needs to have a full-time legal department to respond to requests, but it also runs the risk that rogue employees will surreptitiously activate the intercept feature to access user communications.[20] Therefore, the developer, which may be offering its communications tool for free, would have to establish a systemic security program. It would have to adopt new standards for personnel security: to protect all information about development and operation of the intercept feature, to prevent misuse of the feature by employees, and to ensure that employees preserve the confidentiality of each wiretap in order to protect ongoing investigations. It would have to harden its own network with internal monitoring to prevent employee abuse and with outward facing measures to ensure that an outsider does not

[18] For a technical definition of wiretapping, see Section 3 of RFC 2804: Internet Architecture Board, Internet Engineering Steering Group, "IETF Policy on Wiretapping", IETF, RFC 2804, May 2000, *available at:* https://tools.ietf.org/rfc/rfc2804.txt.

[19] *See*, e.g., Vassilis Prevelakis and Diomidis Spinellis, "The Athens Affair", IEEE Spectrum, 44:7, July 2007, *available at:* http://spectrum.ieee.org/telecom/security/the-athens-affair/.

[20] Rogue insider employees may abuse their privileges and gain unauthorized access to sensitive data. *See*, e.g., Adrian Chen, "Google Engineer Stalked Teens, Spied on Chats," Gawker, (Sep. 14, 2010), *available at:* http://gawker.com/5637234/.

take over the surveillance feature or gain access to it for counter-intelligence purposes.[21] This level of security and control is simply not feasible for any but the largest vendors. Consequently, developer controlled intercept capabilities are likely to be highly insecure.

The alternative approach, providing unmediated access to government agencies, is worse. In the U.S. alone, there are many law enforcement agencies at the federal, state, and local level authorized to carry out electronic surveillance.[22] In the context of CALEA I, it is difficult for the employees of these agencies to effectuate a wiretap without the cooperation of the service provider. In the world of CALEA II, employees at each of these agencies would potentially have access to the functioning of the intercept capability, which they could then execute without the cooperation of the developer or the network operator. There would be no way for the developer or the network operator to audit or log the uses of the feature (and, of course, if the feature were well-designed to prevent compromise of investigations, it would be very difficult to know when it was activated).

This eavesdropping capability will not be limited to services for personal and commercial use. Increasingly, the U.S. government, including law enforcement and national security entities, uses commodity software and hardware. Moreover, because the same software is delivered throughout a global market, once a developer has provided access to one government, it will be under enormous pressure to provide access to many governments. The result will be endpoints that are vulnerable to monitoring by hundreds of governments, many of which have adversarial relationships with the United States and with U.S. companies and some of which suffer from high levels of corruption or close relationships with criminal elements. In short, requiring that developers build monitoring capability into end-user software and equipment poses a threat to the economic well-being and national security of the United States.

3.2.2 It Will Not Be Possible to Block Non-Compliant Implementations

The foregoing presumes that the intercept feature must be kept secret.[23] However, many modern communication software systems are built on open standards, open source implementations, or both. For instance, two of the most popular web browsers — Google's Chrome and Mozilla's Firefox — are open source programs that are developing secure communication systems based on the IETF/W3C suite of standards known as WebRTC.[24] Many open instant messaging systems support the popular Off-the-Record (OTR)[25] open source secure communications system. In such systems, it will not be possible to hide the introduction and functioning of intercept capabilities. This could compromise the effectiveness of the surveillance function, its security or both.

Furthermore, for the many products that are open source, it will be trivial for someone to build and redistribute software without the monitoring capability. This sort of "fork" is not exceptional, but rather common. The nature of Open Source software is that people take it, make small modifications, and redistribute. To provide two especially relevant examples, Iron[26] is a fork of Google Chrome that focuses on improved privacy, and the Tor Project[27] maintains its own version of Firefox that is designed to allow private anonymous communications on the Internet under extremely adversarial conditions, such as dissident users in Iran or China. If U.S. software vendors are forced to introduce wiretap capability, it seems certain that there will be non-U.S. forks of popular

[21] Kenneth Corbin, "'Aurora' Cyber Attackers Were Really Running Counter-Intelligence," CIO, (April 22, 2013), *available at:* http://www.cio.com/article/732122/_Aurora_Cyber_Attackers_Were_Really_Running_Counter_Intelligence.

[22] Forty-seven states (including the District of Columbia and the Virgin Islands) have adopted statutes authorizing law enforcement agencies at the state level and in many cases the local level to carry out wiretaps. *See*: "Annual Wiretap Report for 2011," U.S. Administrative Office of the Courts, (2012), Table 1, *available at:* http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2011/Table1.pdf.

[23] CALEA I favored the use of published standards for wiretap capabilities to help protect against government overreaching or security vulnerabilities in the implementation of the statutory mandates; it did so by granting a safe harbor in using published standards. CALEA I could do this without loss of security because *service providers* executed wiretaps. Under CALEA II, given the diversity of services covered, it may not be possible to have standardized intercept capabilities.

[24] *See:* WebRTC, http://www.webrtc.org/.

[25] *See:* Off-the-Record Messaging, http://www.cypherpunks.ca/otr/.

[26] *See:* SRWare Iron: The Browser of the future, https://www.srware.net/en/software_srware_iron.php.

[27] *See:* The Tor Project, https://www.torproject.org/.

open source communications packages that do not allow such access. Moreover, this likelihood of non-compliant forks being developed is not limited to open source software, but also potentially relevant to proprietary, closed-source products, albeit with more effort by the fork's developers. For instance, just as it is possible to "jailbreak" proprietary phone operating system software by downloading a program that "tweaks" the software, disabling monitoring capability in wiretap-modified software may be as easy as clicking a link and running a small program that can disable intercept functionality.

It is important to understand that because these systems are built on open standards, modified software *without lawful intercept capability* will be able to interoperate with systems with the intercept capability and with unmodified systems. To take an extreme example, say that all U.S.-made Web browsers support CALEA II, thus allowing wiretapping of any WebRTC session. Two users who desire unmonitorable communications need only download secure foreign-made versions of one of the major browsers and they can make secure calls using *exactly the same infrastructure* as those that must use compliant versions. We should expect that any user who is concerned about monitoring — including many potential monitoring targets — would obtain and use an unmonitorable version of a given product or service. Ironically, then, potential terrorists may easily be able to use stronger security than the U.S. government, which is less likely to install non-U.S. forks of these programs.

4 Conclusion

The FBI's desire to expand CALEA mandates amounts to developing for our adversaries capabilities that they may not have the competence, access, or resources to develop on their own. In that sense, the endpoint wiretap mandate of CALEA II may lower the already low barriers to successful cybersecurity attacks. We believe that on balance mandating that endpoint software vendors build intercept functionality into their products will be much more costly to personal, economic and governmental security overall than the risks associated with *not* being able to wiretap all communications.

© IEEE Security & Privacy 11:1, Jan/Feb 2013, http://dx.doi.org/10.1109/MSP.2012.138

Going Bright: Wiretapping without Weakening Communications Infrastructure

Steven M. Bellovin | Columbia University
Matt Blaze and Sandy Clark | University of Pennsylvania
Susan Landau | Privacy Ink

Mobile IP-based communications and changes in technologies have been a subject of concern for law enforcement, which seeks to extend current wiretap design requirements for digital voice networks. Such an extension would create considerable security risks as well as seriously harm innovation. Exploitation of naturally occurring bugs in the platforms being used by targets may be a better alternative.

For law enforcement wiretaps, this is the best of times and the worst of times. Tracking suspects through transactional data vastly simplifies investigators' efforts. Yet accessing communications content through traditional means could be getting harder. Because of peer-to-peer communication methods, encryption, and service providers located outside the US, law enforcement says its ability to execute legally authorized wiretaps is becoming increasingly problematic. The US Federal Bureau of Investigation (FBI) claims its wiretapping capability is "going dark" (http://judiciary.house.gov/hearings/hear_02172011.html).

Law enforcement's preferred solution? Since 2010, the FBI has advocated expanding the scope of the Communications Assistance for Law Enforcement Act (CALEA), a 1994 law that requires that switches in digital telephone networks be built wiretap enabled. The FBI wants to extend such requirements to IP-based communications.

CALEA and the Internet

CALEA was controversial because it introduced new security risks into the voice telephone network; indeed, there have been several publicly known cases of telephone switches being compromised through their wiretap interfaces. This article is primarily focused on the issues associated with CALEA if it were to be extended to emerging Internet-based services.

There are several possible policy options for wiretapping as these trends continue. These include maintaining the status quo, which would increasingly limit content wiretaps to (decreasingly relevant) switched telephone networks.

Law enforcement could increasingly rely on (non-content) communications records, which can reveal a great deal of information about a target's location, contacts, movement, and so on.[1] The legal and privacy implications of widespread use of communications records by law enforcement are a matter of some controversy, however, and at scale, it's difficult to ensure that information about innocent third parties won't find its way into law enforcement databases along with the records of suspects.

But there is yet another possibility. As the CALEA approach has become less viable (and more dangerous to emerging infrastructure), targeted interception approaches—ones that don't entail the risks and costs of nationally mandated wiretap interfaces—have become increasingly practical. One approach is to leverage the fact that targets' communications devices in modern networks are virtually always built on complex software platforms. Continuing technical access to authorized wiretaps can be achieved—without expanding CALEA—by exploiting naturally occurring weaknesses in subjects' devices, enabling law enforcement to install surreptitious interception software at a target

1540-7993/13/$31.00 © 2013 IEEE

endpoint as required. Many such weaknesses are *0-day vulnerabilities*, ones that might be completely unknown to others and for which no vendor fix exists. (Conceptually, the bug is discovered on day zero and reported and patched sometime later.)

Communication devices in modern networks are essentially always built on complex software platforms. Due to the inexact nature of software development, all complex programs contain inadvertent vulnerabilities. Without requiring any explicit wiretap support in the network or any compromise of nontargeted devices, law enforcement can exploit software vulnerabilities on end devices to facilitate interception. The US law enforcement community can fund a laboratory to develop targeted interception tools that take advantage of such vulnerabilities, an idea proposed in the 1996 National Research Council report on cryptography.[2] (Note, however, that the FBI has a role in crime prevention, but it isn't tasked with securing communications or communications infrastructure.[3]) Such an approach isn't without its own policy concerns and risks, yet it's far more protective of national communications security and privacy than other proposed alternatives, including and especially CALEA-type design mandates.

Some work in this direction is already in progress by law enforcement. As has been reported elsewhere,[4,5] the FBI has established a Domestic Communications Assistance Center (DCAC) to tackle the technical side of the "going dark" problem. In 2012, the FBI requested US$15 million to fund this lab. We believe that approaches such as expanding DCAC's efforts—and not expanding CALEA's scope—are effectively the only path to facilitating legally authorized wiretapping that doesn't also undermine the security of the US communications infrastructure.

We conclude that

- any past success network-based interception schemes such as CALEA may have enjoyed in the telephony domain won't translate to similar success for Internet-based services;
- many emerging communications services are inherently interceptable by passive means;
- requiring additional centralized interception capabilities will be unnecessarily redundant and will introduce increasingly more serious security risks to infrastructure while being increasingly less effective in producing useful evidence for law enforcement;
- law enforcement development of a sufficiently broad range of targeted passive and endpoint-based interception tools to meet ongoing wiretap needs is technically and economically feasible;
- law enforcement's use of passive interception and targeted vulnerability exploitation tools creates fewer security risks for nontargets and critical infrastructure than do design mandates for wiretap interfaces; and
- moving forward, targeted exploitation solutions are likely to be the only viable approaches for providing law enforcement with reliable interception capabilities against modern platforms, even if wiretap interfaces in infrastructure were mandated.

In particular, it is critical for national security that communications software and systems be designed to be as secure as possible against attack. Deliberate backdoors—whether by way of CALEA or through hidden "lawful intercept" access features included by software vendors—inherently make systems more vulnerable; worse yet, all users, not just wiretap targets, suffer the increased exposure. However, the absence of explicit lawful intercept backdoors need not preclude law enforcement access when it's required, as we'll discuss later.

Note that our discussion is US focused: CALEA is a US law. However, the 1994 US solution of building wiretapping capabilities into switches was rapidly taken up in many other parts of the world under the generic name "lawful intercept." The security risks inherent in extending CALEA to the Internet are security risks facing any nation contemplating similar approaches to a CALEA-type regime for IP-based networks. Thus, while our context is local, our analysis is global in its applicability.

Wiretapping: The Present Situation

By requiring that communications providers include wiretapping capabilities within switching mechanisms, CALEA was a surprising development on the regulatory front.

For a quarter of a century, the process under which authorized wiretaps were done in the US was straightforward. Two laws, the 1968 Title III of the Omnibus Crime Control and Safe Streets Act (for criminal investigations) and the 1978 Foreign Intelligence Surveillance Act (FISA; for foreign intelligence cases), governed wiretap order applications. Once a judge granted an order, the wiretap could be installed.

The divestiture of AT&T meant that instead of a single monopoly handling both telephones and service, many more product and service providers emerged, along with increasing innovation in communication technologies. Law enforcement found itself thwarted in carrying out some legally authorized wiretaps. (Because we focus on possible extensions to CALEA and the harm they represent, we don't discuss the much richer surveillance capabilities now available to law enforcement—the plethora of communications, the fact that these frequently reveal location, and so forth—that provide a different situation than when Title III and FISA were passed.) Their solution was CALEA.

CALEA was implemented through an interface standard developed by the Telephone Industry Association in consultation with law enforcement.[6] This standard pleased no one: civil liberties groups wanted greater privacy protections than the standard provided, industry wanted greater clarity on the standard's technical requirements, and law enforcement wanted greater surveillance capabilities than were included. Several lawsuits and court rulings ensued, but by 2002, the requirements for CALEA compliance finally solidified. Although nobody was fully satisfied, CALEA became the dominant mechanism for implementing telephone wiretaps.

The FBI soon raised a new concern: Voice over IP (VoIP). IP-based communications are often peer to peer, and the CALEA model of tapping at the switch doesn't easily fit in with that. The Federal Communications Commission (FCC) and a federal appeals court cut this Gordian knot by deciding that CALEA would apply to facilities-based broadband, systems with wired lines (or wireless channels) to the end user. These communications systems are centralized, just like the public switched telephone network (PSTN), and applying CALEA-type solutions isn't especially technically difficult.

Innovation rarely pauses in technology. Because of a combination of increasing levels of peer-to-peer communications and encryption, along with such changes as overseas communications providers offering services in the US (creating difficulties when a wiretap is needed), law enforcement is again facing difficulties. What CALEA extensions the FBI actually seeks remain unclear. There have been various news reports since autumn 2010, but as of this writing, no bill has been produced.

CALEA worked for a reason that no one fully articulated: circuit-switched telephones (and cellphones) were the primary mode of communication. That era is now ending. Efforts to extend CALEA-type controls to the nearly infinite number of communications devices and applications cannot be effective.

The CALEA "Solution"

CALEA was intended to address a specific and rather unique set of technological circumstances brought about by incremental advances in voice telephone technology. Prior to CALEA, there was neither a mandate requiring telephone companies to design technology facilitating wiretapping nor a standard telephone wiretapping interface. Instead, wiretaps relied on local loops, the pairs of wires between a local telephone office and its subscribers. Law-enforcement agencies developed local-loop tapping technology, which it deployed by connecting to subscriber wire pairs. Sometimes law enforcement deployed taps with assistance from the carrier; sometimes it did it on its own.

Tapping technology was simple and largely unchanging because telephone subscriber loop technology was, at least until the 1990s, simple and relatively unchanging. Carrying analog voice and signaling, the telephone local loop remained essentially the same for half a century. Tapping a telephone was a relatively simple matter of gaining physical access to the target's pair of wires and recording the electrical signals and voice audio the wires carried.

By the 1990s, two new subscriber loop technologies had emerged that weren't directly compatible with traditional analog wiretapping techniques. ISDN employed a pair of wires between the telephone central office and the subscriber but used digital signals and digitally encoded audio, which can require far more sophisticated technology for third-party interception. The other new technology was wireless cellular, in which the local loop was replaced with a two-way radio link, allowing the subscriber to move freely about the coverage area.

It's important to note that while ISDN and cellular services might have radically altered the local loop between the telephone company and the subscriber, these technologies did relatively little to alter telephony's centralized architecture. The basic service for both ISDN and cellular was and is voice calls linked to the PSTN. Subscribers still obtain their service from a single one of relatively few providers, which are themselves highly regulated by local franchises or hold federal licenses for part of the limited wireless spectrum.

Current Internet service architectures are far more complex than the telephone networks of the 1990s. Link technologies, including cable, fiber optics, DSL, and several forms of cellular wireless, were widely implemented. VoIP services, of which there are various varieties, have added a third local loop technology; it adds the challenge of separating the infrastructure provider from the physical plant provider, greatly complicating the wiretapping effort.[7]

Currently relatively few entities have had to comply with the current CALEA voice wiretap interface mandates. Those that do provide a common basic service:

voice calls. Compared with typical Internet infrastructure, switches for voice calls—the primary devices required to have CALEA interfaces—are very expensive, amortized over long periods, and relatively slow to change. This means that the costs, innovation burden, and security risks associated with implementing CALEA for voice telephony, while not trivial, are both somewhat calculable and relatively manageable. Yet even in the domain of voice telephony, CALEA is far from a win-win solution for wiretapping. Still, for IP-based communications, CALEA represents a lose-lose situation.

CALEA Insecurities

CALEA requires that a deliberate security weakness—the wiretap interface and control system—be architected into the switches of a communications network. In 2000, the Internet Engineering Task Force observed that, "Experience shows that if a vulnerability exists in a security system, it is likely that someone will take advantage of it sooner or later."[8] That situation has come to pass for CALEA-type interfaces.

The story of the 10-month interception of the most senior officials of the Greek government in 2004 to 2005 using a CALEA-type interface that had been surreptitiously turned on is well known.[9] Less well known is the 10-year wiretapping of 6,000 Italians that occurred through Telecom Italia,[10] the targets of which included political figures, judges, referees, and celebrities. The US has not been immune. Examinations by the National Security Agency (NSA) of CALEA-compliant switches to be sold to the Department of Defense found vulnerabilities in the CALEA implementation in every single switch examined.[11]

CALEA-like interfaces are, by definition, designed for surreptitious eavesdropping. They're intentional backdoors and thus both easier to exploit and more damaging when penetrated. The recent massive increase in cyberexploitation—theft of data from governments and companies around the world—adds to the concern about the vulnerabilities created through CALEA-type architectures. Furthermore, there are subtle but essential differences between the architecture of the PSTN and those of contemporary and emerging Internet-based services. These make generalized wiretap interfaces for Internet communications far more technically difficult, complex, and economically burdensome than they are in traditional telephony.

It's certainly true that unauthorized remote wiretaps can be implemented by using other forms of remote access including craft interfaces, which are used to test installations, check reported faults, and so on. But such remote accesses are much more difficult to conduct surreptitiously because, unlike CALEA, they're deliberately designed to be logged and to trigger other, semiautomatic changes within the system. In contrast, CALEA interfaces are specifically intended for surreptitious wiretapping. By design, indicia of such taps are carefully restricted and invisible outside the CALEA control console. They thus provide a more attractive attack surface for exploitation by criminals and foreign intelligence services.

It's far from clear that CALEA for telephony has successfully balanced law enforcement requirements for surveillance access with the broader goal of preventing illicit access to critical infrastructure by criminals and foreign governments. But even if we assume that CALEA for telephony has been on the whole a success, the conditions that might have made it so aren't present in the Internet services for which the government seeks to apply the same approach. Communications infrastructure lasts a long time. Given increasing cyber-exploitation efforts, switch longevity makes the security concerns even more trenchant.

The CALEA Problem

Internet-based services have very different technical and economic properties from traditional telephony. These make the CALEA approach far less attractive for the Internet while simultaneously introducing considerably more risk.

There are several reasons that lawful intercept mechanisms in all communications software are an exceedingly bad idea. The most obvious is the risk: the more code in an application, the more likely it is to have bugs. By definition, lawful intercept code is an engineered—though nominally controlled—vulnerability; a flaw in it exposes the precise sort of access many attackers will want. Even if the intercept code does not itself offer vulnerabilities, its mere existence simplifies the attackers' efforts (witness what happened in Athens and Italy).

The Internet services the government seeks to tap are provided by a large number of entities operating on ordinary computers that are architecturally, effectively ordinary end points. In contrast, on the PSTN, telephony services are provided by large, centralized switching systems operated by a small number of carriers. This architectural difference underlies the vastly greater pace of technology development in Internet services compared with the telephone network.

On the Internet, any node with sufficient bandwidth can act as a service provider. This has led to innovations that a centralized, slow-moving company wouldn't do. The Web itself was invented at a physics laboratory, not by ISPs. Skype, which provides telephone-style voice service Internet connections, doesn't even use central servers; it's a distributed, peer-to-peer network.

To tap Internet applications in the manner of CALEA, then, requires wiretap interfaces in many widely distributed nodes, rather than a few centralized ones. It imposes design constraints on a large number of service providers around the world, rather than a few domestic phone companies. Requiring lawful intercept interfaces in all Internet communications services and software is simply untenable.

Especially early in their life cycles, Internet-based services tend to be lightweight, inexpensive, rapidly changing, and far more reliant on general-purpose software platforms than are the slow-moving of traditional telephony. Thus the highly diverse and dynamic nature of Internet-based services makes the implementation of any kind of standardized wiretap interface considerably more architecturally disruptive than it has been in the PSTN's switched voice telephony environment. A wiretap interface would have to be integrated over a wide range of often quickly deployed and poorly debugged services and then reimplemented every time a new service is introduced or a software architecture changes. This would prove an expensive burden on the small start-ups that drive online innovation.

Worse, many new services, especially those that rely on a peer-to-peer architecture for routing content between users, simply can't be intercepted via the centralized CALEA model. For these services, no design mandate, short of outlawing the decentralized routing scheme on which the Internet is built, can reliably capture all the traffic law enforcement might seek to intercept. Mandating centralized wiretap capabilities in these services would not only be disruptive to innovation but would also fail to deliver meaningful benefit to law enforcement.

Finally, expanding the number of CALEA-like interfaces in the network would create great insecurity. The vulnerabilities in every CALEA-compliant switch tested by the NSA show how hard it is to get the interception technology correct. Those switches were designed by large service providers working over a relatively long period of time. The difficulty of debugging and testing software to make Internet services secure is a largely unsolved problem, especially at the pace of "Internet time"; requirements for wiretap interfaces would make securing new services significantly more difficult.

Wiretapping by Compromising the Target

Suppose that the FBI were to use vulnerability-based solutions for its targeted Internet intercepts. How would this be done? What is necessary to enable it to happen?

Modern computing and communications devices suffer from an essentially unlimited number of security vulnerabilities. Furthermore, as the widespread proliferation of botnets and other criminal exploitation tools demonstrates, it's easy to exploit these vulnerabilities and gain control over an unwitting user's entire platform and virtually impossible for end users to defend against such attacks. Law enforcement can (and, to a certain extent, already does) exploit this.

However, there are additional requirements for law enforcement exploitation tools beyond those employed by criminals who compromise computers to create botnets or steal private data. Cybercriminal tools generally focus on targets of opportunity, but law enforcement will have specific targets on which to focus. This will require specialized interception tools that work well above the "probabilistic" standard of typical criminal exploits. In particular, tools must have a very high chance of successfully compromising the target without risk of alerting the target. Furthermore, the compromise tool can't risk disrupting a target's computer environment—or anyone else's. Finally, investigators must be able to rapidly determine whether their tools have successfully compromised their target's hardware, must be able to manage it during the intercept period, and must be able to "clean up" once a wiretap has ended.

There are four primary components to any law enforcement tool that exploits target endpoint vulnerabilities: selection or discovery of an appropriate underlying vulnerability, installation mechanisms, mechanisms for obtaining access to the communications being targeted, and ways to send captured data back to the responsible investigators. All are situation-dependent. Developing usable, specialized attack tools to accomplish these tasks would be the core mission of a vulnerability exploitation lab. These tools would generally need to be developed and tested by the government well in advance of their use against any particular target.

Consider a hypothetical example: a wiretap target is using an encrypted communication system we'll call CommApp. If CommApp itself is known to have a remotely exploitable vulnerability (one in which carefully formed messages sent to it over the network can compromise the application), the government can use this directly to install its wiretapping code in the application. In this case, the government's compromise tool for CommApp would have to craft an attack message and deliver it over the network when CommApp is running.

If there are no exploitable vulnerabilities in CommApp itself, the problem becomes twofold: system penetration and application penetration. Both of these are classic problems well known to the security community. For the former, the FBI would have to exploit a vulnerability in any other application used by the target. There is a core of very complex—and hence inherently likely to be vulnerable—software used in most platforms; for computers, this core includes Web browsers, email applications, word processors, spreadsheets, PDF and photo viewing interfaces, and so on. An appropriate vulnerability would be one in which opening a specially crafted file with the vulnerable application allows attack code to be installed in the target's platform. Such vulnerabilities are very common in complex applications. A penetration, then, would involve arranging for the target's computer to open an attack file with the vulnerable application, either through automated means over the network or by subterfuge.[12]

In the (very) rare cases where no remote exploitation is possible, a "black bag job"—a legally authorized surreptitious physical break-in—might be performed to install the exploit code directly on the target's device. This has been done in the past.[13,14]

Once the system is penetrated by running the FBI's code, the exploitation must gain access to the intended communication. In our example, CommApp itself could be modified. The simplest modification would be one that leaked the cryptographic keys, but there are more complex modifications, such as capturing the plaintext voice, that would also work. An alternative approach would be to employ generic modules to capture microphone input, speaker output, and so on.

The central problem in our hypothetical example is surreptitiously exfiltrating the captured content back to the FBI. For content such as text messages, the volume of data is typically low enough that any excess traffic won't disturb a broadband connection. Voice is more difficult, especially on cellphones, which have relatively limited battery and transmission capacity. Sending the captured traffic at low speed over time can avoid a noticeable spike in traffic volume. Alternatively, the exploit code might disable encryption or weaken or leak the session encryption keys, allowing intercepted content to be captured in real time by conventional interception techniques without consuming extra bandwidth.

Maintaining an exploitation development capability involves four major ongoing tasks:

- developing and maintaining a library of penetrations techniques for major operating systems and applications;
- developing and maintaining input and output capture techniques;
- analyzing popular communication applications for specific bugs; and
- as required, developing custom exploits for specific platforms.

There will also be significant operational and legal tasks as well.

Using the tools developed to execute an intercept against a target requires three steps: analyzing the target's network usage to determine the platform and applications he or she is using, compromising the platform to deliver an appropriate exploit, and monitoring the captured messages from the exploit and target. Depending on the tools used, these steps may be augmented by conventional data wiretapping techniques.

Compromising the target's platform is practical because modern software systems are—and will continue to be—inherently vulnerable to attack. New exploitable vulnerabilities in widely used software are discovered at a steady rate, literally daily.

Another aspect of modern communication tools works in our favor. A vulnerability in a commonly used communication tool is likely to be effective against many targets, while lightly used communication tools are less likely to be robust (fewer users means less likelihood of discovering security flaws and, typically, fewer vendor resources to discover the vulnerabilities), and thus vulnerabilities in these will be easier and cheaper to discover. Of course, some targets will use communications systems for which penetration is very difficult or expensive under our proposed scheme, but the same situation is also true today.

Several databases track and attempt to catalog the various characteristics of newly discovered vulnerabilities. One of the most comprehensive is the Common Vulnerabilities Enumeration (CVE) database, which provides a weekly listing of newly published vulnerabilities ranked by severity. For the week of 9 July 2012, for example, it reported 45 newly disclosed vulnerabilities, of which 14 were ranked high severity and 31 medium severity. The CVE is an authoritative repository of publicly disclosed vulnerabilities, but is not always as up to date as other databases, such as Bugtraq. The Bugtraq database has the added feature that, if available, proof-of-concept exploit code is included along with vulnerability characteristics.

In addition, several private companies and individual researchers actively search for exploitable vulnerabilities, often selling them along with exploit code. Although there is an active black market for the sale of private, nondisclosed exploitable vulnerabilities,[17] several commercial firms, such as Vupen (www.vupen.com/english/services/solutions-gov.php), VulnerabilityLab (www.vulnerability-lab.com),

Table 1. Exploitable vulnerabilities discovered from March to mid-July 2012.

Month	Vul-Labs	Microsoft V.R.	Vupen	Bugtraq	ZDI
July	15	2	6	17	14
June	32	2	25	5	39
May	31	1	39	2	0
April	37	2	38	6	20
March	9	1	41	11	13

ZDI (http://dvlabs.tippingpoint.com/advisories/disclosure-policy), and Secunia (https://secunia.com/community/advisories), provide subscription services that make available varying levels of access information about 0-day vulnerabilities to their clients.

These groups discover and release a steady stream of new vulnerabilities in widely used software platforms. Table 1 lists the numbers of remotely exploitable vulnerabilities discovered each month from several of these commercial vulnerability research groups for the period of 1 March through mid-July 2012. (The fact that a new vulnerability is found is usually published immediately. Public disclosure of the details usually occurs a few weeks later, typically to Bugtraq [www.securityfocus.com/archive/1] and Full-disclosure [http://seclists.org/fulldisclosure].)

For law enforcement to rely on this rich supply of vulnerabilities to support its wiretapping needs, it must be economical to develop "law enforcement–grade" tools that exploit them. A rough estimate suggests that the costs of operating a law enforcement exploitation laboratory wouldn't be prohibitive, especially compared with the total costs of surveillance mandates in infrastructure. To create an exploitation tool, the government must first discover (or purchase) an exploitable vulnerability. A lab must then "weaponize" the vulnerability to reliably install wiretap code in the target platforms against which it is used. The tools would have to be extensively tested to ensure that that they don't do collateral damage to other parties.

Note that a federal vulnerability laboratory would likely have additional responsibilities beyond just discovering and developing exploits. Federal law enforcement would likely be in the best position to discover the simplest way to install legally authorized wiretaps; state and local law enforcement lack such depth of expertise. The costs of supporting state and local government intercepts (chiefly educational and consulting) will likely be borne by the federal government. However, these costs are relatively small compared with the actual exploitation development activities and can be estimated by the number of state and local wiretap investigations and investigators. (The National Technical Investigators Association includes essentially all investigators who participate in intercept work; it has 4,000 members. This provides a rough upper bound on the laboratory's teaching responsibilities.)

The bulk of the cost of developing law enforcement–grade wiretap tools against any particular platform is thus the cost of discovering an appropriate vulnerability plus the cost of building reliable systems for exploiting it. Both vulnerability discovery and exploitation tool development have evolved into commodities traded on commercial and underground markets, which allows us to approximately project the cost to law enforcement of conducting these activities. Several vulnerability exploitation products are marketed explicitly as surveillance tools for law enforcement and government.

An upper bound on the cost of vulnerability discovery can be estimated straightforwardly from currently existing markets that traffic in 0-day exploits. The government could either purchase "fresh" 0-day vulnerabilities from the market or discover them internally, as budget, resources, and policy permit.

The expected costs of developing these vulnerabilities into viable law enforcement wiretap tools are more difficult to estimate precisely but can be bounded as lying between the known costs of developing typical research and/or criminal exploit tools (at the low end) and the reported costs of developing elaborate national intelligence and "cyberwar" tools (at the high end). For the most part, law enforcement's needs are likely to lie close to the lower bound and should be comparable in sophistication to commercial penetration testing and criminal exploit tools. Commercial penetration testing products, such as Metasploit (www.rapid7.com/products/metasploit-pro.jsp) and Core Impact (www.coresecurity.com/content/core-impact-overview), give estimates for the low end of this cost spectrum. Note that the "payload" of such tools—the code that actually performs the content intercepts—although probably much larger and more complex than the vulnerability exploitation code, is likely to remain reasonably constant over time. Only the exploitation code itself would likely need to be updated or customized frequently.

Policy Concerns

Expanding the scale of law enforcement exploitation of target platform vulnerabilities naturally raises policy concerns. While our focus here is on technical issues, we briefly discuss the policy concerns raised by this approach. We anticipate a fuller treatment of these in policy and legal venues.

If law enforcement purchases vulnerabilities rather than discovering them in-house, a basic issue is whether government participation in the vulnerabilities market is appropriate. Law enforcement demand might help skew incentives against disclosing patches to the software vendors themselves, and some have argued that the process increases the amount of software left unpatched.[16,17] However, because the FBI's purchase can rarely be exclusive, it isn't clear its purchasing a vulnerability would actually change things. From repressive nation-states to well-funded criminal organizations, any number of bad actors are interested in, and capable of paying for, such vulnerabilities, and the market for 0-day vulnerabilities will exist regardless of law enforcement's participation in it. Because law enforcement's needs are likely to be at the lower end of the scale of commercial penetration testing and criminal exploits, the government's participation in the vulnerabilities market is unlikely to change pricing. These low-end vulnerabilities are priced accordingly and usually aren't available for exclusive purchase.

Once developed, an exploit tool will remain useful for law enforcement until the underlying vulnerability is discovered, disclosed, and patched in the target platforms. This period of viability can actually be expected to be quite long. A recent study of 0-day vulnerabilities exploited by malware found that the average time between initial use and public disclosure of a vulnerability was 312 days; it was only sometime later that a vulnerability ceased to be exploitable.[19]

An additional concern is whether law enforcement's participation in the 0-day market supports a shady business whose very existence is contrary to good public policy. This is, of course, the type of issue with which law enforcement often wrestles (a closely related example is that successful investigations often require the use of paid informers in criminal organizations). While law enforcement's participation doesn't create a market that wouldn't otherwise exist, it does have the potential to make these markets more active and robust, possibly increasing the availability of marketed exploits to criminals.

We emphasize that by no means do we suggest that software be deliberately made or left insecure in order to facilitate law enforcement exploits. Indeed, we firmly believe that those who find vulnerabilities should disclose details to the vendor so that they can be fixed as quickly as possible. That said, serious vulnerabilities do and almost certainly will continue to exist in virtually all platforms and applications of interest. We regret this, but the fact remains that exploitable vulnerabilities do exist. Taking advantage of them is far preferable to introducing new vulnerabilities into other applications or infrastructure, as the CALEA approach does.

A related issue arising from law enforcement use of unpublished vulnerabilities (whether discovered internally or purchased) is whether the government should be reporting exploitable vulnerabilities and having them fixed, rather than quietly exploiting them. This question is especially acute for vulnerabilities in common platforms. Perhaps the FBI should be sharing discovered weaknesses with software vendors so that they might patch them and prevent criminal exploitation. On the other hand, given the vast number of potential exploits that naturally occur, law enforcement's choice to use any given vulnerability rather than report it is arguably unlikely to have a major practical impact.

These are legitimate—and difficult—policy questions. We take no position here as to whether law enforcement should purchase 0-day vulnerability information from commercial markets or discover them through in-house research, nor precisely how it should weigh the "report or exploit" question. This is, however, an issue of relative risk; we note that even in the worst case, the overall harm done by law enforcement's discovery and use of vulnerabilities would be far smaller than the harm caused from weakening the infrastructure via wiretap mandates in software and systems. However, to ensure that conflicts between public disclosure and law enforcement silence are properly weighed, it would be appropriate to have technical and policy overseers examining these decisions as they're made.

One important issue is that discovering 0-day vulnerabilities and developing tools that exploit them gives law enforcement more technical capability than it has had in the past. The use of such tools to perform content wiretaps will, of course, require a wiretap order, and thus be legally controlled. However, it's also possible that law enforcement might wish to use these tools in other circumstances, for example, in accessing stored data. What rules should govern this? In 2011, the US Court of Appeals ruled that the court cannot require the plaintiff to reveal his or her encryption key because the state would have access to all the suspect's files and had not specified which ones were of interest.[19] Analyzing the right set of legal responses to this situation is out of scope for this article, but as "Time works changes [and] brings into existence new conditions and purposes,"[20] we note that the extensive use of vulnerabilities/0-day tools could raise new legal issues.

Any shift from carrier-based interception (such as

Practical Concerns

The use of vulnerabilities to enable legally authorized wiretaps raises questions for a variety of communities. For example, the policy community must examine under what circumstances law enforcement's participation in the vulnerabilities market is appropriate. If law enforcement becomes aware that a vulnerability it uses could create serious harm to multiple users or a critical infrastructure, what should its course of action be? What are the national security implications of law enforcement's participation in the vulnerabilities market? Technologists face the issue of "do no harm": an installed vulnerability shouldn't act against anyone but the target (and for the target, the action should be limited to wiretapping the target's communications and not causing other disruption on his or her device).

Another issue is that the vulnerability shouldn't "escape" the target's machine,[1] which might enable the use of the vulnerability by other, nefarious actors. There are additional questions for researchers: What would the sorts of vulnerabilities that law enforcement want to use cost? How would law enforcement's participation in the vulnerabilities market change costs? What's the benefit of using this wiretap data as opposed to the easier-to-obtain stored communications records? All of this returns us to the policy community's issues: online social networks aren't classic communications providers under the law, but they serve many of the same functions. What should their legal responsibilities be?[2] And in an age of ubiquitous online presence, should laws regarding law enforcement's access to communications' transactional data be updated?

References

1. D. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, Crown, 2012.
2. S. Landau, "Testimony before the House of Representatives Committee on the Judiciary, Subcommittee on Crime, Terrorism, and Homeland Security," *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies*, 17 Feb. 2011.

with CALEA) to direct exploitation by law enforcement can make it more difficult to detect extralegal abuse of the interception tools by rogue investigators or agencies. With CALEA, a third party—the telecom carrier—is always involved in provisioning intercepts; exploitation tools, in contrast, can be used unilaterally and potentially without the knowledge of any independent party. We note that this isn't an issue unique to computer interception; many law enforcement capabilities, from deadly weapons to access to sensitive databases, are potentially subject to misuse. Developing robust technical and procedural mechanisms to audit and control the use of, and the data collected by, interception tools must be a central requirement for their expanded use.

A crucial issue, with both legal and technical implications, is the reliability of data gathered by intercept tools. Although a detailed examination of the issue is beyond our scope here, we do note that judges must be convinced that such tools are reliable and trustworthy: such tools must capture exactly the traffic authorized, no more and no less. A tool that misses some traffic might miss exculpatory evidence; a tool that captures too much could lead to confusion over who, precisely, made incriminating comments, and may violate the warrant's limits. Mechanisms that affect third parties' computers, intentionally or accidentally, are especially problematic from this perspective. This is a different issue from minimization, which ensures that the wiretap captures only the subject of an order and only when he or she is engaged in criminal activity. Minimization will also need to be conducted, as it is for any wiretap.

The FBI has dealt with related concerns in deploying the Computer and Internet Protocol Address Verifier (CIPAV),[12] a program that "calls home," meaning that it informs the FBI of a target machine's addressing and protocol data and information such as current IP address, MAC address, open ports, and so on. CIPAV is employed to enable surveillance of the targeted machine.

CIPAV details aren't public, but thanks to documents obtained under the Freedom of Information Act, some information on how the FBI handles the legal aspects of surveilling a target's machine is available.[12] Installing CIPAV requires accessing the target's computer, so first law enforcement seeks a search warrant to install CIPAV on the target's machine. Once it has the IP address and any other information necessary for conducting the surveillance, law enforcement returns to court to obtain a pen register/trap-and-trace order (https://www.eff.org/node/58430). Such a carefully constructed approach might be an appropriate model for law enforcement's use of targeted exploitation tools generally.

Developing a large, well-funded vulnerability exploitation laboratory potentially represents a significant increase in the FBI's technological capabilities. But in a world that's rapidly converting to fully IP-based communications, such capabilities will likely become increasingly important in supporting legally authorized surveillance. Given that law enforcement and intelligence agencies are already using such techniques at a small scale today, it's critical that judges, magistrates, and policymakers be given meaningful technical context for evaluating the impact of the intercept technologies that they're asked to authorize.

Finally, we note that we've focused here on the collection of content; we don't address the issue of data collected by pen registers and trap-and-trace devices. (Pen registers capture dialing, routing, addressing, and signaling information from the target, while trap-and-trace devices capture the information on communications received by the target.) If the communications architecture shares pen register and trap-and-trace data with a service provider, then the information is obtainable from the service provider; however, many highly decentralized architectures, including peer to peer, do not create such records.

When the basic model for voice communications was circuit-switched connections, CALEA was technically feasible even if its security might have been poor. The increasing diversity of local-loop technologies in the 1990s, even with the introduction of ISDN and wireless, still involved the same service (voice telephony) in a landscape that remained both highly regulated and relatively slow moving. The fact that voice communications were circuit-switched meant that you could make a plausible argument for CALEA's approach of shifting wiretaps out of the local loop.

But that argument is no longer applicable in the Internet context. We not only have increased diversity of the local loop (which can be IP-based, DSL, ISDN, or wireless), but we've also increased diversity of the services themselves (voice, email, IM, VoIP, and so on) and of the carrier/ISP infrastructures implementing them. From a situation that had a limited set of service providers providing centralized communications, we've moved to a world with a nearly infinite set of application providers offering highly decentralized ones. The conditions that might have briefly favored the CALEA approach increasingly no longer exist, and they're highly unlikely to return.

By placing wiretapping infrastructure costs on telecommunications carriers, CALEA functioned as a cost-shifting mechanism for the government. But the economic impact of the changes in telecommunications means that the externalities of the CALEA approach—particularly the costs to innovation and security—are now rapidly going up, even while the effectiveness of the CALEA approach is rapidly diminishing.

CALEA effectively imposed a hidden wiretapping tax. Funding a laboratory (such as DCAC) at a level that enables law enforcement to reliably conduct legally authorized surveillance is a much more efficient use of scarce resources and shifts the costs back to the model that existed before CALEA. Passive interception and targeted vulnerability exploitation tools can provide law enforcement with capabilities that give investigators what they need without simultaneously increasing the insecurity of the telecommunications infrastructure.

This latter point is critical. If legally authorized wiretaps are a tool that government occasionally needs, law enforcement will seek viable paths for conducting them. We can either mandate artificially introduced vulnerabilities across all our communications platforms (the CALEA approach), or law enforcement can take advantage of capabilities—the weaknesses that unavoidably occur in complex software systems—that are already there. The latter is ultimately preferable. Software vulnerabilities exist whether law enforcement uses them against its targets or not. By focusing on discovering and exploiting preexisting weaknesses in targets' platforms and ending the business of introducing weaknesses into the communications fabric, law enforcement effectively promotes a national infrastructure that doesn't preclude legally authorized wiretapping but that doesn't create new opportunities for criminal exploitation. This turns us away from the vulnerabilities introduced by the CALEA approach and toward a model where law enforcement supports securing the communications infrastructure, a win for both law enforcement and the broader society. ■

Acknowledgments

We're grateful for the discussions and suggestions made by Herbert Lin, Marty Stansell-Gamm, Lee Tien, Marcus Thomas, and an unnamed reviewer. Their help does not in any way imply endorsement of the ideas presented in this article.

References

1. E. Lichtblau, "Police Are Using Phone Tracking as a Routine Tool," *The New York Times*, 1 Apr. 2012, p. A1.
2. K. Dam and H. Lin, *Cryptography's Role in Securing the Information Society*, Nat'l Academy Press, 1996.
3. S. Landau, *Surveillance or Security? The Risks Posed by New Wiretapping Technologies*, MIT Press, 2011.
4. V. Caproni, "Going Dark: Lawful Electronic Surveillance in the Face of New Technologies," Subcommittee on Crime, Terrorism, and Homeland Security, Committee on Judiciary, 17 Feb. 2011; http://judiciary.house.gov/hearings/hear_02172011.html.
5. D. McCullagh, "FBI Quietly Forms Secretive Net-Surveillance," CNET, 22 May 2012; http://news.cnet.com/8301-1009_3-57439734-83/fbi-quietly-forms-secretive-net-surveillance-unit.
6. A. Gidari, "Designing the Right Wiretap Solution: Setting Standards under CALEA," *IEEE Security & Privacy*, vol. 4, no. 3, 2006, pp. 29–36.
7. S. Bellovin et al., "Security Implications of Applying the Communications Assistance to Law Enforcement Act to

Voice over IP," 2006; http://privacyink.org/pdf/CALEAVOIPreport.pdf.

8. Network Working Group, *IETF Policy on Wiretapping*, IETF RFC 2804, May 2000.
9. V. Prevelakis and D. Spinellis, "The Athens Affair," *IEEE Spectrum*, July 2007, pp. 18–25.
10. P. Colaprico, "Da Telecom dossier sui Ds, Mancini parla dei politici," (in Italian), *La Repubblica*, 26 Jan. 2007.
11. S. Landau, "The Large Immortal Machine and the Ticking Time Bomb," *J. Telecommunications and High Technology Law*, vol. 11, no. 1, 2013, pp. 1–43.
12. J. Lynch, "New FBI Documents Provide Details on Government's Surveillance Software," Electronic Frontier Foundation, 29 Apr. 2011; https://www.eff.org/deeplinks/2011/04/new-fbi-documents-show-depth-government#footnote2_01mhuxa.
13. G. Anastasia, "Big Brother and the Bookie," *Mother Jones*, Jan./Feb. 2002.
14. *United States v. Nicodemo S. Scarfo*, et al.
15. Criminal Action No. 00-404 (NHP), US District Court for the District of New Jersey.
16. A. Greenberg, "Shopping for Zero-Days: A Price List for Hackers' Secret Software Exploits," *Forbes*, 23 Mar. 2012; www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/.
17. M. Hofmann and T. Timm, "'Zero-Day' Exploit Sales Should Be Key Point in Cybersecurity Debate," Electronic Frontier Foundation, 29 Mar. 2012; https://www.eff.org/deeplinks/2012/03/zero-day-exploit-sales-should-be-key-point-cybersecurity-debate.
18. B. Schneier, "The Vulnerabilities Market and the Future of Security," *Forbes*, 30 May 2012; www.forbes.com/sites/bruceschneier/2012/05/30/the-vulnerabilities-market-and-the-future-of-security/.
19. L. Bilge and T. Dimitras, "Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World," *Proc. 2012 ACM Conf. on Computer and Communications Security*, ACM, 2012.
20. Grand Jury Subpoena Duces Tecum, 25 Mar. 2011, United States of America, Plaintiff-Appellee, versus John Doe, Defendant-Appellant, for Judges Understanding Capabilities of the Technical Tools in the United States Court of Appeals for the Eleventh Circuit, nos. 11-12268 & 11-15421, DC Docket no. 3:11-mc-00041-LAC.
21. *Weems v. United States*, US Reports, vol. 217, 1910, p. 349.

Steven M. Bellovin is a professor of computer science at Columbia University; he's currently on leave and serving as chief technologist of the Federal Trade Commission. (His work on this article was completed before he joined the FTC; opinions expressed are personal and not those of the FTC.) He works on security, privacy, and related public policy issues. Bellovin has a PhD in computer science from the University of North Carolina at Chapel Hill. He is a member of the ACM. Contact him at smb@cs.columbia.edu.

Matt Blaze directs the Distributed Systems Laboratory at the University of Pennsylvania, where his research focuses on security, privacy, and scale in computing and communications systems. Blaze has a PhD in computer science from Princeton University. Contact him at blaze@cis.upenn.edu.

Sandy Clark is a PhD candidate in the Distributed Systems Lab at the University of Pennsylvania and is advised by Matt Blaze and coadvised by Jonathan Smith. Her research focuses on understanding the mechanisms involved in the computer security arms race. Contact her at clarks@cis.upenn.edu.

Susan Landau works in cybersecurity, privacy, and public policy and is currently a Guggenheim Fellow. She was previously a Distinguished Engineer at Sun Microsystems and a faculty member at the University of Massachusetts Amherst and Wesleyan University. Landau has a PhD from MIT and is a member of AAAS, ACM, AMS, and IEEE. Contact her at susan.landau@privacyink.org.

Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.

Emmett, Jamie

From:	Plunkett, Shawn
Sent:	May-28-13 12:17 PM
To:	Dincoy, Rana; Hawrylak, Maciek; Durand, Mathieu
Subject:	FW: Paper on lawful access

FYI. Interesting conclusion.

From: Grigsby, Alexandre
Sent: May-28-13 11:33 AM
To: Plunkett, Shawn; Hamilton, Sharon; Cameron, Bud; Bonvie, Jeff; Dvorkin, Corey; Bradley, Kees
Cc: Hatfield, Adam
Subject: Paper on lawful access

Hi all,

Came across this paper that might be of interest. It's authored by some engineers concerned that mandating backdoors in software for lawful intercept purposes introduces new vulnerabilities into software that will be exploited by non-authorized purposes. Their solution seems to be: "all software has vulnerabilities – just have law enforcement exploit existing vulnerabilities as opposed to creating new ones"

https://www.cs.columbia.edu/~smb/papers/GoingBright.pdf

alex

Alexandre Grigsby
Analyst | Analyste
National Cyber Security Directorate | Direction générale de la cybersécurité nationale
Public Safety Canada | Sécurité publique Canada
tel. 613.949.4243
www.publicsafety.gc.ca | www.securitepublique.gc.ca

© IEEE Security & Privacy 11:1, Jan/Feb 2013, http://dx.doi.org/10.1109/MSP.2012.138

Going Bright: Wiretapping without Weakening Communications Infrastructure

Steven M. Bellovin | Columbia University
Matt Blaze and Sandy Clark | University of Pennsylvania
Susan Landau | Privacy Ink

Mobile IP-based communications and changes in technologies have been a subject of concern for law enforcement, which seeks to extend current wiretap design requirements for digital voice networks. Such an extension would create considerable security risks as well as seriously harm innovation. Exploitation of naturally occurring bugs in the platforms being used by targets may be a better alternative.

For law enforcement wiretaps, this is the best of times and the worst of times. Tracking suspects through transactional data vastly simplifies investigators' efforts. Yet accessing communications content through traditional means could be getting harder. Because of peer-to-peer communication methods, encryption, and service providers located outside the US, law enforcement says its ability to execute legally authorized wiretaps is becoming increasingly problematic. The US Federal Bureau of Investigation (FBI) claims its wiretapping capability is "going dark" (http://judiciary.house.gov/hearings/hear_02172011.html).

Law enforcement's preferred solution? Since 2010, the FBI has advocated expanding the scope of the Communications Assistance for Law Enforcement Act (CALEA), a 1994 law that requires that switches in digital telephone networks be built wiretap enabled. The FBI wants to extend such requirements to IP-based communications.

CALEA and the Internet

CALEA was controversial because it introduced new security risks into the voice telephone network; indeed, there have been several publicly known cases of telephone switches being compromised through their wiretap interfaces. This article is primarily focused on the issues associated with CALEA if it were to be extended to emerging Internet-based services.

There are several possible policy options for wiretapping as these trends continue. These include maintaining the status quo, which would increasingly limit content wiretaps to (decreasingly relevant) switched telephone networks.

Law enforcement could increasingly rely on (non-content) communications records, which can reveal a great deal of information about a target's location, contacts, movement, and so on.[1] The legal and privacy implications of widespread use of communications records by law enforcement are a matter of some controversy, however, and at scale, it's difficult to ensure that information about innocent third parties won't find its way into law enforcement databases along with the records of suspects.

But there is yet another possibility. As the CALEA approach has become less viable (and more dangerous to emerging infrastructure), targeted interception approaches—ones that don't entail the risks and costs of nationally mandated wiretap interfaces—have become increasingly practical. One approach is to leverage the fact that targets' communications devices in modern networks are virtually always built on complex software platforms. Continuing technical access to authorized wiretaps can be achieved—without expanding CALEA—by exploiting naturally occurring weaknesses in subjects' devices, enabling law enforcement to install surreptitious interception software at a target endpoint as required. Many such weaknesses are *0-day vulnerabilities*, ones that might be completely unknown to others and for which no vendor fix exists. (Conceptually, the bug is discovered on day zero and reported and patched sometime later.)

Communication devices in modern networks are essentially always built on complex software platforms. Due to the inexact nature of software development, all complex programs contain inadvertent vulnerabilities. Without requiring any explicit wiretap support in the network or any compromise of nontargeted devices, law enforcement can exploit software vulnerabilities on end devices to facilitate interception. The US law enforcement community can fund a laboratory to develop targeted interception tools that take advantage of such vulnerabilities, an idea proposed in the 1996 National Research Council report on cryptography.[2] (Note, however, that the FBI has a role in crime prevention, but it isn't tasked with securing communications or communications infrastructure.[3]) Such an approach isn't without its own policy concerns and risks, yet it's far more protective of national communications security and privacy than other proposed alternatives, including and especially CALEA-type design mandates.

Some work in this direction is already in progress by law enforcement. As has been reported elsewhere,[4,5] the FBI has established a Domestic Communications Assistance Center (DCAC) to tackle the technical side of the "going dark" problem. In 2012, the FBI requested US$15 million to fund this lab. We believe that approaches such as expanding DCAC's efforts—and not expanding CALEA's scope—are effectively the only path to facilitating legally authorized wiretapping that doesn't also undermine the security of the US communications infrastructure.

We conclude that

- any past success network-based interception schemes such as CALEA may have enjoyed in the telephony domain won't translate to similar success for Internet-based services;
- many emerging communications services are inherently interceptable by passive means;
- requiring additional centralized interception capabilities will be unnecessarily redundant and will introduce increasingly more serious security risks to infrastructure while being increasingly less effective in producing useful evidence for law enforcement;
- law enforcement development of a sufficiently broad range of targeted passive and endpoint-based interception tools to meet ongoing wiretap needs is technically and economically feasible;
- law enforcement's use of passive interception and targeted vulnerability exploitation tools creates fewer security risks for nontargets and critical infrastructure than do design mandates for wiretap interfaces; and
- moving forward, targeted exploitation solutions are likely to be the only viable approaches for providing law enforcement with reliable interception capabilities against modern platforms, even if wiretap interfaces in infrastructure were mandated.

In particular, it is critical for national security that communications software and systems be designed to be as secure as possible against attack. Deliberate backdoors—whether by way of CALEA or through hidden "lawful intercept" access features included by software vendors—inherently make systems more vulnerable; worse yet, all users, not just wiretap targets, suffer the increased exposure. However, the absence of explicit lawful intercept backdoors need not preclude law enforcement access when it's required, as we'll discuss later.

Note that our discussion is US focused: CALEA is a US law. However, the 1994 US solution of building wiretapping capabilities into switches was rapidly taken up in many other parts of the world under the generic name "lawful intercept." The security risks inherent in extending CALEA to the Internet are security risks facing any nation contemplating similar approaches to a CALEA-type regime for IP-based networks. Thus, while our context is local, our analysis is global in its applicability.

Wiretapping: The Present Situation

By requiring that communications providers include wiretapping capabilities within switching mechanisms, CALEA was a surprising development on the regulatory front.

For a quarter of a century, the process under which authorized wiretaps were done in the US was straightforward. Two laws, the 1968 Title III of the Omnibus Crime Control and Safe Streets Act (for criminal investigations) and the 1978 Foreign Intelligence Surveillance Act (FISA; for foreign intelligence cases), governed wiretap order applications. Once a judge granted an order, the wiretap could be installed.

The divestiture of AT&T meant that instead of a single monopoly handling both telephones and service, many more product and service providers emerged, along with increasing innovation in communication technologies. Law enforcement found itself thwarted in carrying out some legally authorized wiretaps. (Because we focus on possible extensions to CALEA and the harm they represent, we don't discuss the much richer surveillance capabilities now available to law enforcement—the plethora of communications, the fact that these frequently reveal location, and so forth—that provide a different situation than when Title III and FISA were passed.) Their solution was CALEA.

CALEA was implemented through an interface standard developed by the Telephone Industry Association in consultation with law enforcement.[6] This standard pleased no one: civil liberties groups wanted greater privacy protections than the standard provided, industry wanted greater clarity on the standard's technical requirements, and law enforcement wanted greater surveillance capabilities than were included. Several lawsuits and court rulings ensued, but by 2002, the requirements for CALEA compliance finally solidified. Although nobody was fully satisfied, CALEA became the dominant mechanism for implementing telephone wiretaps.

The FBI soon raised a new concern: Voice over IP (VoIP). IP-based communications are often peer to peer, and the CALEA model of tapping at the switch doesn't easily fit in with that. The Federal Communications Commission (FCC) and a federal appeals court cut this Gordian knot by deciding that CALEA would apply to facilities-based broadband, systems with wired lines (or wireless channels) to the end user. These communications systems are centralized, just like the public switched telephone network (PSTN), and applying CALEA-type solutions isn't especially technically difficult.

Innovation rarely pauses in technology. Because of a combination of increasing levels of peer-to-peer communications and encryption, along with such changes as overseas communications providers offering services in the US (creating difficulties when a wiretap is needed), law enforcement is again facing difficulties. What CALEA extensions the FBI actually seeks remain unclear. There have been various news reports since autumn 2010, but as of this writing, no bill has been produced.

CALEA worked for a reason that no one fully articulated: circuit-switched telephones (and cellphones) were the primary mode of communication. That era is now ending. Efforts to extend CALEA-type controls to the nearly infinite number of communications devices and applications cannot be effective.

The CALEA "Solution"

CALEA was intended to address a specific and rather unique set of technological circumstances brought about by incremental advances in voice telephone technology. Prior to CALEA, there was neither a mandate requiring telephone companies to design technology facilitating wiretapping nor a standard telephone wiretapping interface. Instead, wiretaps relied on local loops, the pairs of wires between a local telephone office and its subscribers. Law-enforcement agencies developed local-loop tapping technology, which it deployed by connecting to subscriber wire pairs. Sometimes law enforcement deployed taps with assistance from the carrier; sometimes it did it on its own.

Tapping technology was simple and largely unchanging because telephone subscriber loop technology was, at least until the 1990s, simple and relatively unchanging. Carrying analog voice and signaling, the telephone local loop remained essentially the same for half a century. Tapping a telephone was a relatively simple matter of gaining physical access to the target's pair of wires and recording the electrical signals and voice audio the wires carried.

By the 1990s, two new subscriber loop technologies had emerged that weren't directly compatible with traditional analog wiretapping techniques. ISDN employed a pair of wires between the telephone central office and the subscriber but used digital signals and digitally encoded audio, which can require far more sophisticated technology for third-party interception. The other new technology was wireless cellular, in which the local loop was replaced with a two-way radio link, allowing the subscriber to move freely about the coverage area.

It's important to note that while ISDN and cellular services might have radically altered the local loop between the telephone company and the subscriber, these technologies did relatively little to alter telephony's centralized architecture. The basic service for both ISDN and cellular was and is voice calls linked to the PSTN. Subscribers still obtain their service from a single one of relatively few providers, which are themselves highly regulated by local franchises or hold federal licenses for part of the limited wireless spectrum.

Current Internet service architectures are far more complex than the telephone networks of the 1990s. Link technologies, including cable, fiber optics, DSL, and several forms of cellular wireless, were widely implemented. VoIP services, of which there are various varieties, have added a third local loop technology; it adds the challenge of separating the infrastructure provider from the physical plant provider, greatly complicating the wiretapping effort.[7]

Currently relatively few entities have had to comply with the current CALEA voice wiretap interface mandates. Those that do provide a common basic service:

voice calls. Compared with typical Internet infrastructure, switches for voice calls—the primary devices required to have CALEA interfaces—are very expensive, amortized over long periods, and relatively slow to change. This means that the costs, innovation burden, and security risks associated with implementing CALEA for voice telephony, while not trivial, are both somewhat calculable and relatively manageable. Yet even in the domain of voice telephony, CALEA is far from a win-win solution for wiretapping. Still, for IP-based communications, CALEA represents a lose-lose situation.

CALEA Insecurities

CALEA requires that a deliberate security weakness—the wiretap interface and control system—be architected into the switches of a communications network. In 2000, the Internet Engineering Task Force observed that, "Experience shows that if a vulnerability exists in a security system, it is likely that someone will take advantage of it sooner or later."[8] That situation has come to pass for CALEA-type interfaces.

The story of the 10-month interception of the most senior officials of the Greek government in 2004 to 2005 using a CALEA-type interface that had been surreptitiously turned on is well known.[9] Less well known is the 10-year wiretapping of 6,000 Italians that occurred through Telecom Italia,[10] the targets of which included political figures, judges, referees, and celebrities. The US has not been immune. Examinations by the National Security Agency (NSA) of CALEA-compliant switches to be sold to the Department of Defense found vulnerabilities in the CALEA implementation in every single switch examined.[11]

CALEA-like interfaces are, by definition, designed for surreptitious eavesdropping. They're intentional backdoors and thus both easier to exploit and more damaging when penetrated. The recent massive increase in cyberexploitation—theft of data from governments and companies around the world—adds to the concern about the vulnerabilities created through CALEA-type architectures. Furthermore, there are subtle but essential differences between the architecture of the PSTN and those of contemporary and emerging Internet-based services. These make generalized wiretap interfaces for Internet communications far more technically difficult, complex, and economically burdensome than they are in traditional telephony.

It's certainly true that unauthorized remote wiretaps can be implemented by using other forms of remote access including craft interfaces, which are used to test installations, check reported faults, and so on. But such remote accesses are much more difficult to conduct surreptitiously because, unlike CALEA, they're deliberately designed to be logged and to trigger other, semiautomatic changes within the system. In contrast, CALEA interfaces are specifically intended for surreptitious wiretapping. By design, indicia of such taps are carefully restricted and invisible outside the CALEA control console. They thus provide a more attractive attack surface for exploitation by criminals and foreign intelligence services.

It's far from clear that CALEA for telephony has successfully balanced law enforcement requirements for surveillance access with the broader goal of preventing illicit access to critical infrastructure by criminals and foreign governments. But even if we assume that CALEA for telephony has been on the whole a success, the conditions that might have made it so aren't present in the Internet services for which the government seeks to apply the same approach. Communications infrastructure lasts a long time. Given increasing cyberexploitation efforts, switch longevity makes the security concerns even more trenchant.

The CALEA Problem

Internet-based services have very different technical and economic properties from traditional telephony. These make the CALEA approach far less attractive for the Internet while simultaneously introducing considerably more risk.

There are several reasons that lawful intercept mechanisms in all communications software are an exceedingly bad idea. The most obvious is the risk: the more code in an application, the more likely it is to have bugs. By definition, lawful intercept code is an engineered—though nominally controlled—vulnerability; a flaw in it exposes the precise sort of access many attackers will want. Even if the intercept code does not itself offer vulnerabilities, its mere existence simplifies the attackers' efforts (witness what happened in Athens and Italy).

The Internet services the government seeks to tap are provided by a large number of entities operating on ordinary computers that are architecturally, effectively ordinary end points. In contrast, on the PSTN, telephony services are provided by large, centralized switching systems operated by a small number of carriers. This architectural difference underlies the vastly greater pace of technology development in Internet services compared with the telephone network.

On the Internet, any node with sufficient bandwidth can act as a service provider. This has led to innovations that a centralized, slow-moving company wouldn't do. The Web itself was invented at a physics laboratory, not by ISPs. Skype, which provides telephone-style voice service Internet connections, doesn't even use central servers; it's a distributed, peer-to-peer network.

To tap Internet applications in the manner of CALEA, then, requires wiretap interfaces in many widely distributed nodes, rather than a few centralized ones. It imposes design constraints on a large number of service providers around the world, rather than a few domestic phone companies. Requiring lawful intercept interfaces in all Internet communications services and software is simply untenable.

Especially early in their life cycles, Internet-based services tend to be lightweight, inexpensive, rapidly changing, and far more reliant on general-purpose software platforms than are the slow-moving of traditional telephony. Thus the highly diverse and dynamic nature of Internet-based services makes the implementation of any kind of standardized wiretap interface considerably more architecturally disruptive than it has been in the PSTN's switched voice telephony environment. A wiretap interface would have to be integrated over a wide range of often quickly deployed and poorly debugged services and then reimplemented every time a new service is introduced or a software architecture changes. This would prove an expensive burden on the small start-ups that drive online innovation.

Worse, many new services, especially those that rely on a peer-to-peer architecture for routing content between users, simply can't be intercepted via the centralized CALEA model. For these services, no design mandate, short of outlawing the decentralized routing scheme on which the Internet is built, can reliably capture all the traffic law enforcement might seek to intercept. Mandating centralized wiretap capabilities in these services would not only be disruptive to innovation but would also fail to deliver meaningful benefit to law enforcement.

Finally, expanding the number of CALEA-like interfaces in the network would create great insecurity. The vulnerabilities in every CALEA-compliant switch tested by the NSA show how hard it is to get the interception technology correct. Those switches were designed by large service providers working over a relatively long period of time. The difficulty of debugging and testing software to make Internet services secure is a largely unsolved problem, especially at the pace of "Internet time"; requirements for wiretap interfaces would make securing new services significantly more difficult.

Wiretapping by Compromising the Target

Suppose that the FBI were to use vulnerability-based solutions for its targeted Internet intercepts. How would this be done? What is necessary to enable it to happen?

Modern computing and communications devices suffer from an essentially unlimited number of security vulnerabilities. Furthermore, as the widespread proliferation of botnets and other criminal exploitation tools demonstrates, it's easy to exploit these vulnerabilities and gain control over an unwitting user's entire platform and virtually impossible for end users to defend against such attacks. Law enforcement can (and, to a certain extent, already does) exploit this.

However, there are additional requirements for law enforcement exploitation tools beyond those employed by criminals who compromise computers to create botnets or steal private data. Cybercriminal tools generally focus on targets of opportunity, but law enforcement will have specific targets on which to focus. This will require specialized interception tools that work well above the "probabilistic" standard of typical criminal exploits. In particular, tools must have a very high chance of successfully compromising the target without risk of alerting the target. Furthermore, the compromise tool can't risk disrupting a target's computer environment—or anyone else's. Finally, investigators must be able to rapidly determine whether their tools have successfully compromised their target's hardware, must be able to manage it during the intercept period, and must be able to "clean up" once a wiretap has ended.

There are four primary components to any law enforcement tool that exploits target endpoint vulnerabilities: selection or discovery of an appropriate underlying vulnerability, installation mechanisms, mechanisms for obtaining access to the communications being targeted, and ways to send captured data back to the responsible investigators. All are situation-dependent. Developing usable, specialized attack tools to accomplish these tasks would be the core mission of a vulnerability exploitation lab. These tools would generally need to be developed and tested by the government well in advance of their use against any particular target.

Consider a hypothetical example: a wiretap target is using an encrypted communication system we'll call CommApp. If CommApp itself is known to have a remotely exploitable vulnerability (one in which carefully formed messages sent to it over the network can compromise the application), the government can use this directly to install its wiretapping code in the application. In this case, the government's compromise tool for CommApp would have to craft an attack message and deliver it over the network when CommApp is running.

If there are no exploitable vulnerabilities in CommApp itself, the problem becomes twofold: system penetration and application penetration. Both of these are classic problems well known to the security community. For the former, the FBI would have to exploit a vulnerability in any other application used by the target. There is a core of very complex—and hence inherently likely to be vulnerable—software used in most platforms; for computers, this core includes Web browsers, email applications, word processors, spreadsheets, PDF and photo viewing interfaces, and so on. An appropriate vulnerability would be one in which opening a specially crafted file with the vulnerable application allows attack code to be installed in the target's platform. Such vulnerabilities are very common in complex applications. A penetration, then, would involve arranging for the target's computer to open an attack file with the vulnerable application, either through automated means over the network or by subterfuge.[12]

In the (very) rare cases where no remote exploitation is possible, a "black bag job"—a legally authorized surreptitious physical break-in—might be performed to install the exploit code directly on the target's device. This has been done in the past.[13,14]

Once the system is penetrated by running the FBI's code, the exploitation must gain access to the intended communication. In our example, CommApp itself could be modified. The simplest modification would be one that leaked the cryptographic keys, but there are more complex modifications, such as capturing the plaintext voice, that would also work. An alternative approach would be to employ generic modules to capture microphone input, speaker output, and so on.

The central problem in our hypothetical example is surreptitiously exfiltrating the captured content back to the FBI. For content such as text messages, the volume of data is typically low enough that any excess traffic won't disturb a broadband connection. Voice is more difficult, especially on cellphones, which have relatively limited battery and transmission capacity. Sending the captured traffic at low speed over time can avoid a noticeable spike in traffic volume. Alternatively, the exploit code might disable encryption or weaken or leak the session encryption keys, allowing intercepted content to be captured in real time by conventional interception techniques without consuming extra bandwidth.

Maintaining an exploitation development capability involves four major ongoing tasks:

- developing and maintaining a library of penetrations techniques for major operating systems and applications;
- developing and maintaining input and output capture techniques;
- analyzing popular communication applications for specific bugs; and
- as required, developing custom exploits for specific platforms.

There will also be significant operational and legal tasks as well.

Using the tools developed to execute an intercept against a target requires three steps: analyzing the target's network usage to determine the platform and applications he or she is using, compromising the platform to deliver an appropriate exploit, and monitoring the captured messages from the exploit and target. Depending on the tools used, these steps may be augmented by conventional data wiretapping techniques.

Compromising the target's platform is practical because modern software systems are—and will continue to be—inherently vulnerable to attack. New exploitable vulnerabilities in widely used software are discovered at a steady rate, literally daily.

Another aspect of modern communication tools works in our favor. A vulnerability in a commonly used communication tool is likely to be effective against many targets, while lightly used communication tools are less likely to be robust (fewer users means less likelihood of discovering security flaws and, typically, fewer vendor resources to discover the vulnerabilities), and thus vulnerabilities in these will be easier and cheaper to discover. Of course, some targets will use communications systems for which penetration is very difficult or expensive under our proposed scheme, but the same situation is also true today.

Several databases track and attempt to catalog the various characteristics of newly discovered vulnerabilities. One of the most comprehensive is the Common Vulnerabilities Enumeration (CVE) database, which provides a weekly listing of newly published vulnerabilities ranked by severity. For the week of 9 July 2012, for example, it reported 45 newly disclosed vulnerabilities, of which 14 were ranked high severity and 31 medium severity. The CVE is an authoritative repository of publicly disclosed vulnerabilities, but is not always as up to date as other databases, such as Bugtraq. The Bugtraq database has the added feature that, if available, proof-of-concept exploit code is included along with vulnerability characteristics.

In addition, several private companies and individual researchers actively search for exploitable vulnerabilities, often selling them along with exploit code. Although there is an active black market for the sale of private, nondisclosed exploitable vulnerabilities,[17] several commercial firms, such as Vupen (www.vupen.com/english/services/solutions-gov.php), VulnerabilityLab (www.vulnerability-lab.com),

Table 1. Exploitable vulnerabilities discovered from March to mid-July 2012.

Month	Vul-Labs	Microsoft V.R.	Vupen	Bugtraq	ZDI
July	15	2	6	17	14
June	32	2	25	5	39
May	31	1	39	2	0
April	37	2	38	6	20
March	9	1	41	11	13

ZDI (http://dvlabs.tippingpoint.com/advisories/disclosure-policy), and Secunia (https://secunia.com/community/advisories), provide subscription services that make available varying levels of access information about 0-day vulnerabilities to their clients.

These groups discover and release a steady stream of new vulnerabilities in widely used software platforms. Table 1 lists the numbers of remotely exploitable vulnerabilities discovered each month from several of these commercial vulnerability research groups for the period of 1 March through mid-July 2012. (The fact that a new vulnerability is found is usually published immediately. Public disclosure of the details usually occurs a few weeks later, typically to Bugtraq [www.securityfocus.com/archive/1] and Full-disclosure [http://seclists.org/fulldisclosure].)

For law enforcement to rely on this rich supply of vulnerabilities to support its wiretapping needs, it must be economical to develop "law enforcement–grade" tools that exploit them. A rough estimate suggests that the costs of operating a law enforcement exploitation laboratory wouldn't be prohibitive, especially compared with the total costs of surveillance mandates in infrastructure. To create an exploitation tool, the government must first discover (or purchase) an exploitable vulnerability. A lab must then "weaponize" the vulnerability to reliably install wiretap code in the target platforms against which it is used. The tools would have to be extensively tested to ensure that that they don't do collateral damage to other parties.

Note that a federal vulnerability laboratory would likely have additional responsibilities beyond just discovering and developing exploits. Federal law enforcement would likely be in the best position to discover the simplest way to install legally authorized wiretaps; state and local law enforcement lack such depth of expertise. The costs of supporting state and local government intercepts (chiefly educational and consulting) will likely be borne by the federal government. However, these costs are relatively small compared with the actual exploitation development activities and can be estimated by the number of state and local wiretap investigations and investigators. (The National Technical Investigators Association includes essentially all investigators who participate in intercept work; it has 4,000 members. This provides a rough upper bound on the laboratory's teaching responsibilities.)

The bulk of the cost of developing law enforcement–grade wiretap tools against any particular platform is thus the cost of discovering an appropriate vulnerability plus the cost of building reliable systems for exploiting it. Both vulnerability discovery and exploitation tool development have evolved into commodities traded on commercial and underground markets, which allows us to approximately project the cost to law enforcement of conducting these activities. Several vulnerability exploitation products are marketed explicitly as surveillance tools for law enforcement and government.

An upper bound on the cost of vulnerability discovery can be estimated straightforwardly from currently existing markets that traffic in 0-day exploits. The government could either purchase "fresh" 0-day vulnerabilities from the market or discover them internally, as budget, resources, and policy permit.

The expected costs of developing these vulnerabilities into viable law enforcement wiretap tools are more difficult to estimate precisely but can be bounded as lying between the known costs of developing typical research and/or criminal exploit tools (at the low end) and the reported costs of developing elaborate national intelligence and "cyberwar" tools (at the high end). For the most part, law enforcement's needs are likely to lie close to the lower bound and should be comparable in sophistication to commercial penetration testing and criminal exploit tools. Commercial penetration testing products, such as Metasploit (www.rapid7.com/products/metasploit-pro.jsp) and Core Impact (www.coresecurity.com/content/core-impact-overview), give estimates for the low end of this cost spectrum. Note that the "payload" of such tools—the code that actually performs the content intercepts—although probably much larger and more complex than the vulnerability exploitation code, is likely to remain reasonably constant over time. Only the exploitation code itself would likely need to be updated or customized frequently.

Policy Concerns

Expanding the scale of law enforcement exploitation of target platform vulnerabilities naturally raises policy concerns. While our focus here is on technical issues, we briefly discuss the policy concerns raised by this approach. We anticipate a fuller treatment of these in policy and legal venues.

If law enforcement purchases vulnerabilities rather than discovering them in-house, a basic issue is whether government participation in the vulnerabilities market is appropriate. Law enforcement demand might help skew incentives against disclosing patches to the software vendors themselves, and some have argued that the process increases the amount of software left unpatched.[16,17] However, because the FBI's purchase can rarely be exclusive, it isn't clear its purchasing a vulnerability would actually change things. From repressive nation-states to well-funded criminal organizations, any number of bad actors are interested in, and capable of paying for, such vulnerabilities, and the market for 0-day vulnerabilities will exist regardless of law enforcement's participation in it. Because law enforcement's needs are likely to be at the lower end of the scale of commercial penetration testing and criminal exploits, the government's participation in the vulnerabilities market is unlikely to change pricing. These low-end vulnerabilities are priced accordingly and usually aren't available for exclusive purchase.

Once developed, an exploit tool will remain useful for law enforcement until the underlying vulnerability is discovered, disclosed, and patched in the target platforms. This period of viability can actually be expected to be quite long. A recent study of 0-day vulnerabilities exploited by malware found that the average time between initial use and public disclosure of a vulnerability was 312 days; it was only sometime later that a vulnerability ceased to be exploitable.[19]

An additional concern is whether law enforcement's participation in the 0-day market supports a shady business whose very existence is contrary to good public policy. This is, of course, the type of issue with which law enforcement often wrestles (a closely related example is that successful investigations often require the use of paid informers in criminal organizations). While law enforcement's participation doesn't create a market that wouldn't otherwise exist, it does have the potential to make these markets more active and robust, possibly increasing the availability of marketed exploits to criminals.

We emphasize that by no means do we suggest that software be deliberately made or left insecure in order to facilitate law enforcement exploits. Indeed, we firmly believe that those who find vulnerabilities should disclose details to the vendor so that they can be fixed as quickly as possible. That said, serious vulnerabilities do and almost certainly will continue to exist in virtually all platforms and applications of interest. We regret this, but the fact remains that exploitable vulnerabilities do exist. Taking advantage of them is far preferable to introducing new vulnerabilities into other applications or infrastructure, as the CALEA approach does.

A related issue arising from law enforcement use of unpublished vulnerabilities (whether discovered internally or purchased) is whether the government should be reporting exploitable vulnerabilities and having them fixed, rather than quietly exploiting them. This question is especially acute for vulnerabilities in common platforms. Perhaps the FBI should be sharing discovered weaknesses with software vendors so that they might patch them and prevent criminal exploitation. On the other hand, given the vast number of potential exploits that naturally occur, law enforcement's choice to use any given vulnerability rather than report it is arguably unlikely to have a major practical impact.

These are legitimate—and difficult—policy questions. We take no position here as to whether law enforcement should purchase 0-day vulnerability information from commercial markets or discover them through in-house research, nor precisely how it should weigh the "report or exploit" question. This is, however, an issue of relative risk; we note that even in the worst case, the overall harm done by law enforcement's discovery and use of vulnerabilities would be far smaller than the harm caused from weakening the infrastructure via wiretap mandates in software and systems. However, to ensure that conflicts between public disclosure and law enforcement silence are properly weighed, it would be appropriate to have technical and policy overseers examining these decisions as they're made.

One important issue is that discovering 0-day vulnerabilities and developing tools that exploit them gives law enforcement more technical capability than it has had in the past. The use of such tools to perform content wiretaps will, of course, require a wiretap order, and thus be legally controlled. However, it's also possible that law enforcement might wish to use these tools in other circumstances, for example, in accessing stored data. What rules should govern this? In 2011, the US Court of Appeals ruled that the court cannot require the plaintiff to reveal his or her encryption key because the state would have access to all the suspect's files and had not specified which ones were of interest.[19] Analyzing the right set of legal responses to this situation is out of scope for this article, but as "Time works changes [and] brings into existence new conditions and purposes,"[20] we note that the extensive use of vulnerabilities/0-day tools could raise new legal issues.

Any shift from carrier-based interception (such as

Practical Concerns

The use of vulnerabilities to enable legally authorized wiretaps raises questions for a variety of communities. For example, the policy community must examine under what circumstances law enforcement's participation in the vulnerabilities market is appropriate. If law enforcement becomes aware that a vulnerability it uses could create serious harm to multiple users or a critical infrastructure, what should its course of action be? What are the national security implications of law enforcement's participation in the vulnerabilities market? Technologists face the issue of "do no harm": an installed vulnerability shouldn't act against anyone but the target (and for the target, the action should be limited to wiretapping the target's communications and not causing other disruption on his or her device).

Another issue is that the vulnerability shouldn't "escape" the target's machine,[1] which might enable the use of the vulnerability by other, nefarious actors. There are additional questions for researchers: What would the sorts of vulnerabilities that law enforcement want to use cost? How would law enforcement's participation in the vulnerabilities market change costs? What's the benefit of using this wiretap data as opposed to the easier-to-obtain stored communications records? All of this returns us to the policy community's issues: online social networks aren't classic communications providers under the law, but they serve many of the same functions. What should their legal responsibilities be?[2] And in an age of ubiquitous online presence, should laws regarding law enforcement's access to communications' transactional data be updated?

References

1. D. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, Crown, 2012.
2. S. Landau, "Testimony before the House of Representatives Committee on the Judiciary, Subcommittee on Crime, Terrorism, and Homeland Security," *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies*, 17 Feb. 2011.

with CALEA) to direct exploitation by law enforcement can make it more difficult to detect extralegal abuse of the interception tools by rogue investigators or agencies. With CALEA, a third party—the telecom carrier—is always involved in provisioning intercepts; exploitation tools, in contrast, can be used unilaterally and potentially without the knowledge of any independent party. We note that this isn't an issue unique to computer interception; many law enforcement capabilities, from deadly weapons to access to sensitive databases, are potentially subject to misuse. Developing robust technical and procedural mechanisms to audit and control the use of, and the data collected by, interception tools must be a central requirement for their expanded use.

A crucial issue, with both legal and technical implications, is the reliability of data gathered by intercept tools. Although a detailed examination of the issue is beyond our scope here, we do note that judges must be convinced that such tools are reliable and trustworthy: such tools must capture exactly the traffic authorized, no more and no less. A tool that misses some traffic might miss exculpatory evidence; a tool that captures too much could lead to confusion over who, precisely, made incriminating comments, and may violate the warrant's limits. Mechanisms that affect third parties' computers, intentionally or accidentally, are especially problematic from this perspective. This is a different issue from minimization, which ensures that the wiretap captures only the subject of an order and only when he or she is engaged in criminal activity. Minimization will also need to be conducted, as it is for any wiretap.

The FBI has dealt with related concerns in deploying the Computer and Internet Protocol Address Verifier (CIPAV),[12] a program that "calls home," meaning that it informs the FBI of a target machine's addressing and protocol data and information such as current IP address, MAC address, open ports, and so on. CIPAV is employed to enable surveillance of the targeted machine.

CIPAV details aren't public, but thanks to documents obtained under the Freedom of Information Act, some information on how the FBI handles the legal aspects of surveilling a target's machine is available.[12] Installing CIPAV requires accessing the target's computer, so first law enforcement seeks a search warrant to install CIPAV on the target's machine. Once it has the IP address and any other information necessary for conducting the surveillance, law enforcement returns to court to obtain a pen register/trap-and-trace order (https://www.eff.org/node/58430). Such a carefully constructed approach might be an appropriate model for law enforcement's use of targeted exploitation tools generally.

Developing a large, well-funded vulnerability exploitation laboratory potentially represents a significant increase in the FBI's technological capabilities. But in a world that's rapidly converting to fully IP-based communications, such capabilities will likely become increasingly important in supporting legally authorized surveillance. Given that law enforcement and intelligence agencies are already using such techniques at a small scale today, it's critical that judges, magistrates, and policymakers be given meaningful technical context for evaluating the impact of the intercept technologies that they're asked to authorize.

Finally, we note that we've focused here on the collection of content; we don't address the issue of data collected by pen registers and trap-and-trace devices. (Pen registers capture dialing, routing, addressing, and signaling information from the target, while trap-and-trace devices capture the information on communications received by the target.) If the communications architecture shares pen register and trap-and-trace data with a service provider, then the information is obtainable from the service provider; however, many highly decentralized architectures, including peer to peer, do not create such records.

When the basic model for voice communications was circuit-switched connections, CALEA was technically feasible even if its security might have been poor. The increasing diversity of local-loop technologies in the 1990s, even with the introduction of ISDN and wireless, still involved the same service (voice telephony) in a landscape that remained both highly regulated and relatively slow moving. The fact that voice communications were circuit-switched meant that you could make a plausible argument for CALEA's approach of shifting wiretaps out of the local loop.

But that argument is no longer applicable in the Internet context. We not only have increased diversity of the local loop (which can be IP-based, DSL, ISDN, or wireless), but we've also increased diversity of the services themselves (voice, email, IM, VoIP, and so on) and of the carrier/ISP infrastructures implementing them. From a situation that had a limited set of service providers providing centralized communications, we've moved to a world with a nearly infinite set of application providers offering highly decentralized ones. The conditions that might have briefly favored the CALEA approach increasingly no longer exist, and they're highly unlikely to return.

By placing wiretapping infrastructure costs on telecommunications carriers, CALEA functioned as a cost-shifting mechanism for the government. But the economic impact of the changes in telecommunications means that the externalities of the CALEA approach—particularly the costs to innovation and security—are now rapidly going up, even while the effectiveness of the CALEA approach is rapidly diminishing.

CALEA effectively imposed a hidden wiretapping tax. Funding a laboratory (such as DCAC) at a level that enables law enforcement to reliably conduct legally authorized surveillance is a much more efficient use of scarce resources and shifts the costs back to the model that existed before CALEA. Passive interception and targeted vulnerability exploitation tools can provide law enforcement with capabilities that give investigators what they need without simultaneously increasing the insecurity of the telecommunications infrastructure.

This latter point is critical. If legally authorized wiretaps are a tool that government occasionally needs, law enforcement will seek viable paths for conducting them. We can either mandate artificially introduced vulnerabilities across all our communications platforms (the CALEA approach), or law enforcement can take advantage of capabilities—the weaknesses that unavoidably occur in complex software systems—that are already there. The latter is ultimately preferable. Software vulnerabilities exist whether law enforcement uses them against its targets or not. By focusing on discovering and exploiting preexisting weaknesses in targets' platforms and ending the business of introducing weaknesses into the communications fabric, law enforcement effectively promotes a national infrastructure that doesn't preclude legally authorized wiretapping but that doesn't create new opportunities for criminal exploitation. This turns us away from the vulnerabilities introduced by the CALEA approach and toward a model where law enforcement supports securing the communications infrastructure, a win for both law enforcement and the broader society. ■

Acknowledgments

We're grateful for the discussions and suggestions made by Herbert Lin, Marty Stansell-Gamm, Lee Tien, Marcus Thomas, and an unnamed reviewer. Their help does not in any way imply endorsement of the ideas presented in this article.

References

1. E. Lichtblau, "Police Are Using Phone Tracking as a Routine Tool," *The New York Times*, 1 Apr. 2012, p. A1.
2. K. Dam and H. Lin, *Cryptography's Role in Securing the Information Society*, Nat'l Academy Press, 1996.
3. S. Landau, *Surveillance or Security? The Risks Posed by New Wiretapping Technologies*, MIT Press, 2011.
4. V. Caproni, "Going Dark: Lawful Electronic Surveillance in the Face of New Technologies," Subcommittee on Crime, Terrorism, and Homeland Security, Committee on Judiciary, 17 Feb. 2011; http://judiciary.house.gov/hearings/hear_02172011.html.
5. D. McCullagh, "FBI Quietly Forms Secretive Net-Surveillance," CNET, 22 May 2012; http://news.cnet.com/8301-1009_3-57439734-83/fbi-quietly-forms-secretive-net-surveillance-unit.
6. A. Gidari, "Designing the Right Wiretap Solution: Setting Standards under CALEA," *IEEE Security & Privacy*, vol. 4, no. 3, 2006, pp. 29–36.
7. S. Bellovin et al., "Security Implications of Applying the Communications Assistance to Law Enforcement Act to

Voice over IP," 2006; http://privacyink.org/pdf/CALEAVOIPreport.pdf.

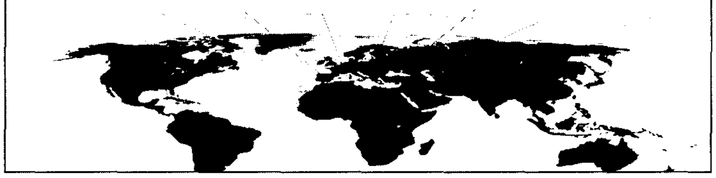
8. Network Working Group, *IETF Policy on Wiretapping*, IETF RFC 2804, May 2000.
9. V. Prevelakis and D. Spinellis, "The Athens Affair," *IEEE Spectrum*, July 2007, pp. 18–25.
10. P. Colaprico, "Da Telecom dossier sui Ds, Mancini parla dei politici," (in Italian), *La Repubblica*, 26 Jan. 2007.
11. S. Landau, "The Large Immortal Machine and the Ticking Time Bomb," *J. Telecommunications and High Technology Law*, vol. 11, no. 1, 2013, pp. 1–43.
12. J. Lynch, "New FBI Documents Provide Details on Government's Surveillance Software," Electronic Frontier Foundation, 29 Apr. 2011; https://www.eff.org/deeplinks/2011/04/new-fbi-documents-show-depth-government#footnote2_01mhuxa.
13. G. Anastasia, "Big Brother and the Bookie," *Mother Jones*, Jan./Feb. 2002.
14. *United States v. Nicodemo S. Scarfo*, et al.
15. Criminal Action No. 00-404 (NHP), US District Court for the District of New Jersey.
16. A. Greenberg, "Shopping for Zero-Days: A Price List for Hackers' Secret Software Exploits," *Forbes*, 23 Mar. 2012; www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/.
17. M. Hofmann and T. Timm, "'Zero-Day' Exploit Sales Should Be Key Point in Cybersecurity Debate," Electronic Frontier Foundation, 29 Mar. 2012; https://www.eff.org/deeplinks/2012/03/zero-day-exploit-sales-should-be-key-point-cybersecurity-debate.
18. B. Schneier, "The Vulnerabilities Market and the Future of Security," *Forbes*, 30 May 2012; www.forbes.com/sites/bruceschneier/2012/05/30/the-vulnerabilities-market-and-the-future-of-security/.
19. L. Bilge and T. Dimitras, "Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World," *Proc. 2012 ACM Conf. on Computer and Communications Security*, ACM, 2012.
20. Grand Jury Subpoena Duces Tecum, 25 Mar. 2011, United States of America, Plaintiff-Appellee, versus John Doe, Defendant-Appellant, for Judges Understanding Capabilities of the Technical Tools in the United States Court of Appeals for the Eleventh Circuit, nos. 11-12268 & 11-15421, DC Docket no. 3:11-mc-00041-LAC.
21. *Weems v. United States*, US Reports, vol. 217, 1910, p. 349.

Steven M. Bellovin is a professor of computer science at Columbia University; he's currently on leave and serving as chief technologist of the Federal Trade Commission. (His work on this article was completed before he joined the FTC; opinions expressed are personal and not those of the FTC.) He works on security, privacy, and related public policy issues. Bellovin has a PhD in computer science from the University of North Carolina at Chapel Hill. He is a member of the ACM. Contact him at smb@cs.columbia.edu.

Matt Blaze directs the Distributed Systems Laboratory at the University of Pennsylvania, where his research focuses on security, privacy, and scale in computing and communications systems. Blaze has a PhD in computer science from Princeton University. Contact him at blaze@cis.upenn.edu.

Sandy Clark is a PhD candidate in the Distributed Systems Lab at the University of Pennsylvania and is advised by Matt Blaze and coadvised by Jonathan Smith. Her research focuses on understanding the mechanisms involved in the computer security arms race. Contact her at clarks@cis.upenn.edu.

Susan Landau works in cybersecurity, privacy, and public policy and is currently a Guggenheim Fellow. She was previously a Distinguished Engineer at Sun Microsystems and a faculty member at the University of Massachusetts Amherst and Wesleyan University. Landau has a PhD from MIT and is a member of AAAS, ACM, AMS, and IEEE. Contact her at susan.landau@privacyink.org.



Emmett, Jamie

From:	Emmett, Jamie
Sent:	May-27-13 11:43 AM
To:	Hawrylak, Maciek; Dyer, Lara; Durand, Mathieu; Thompson, Julie
Cc:	Chayer, Marie-Helene
Subject:	Lawful Access Reference
Follow Up Flag:	Follow up
Flag Status:	Flagged

Tracking:

Recipient	**Read**
Hawrylak, Maciek	
Dyer, Lara	Read: 27/05/2013 11:43 AM
Durand, Mathieu	Read: 27/05/2013 12:05 PM
Thompson, Julie	
Chayer, Marie-Helene	

Morning,

In response to the Via Rail plot arrests, SECU held a briefing session on rail security on 9 May (witness testimony is available at http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=6148233&Language=E&Mode=1&Parl=41&Ses=1). Witnesses included John Davies (NSPD), Gerard McDonald (Transport Canada), Larry Tremblay (RCMP), Michel Coulombe (CSIS), and Marc Tessier, March Beaulieu and Jacques Gagnon (VIA Rail).

There was a question related to the need for Lawful Access legislation and one about the utility of checking VIA passengers against the specified persons list.

Lawful Access:

Hon. Laurie Hawn (Edmonton Centre, CPC): Thank you, Mr.Chair.

Thank you to all our witnesses for appearing on pretty short notice.

I'd like to start with Public Safety Canada, Mr. Davies. You talked about the continuum of prevent, detect, deny, and respond. Obviously we'd like to not get to the respond part. We'd like to stop it earlier. I think the key to that is obviously detection, and to mea key to that is having access to the information that's out there. There's a lot of information out there on the Internet and in other sources.

Do you think we need some kind of legislation that would permit lawful access, under appropriate supervision, to the Internet to detect the kind of activity that leads to what we've just witnessed?

Mr. John Davies: In broad terms, access to information is intelligence. They're synonyms. They go together. Any kind of policy program or legislative improvement that helps law enforcement, our intelligence agencies, access more information to make it lawful to lower risk to Canadians, that's obviously something you want to consider. You want to consider all the pros and cons of doing that and the best way to legislate it, for sure. Obviously information sharing with the private sector, with other parts of government, anything we can do to facilitate that is a good thing in my view.

Hon. Laurie Hawn: I'm guessing that none of the other panellists would disagree with that. I'm not seeing any disagreement, thank you.

Utility of checking VIA passengers against the specified persons list:

Mr. Francis Scarpaleggia: McDonald, correct me if I'm wrong, but every time someone gets on a plane in Canada, their name is checked against an RCMP list or some kind of list to see if they're a person of interest. Or is it just people travelling in and out of Canada, especially to the United States?

Mr. Gerard McDonald: Their names are checked against what is called a specified persons list.

Mr. Francis Scarpaleggia: Is that done for people getting on VIA trains? If not, would it be very expensive and complicated to do it for VIA passenger lists as well?

Mr. Gerard McDonald: It is not done for VIA trains. One would have to assess what the value of that would be before determining whether it would be a worthwhile exercise and whether it would mitigate any security risks.

Mr. Francis Scarpaleggia: Well, I would think that if it mitigates security risks in one area, it would mitigate them in another. We're talking in both cases about mass transit. Obviously, in some ways, I suppose, there's more concern about air travel, but we're talking about probably the same passenger loads, and so on and so forth. Given that there's no screening of baggage that gets on a VIA Rail train, probably there's a good reason to screen the lists. I would suggest that this is something that VIA Rail and the government might want to look at, Mr. Chair.

Ms. Jamie Emmett
Policy Analyst | Analyste des politiques
National Security Operations Directorate | Direction des opérations de la sécurité nationale
Investigative Technologies and Telecommunications Policy | Technologies d'enquêtes et politiques des télécommunications
Public Safety Canada | Sécurité publique Canada
340 Laurier Ave W, Ottawa, ON K1A 0P9
Telephone | Téléphone: 613-993-7645
Fax | Télécopieur: 613-991-4669
Jamie.Emmett@ps-sp.gc.ca
Government of Canada | Gouvernement du Canada

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Public Safety and National Security

SECU • NUMBER 086 • 1st SESSION • 41st PARLIAMENT

EVIDENCE

Thursday, May 9, 2013

Chair

Mr. Kevin Sorenson

Standing Committee on Public Safety and National Security

Thursday, May 9, 2013

● (0845)

[*English*]

The Chair (Mr. Kevin Sorenson (Crowfoot, CPC)): Good morning, everyone.

This meeting number 86 of the Standing Committee on Public Safety and National Security, on Thursday, May 9, 2013.

This morning we're leaving our regular study of the economics of policing, and are responding to a motion that came before our committee and was passed unanimously. That is a briefing on security of rail transport.

With us today we have Gerard McDonald, he is assistant deputy minister of safety and security at Transport Canada; John Davies, director general of national security policy at the department of Public Safety and Emergency Preparedness Canada; Chief Superintendent Larry Tremblay, director general of federal policing criminal operations with the Royal Canadian Mounted Police; Michel Coulombe, the deputy director of operations at the Canadian Security Intelligence Service; and also, from VIA Rail Canada we have Marc Tessier, director of corporate security and regulatory affairs, safety, security, and risk management; Marc Beaulieu, the regional general manager east, and chief of transportation; and Jacques Gagnon, the spokesperson for corporate communications.

Our committee thanks all the witnesses for responding to our request to appear and brief us on rail transport security. Canadians thank you and the public servants responsible for keeping Canada's railways safe. Be assured that Canadians rely on your work as they go about their day-to-day business. We place our trust in the work of the employees, the agents, the officers, and others under your command.

We will have time for questions from the members of Parliament on our committee, following the briefings that you present to us today.

I'll remind members, and also officials who appear here, that we aren't looking for any operational details, so to speak, that may put security at risk. We expect that all those security measures will be non-compromised, and that you will have the ability to determine whether or not that is the fact with the question asked.

We're looking forward to your briefings.

We'll open the floor this morning with Mr. Davies.

Mr. John Davies (Director General, National Security Policy, Department of Public Safety and Emergency Preparedness): Thank you, Mr. Chair.

It may make sense that I go first, as my comments are written at a higher level and will give context to the comments of my colleagues.

As many of you know, Public Safety Canada leads policy development on a number of national security issues. Our role's often one of convenor and facilitator, bringing together the security and intelligence community to develop and improve policy. While the recent arrests in Toronto and Montreal may raise concerns about the threat of terrorism, they also demonstrate the ability of law enforcement and intelligence agencies to work well together.

[*Translation*]

Today, I will focus primarily on the Government of Canada's efforts to counter the threat of terrorism.

[*English*]

Last February, the Minister of Public Safety released "Building Resilience Against Terrorism: Canada's Counter-terrorism Strategy". This document describes a framework within which the 15-plus members of the federal security and intelligence community organize their efforts against terrorism. These efforts are framed around four mutually reinforcing elements, namely preventing, detecting, denying, and responding to terrorism.

Activities in the prevention element focus on the resilience of communities to extremism, helping build their capacity to effectively challenge extremists' narratives. This is a long-term effort. The recent terrorist related arrests in Toronto and Montreal, particularly the supportive reaction by local communities, are good examples of many years of engagement efforts to earn their trust by the RCMP, CSIS, Public Safety, and local police. Last year, for example, the RCMP coordinated over 400 specific outreach sessions to raise awareness among youth and adults of national security issues and of the role key agencies play in countering threats and making communities safer.

● (0850)

[*Translation*]

Furthermore, the Cross Cultural Roundtable on Security, which advises the Minister of Public Safety and the Minister of Justice, brings together leading citizens from diverse communities with extensive experience in social and cultural issues to engage with the government on national security issues.

[*English*]

Efforts in the element of detect aim to identify terrorist threats in a manner that often requires timely sharing of information. Detection requires a strong understanding of the threat environment and the strong intelligence capacity to identify threats. Our knowledge has to keep pace with terrorist groups, their capabilities, and the nature of their plans. To accomplish this task within government, departments and agencies share information for national security purposes every day.

There's a strong link to the third element, denying. Emphasis here is on denying terrorists the means and opportunities to carry out their activities through effective law enforcement and prosecution of terrorists.

The key principle in all of these elements is that of partnership. The RCMP-led integrated and national security enforcement teams —also known as INSETs—are models of partnership and key to our work to detect terrorists and deny them the means and opportunity to carry out their intent. INSETs are staffed by employees from CSIS, CBSA, local law enforcement, and the RCMP. This approach has greatly improved the ability of agencies to work together and has led to many successes, including the recent charges in Montreal and Toronto as well as prior arrests including Momin Khawaja in Ottawa and members of the Toronto 18.

Last year, recognizing the value of this model, the government created a new INSET in Edmonton in addition to the existing ones in Ontario, Quebec, and British Columbia. Note also that under the national strategy and action plan for critical infrastructure, sector networks have been established to facilitate information-sharing and risk-management activities among governments and private sector owners and operators, including rail sector stakeholders.

The rail sectors also represent the national cross-sector forum, which brings together public and private sector partners from all ten critical infrastructure sectors to set priorities and address shared issues such as cyber-security and border management.

Finally our approach to counterterrorism also includes a need for a proportionate and rapid response to any terrorist activities and to mitigating their effects. We have infrastructure in place to communicate with government, and between governments at all levels and private sector owners and operators of critical infrastructure including transportation. In the event of a terrorist incident involving transportation, the government operations centre is connected to other key operation centres across government to manage incidents, including those housed within the RCMP, DND, CSIS, DFAIT, CBSA, and Transport Canada.

Given our shared critical infrastructure with the U.S., there's also close collaboration on critical infrastructure protection and response mechanisms to threats.

[*Translation*]

For a terrorist incident within Canada, or for incidents overseas with a domestic impact, the Government has adopted an all hazards approach to emergency management. This is articulated in the Federal Emergency Response Plan, managed by the Minister of Public Safety.

[*English*]

With that, Mr. Chair, I think I'll leave it there.

Thank you.

The Chair: Thank you, Mr. Davies.

We'll move to the next one on the list. We have Chief Superintendent Larry Tremblay of the Royal Canadian Mounted Police.

C/Supt Larry Tremblay (Director General, Federal Policing Criminal Operations, Royal Canadian Mounted Police): Thank you, Mr. Chair. Good morning and thank you for the opportunity to address this committee on these issues of such concern to Canadians.

You are all aware of the sensitivity of many of the issues we will discuss here today. Some of my answers may reflect the care that must be taken when matters are before the court or when assets and personal security must be the priority.

[*Translation*]

I appreciate the opportunity to provide you with some information about programs and partnerships that the RCMP has developed to assist in keeping Canada's infrastructure, including the railway systems, safe.

[*English*]

The recent success in Project Smooth is a clear demonstration of the effectiveness of our integrated approach. The RCMP integrated national security enforcement teams are responsible for investigating potential threats to Canada's critical infrastructure, including railway systems that support passenger and freight trains. But we cannot do so alone.

At the detachment level, through calls for services, the RCMP works with railway police services and rail operators to support criminal investigations that directly impact rail assets and to ensure railway property is secure against potential criminal threats. Examples of regular collaboration between RCMP, rail police services, municipal police, and rail operators include joint exercises that are held throughout various locations. Scenarios from previous exercises included hostage-taking, bomb threats, hijacking, and an explosive attack against a freight train.

Based on operational requirements, members of the RCMP's Jetway team may also deploy to some train stations and passenger trains to counter organized crime and extremist elements that may exploit rail. In addition to the counterterrorism information officer program, the RCMP has provided training to rail operators on how to recognize behaviour that may be indicative of pre-incident attack planning.

The RCMP critical infrastructure intelligence team maintains information-sharing partnerships with rail police services, municipal transit police units, and rail operators throughout the country. Such partners contribute to the suspicious incident reporting program, which is a secure portal where partners voluntarily report behaviour-based incidents that may be indicative of pre-attack planning by extremists.

Having this network of security-cleared rail operators also allows the RCMP to disseminate regular intelligence reporting to these partners, including threat assessment, bulletins on ongoing investigative files, and analytical reports on suspicious incidents. These products are intended to foster strong partnerships, cultivate a two-way flow of information, as well as generate awareness to a particular issue or call for heightened vigilance where appropriate.

Existing partnerships with rail operators have provided the RCMP with a direct line into the organizations that were collaborating with us during Project Smooth. Such collaboration proved invaluable. For example, the critical infrastructure intelligence team seconded from one of the major railway police services directly supported this project by providing technical information on rail operation.

● (0855)

[*Translation*]

Other rail security initiatives where the RCMP has collaborated include government-sponsored classified briefings for owners and operators of surface transportation assets, including passenger and freight rail services. These briefings are hosted by Transport Canada, a valuable partner in the transportation security file.

[*English*]

In addition, the RCMP participates each year in Public Safety Canada's all hazards risk assessment. This year the RCMP is co-leading a scenario involving an extremist attack on rail infrastructure. Such an assessment is intended to support a future exercise intended to test rail security and emergency response.

Thank you, Mr. Chair.

The Chair: Thanks very much, Chief Superintendent.

We'll now move to Michel Coulombe and CSIS, please.

[*Translation*]

Mr. Michel Coulombe (Deputy Director of Operations, Canadian Security Intelligence Service): Mr. Chair, and members of the committee, good morning.

I am pleased to be here today to discuss issues relating to security threats to critical infrastructure in Canada, and particularly to our rail network.

[*English*]

As members will know, CSIS is mandated to collect, analyze, and advise the Government of Canada on threats to the security of Canada. Since attacks on Canada's critical infrastructure are clear threats against the security of Canada, CSIS works closely with other departments and agencies in protecting our critical infrastructure, notably through the national strategy for critical infrastructure, Canada's cyber-security strategy, and Canada's counterterrorism strategy.

That being said, I would like to clarify for the committee that CSIS is not the lead agency when it comes to critical infrastructure protection. Questions relating to actual rail infrastructure security and practices are best addressed to Transport Canada and the rail companies themselves.

[*Translation*]

What I can speak to is the nature of the threat. Mr. Chair, threats to our critical infrastructure can take many forms. They include: terrorism, such as from groups or individuals directed or inspired by al-Qaeda; domestic issue-motivated extremists, whether right- or left-wing; and foreign states, which may have an interest in stealing Canada's technology or even crippling our infrastructure.

Attacks against critical infrastructure and industrial sabotage are not new in Canada. Indeed, our country has a history of such attacks and plots from a variety of groups, including: the bombing of a transmission tower in Quebec in 2004; the Toronto 18 plot to bomb the Toronto Stock Exchange in 2006; and the bombing of pipelines in British Columbia in 2008-09.

● (0900)

[*English*]

These examples remind us all too well that terrorism is not something that happens only in other countries. There are people in groups here and now who seek to commit acts of violence in Canada and who, given the chance, would kill innocent Canadians and destroy civilian infrastructure. The plot that was foiled last month was going to be carried out here in Canada.

That said, terrorism is a globalized threat, and our security cannot be divorced from that of the international community and from the activities of Canadians abroad. We are also increasingly concerned about lone actors working from often deeply personal or plainly unknown motivations. These individuals are hard to track or anticipate, as they provide few operational leads for investigators and are difficult to profile.

[*Translation*]

Computer hacker groups, or "hacktivists," could also pose a threat, as anyone with a predilection for computers and malevolent motivations could cause serious harm to our infrastructure.

And of course, we must not forget the threat posed by certain states, which could target our critical infrastructure to achieve their own military or economic objectives. Given our mandate, countering state-sponsored threats to our infrastructure remains a key priority for the Service.

[English]

In today's digital world, critical infrastructure networks are almost all linked up in ways that make them vulnerable to attacks, particularly cyber-attacks, and it is not difficult to ascertain the advantages of attacking or sabotaging critical infrastructure. Such attacks could cause significant disruption in transportation and commerce, and lead to important economic losses to the intended target. They can also provide easy and predictable news coverage for the perpetrator's propaganda aims and often boost its recruitment efforts.

Finally, by targeting innocent civilians they instill a sense of fear in the general population. Certainly, different groups operate on somewhat different motives. Al-Qaeda-inspired groups and individuals will almost always wish to kill people. Issue-motivated groups may only target property to send a clear and specific message, and foreign states might seek to advance their defence or trade interests.

On that note, Mr. Chair, I would like to thank you for your attention and I would welcome from members questions on any issues I have raised.

The Chair: Thank you very much, sir.

We'll now move to the Department of Transport, to the assistant deputy minister for safety and security, Gerard McDonald.

Welcome.

[Translation]

Mr. Gerard McDonald (Assistant Deputy Minister, Safety and Security, Department of Transport): Thank you, Mr. Chair.

[English]

Thank you committee members. I appreciate this opportunity to meet with your committee today to provide information about Transport Canada's role in enhancing the security of the rail transportation system.

[Translation]

Let me begin by saying that the safety and security of transportation systems are of the utmost importance to the Government of Canada.

[English]

On April 22, 2013, the RCMP arrested two individuals and charged them with conspiring to carry out a terrorist attack against a VIA train. It's important to note that there was no imminent threat to the general public, rail employees, train passengers, or infrastructure. These arrests, however, have highlighted the importance of continued vigilance within the transportation system.

They have also emphasized that securing rail and urban transit requires a partnership approach including all levels of government, local law enforcement, first responders, operators, and industry associations, supported by a range of tools that can be implemented by operators of all sizes.

Transport Canada works closely with operators to safeguard the security of their operations. For example, in 2007 the Government of Canada renewed a memorandum of understanding on security with the Railway Association of Canada and its members.

[Translation]

As part of the MOU, rail operators are required, amongst other things, to conduct security risk assessments and develop security plans relevant to their operations. Based on the identified risks, operators develop and implement appropriate security practices.

Transport Canada works with MOU signatories and conducts oversight and monitoring activities to help industry meet the terms and conditions of the MOU and promote a more secure rail transportation system. For example, Transport Canada uses regionally located inspectors to audit the extent to which signatories meet the terms and conditions of the MOU. This evaluation process involves assessments and inspections of the important aspects of an operator's security program.

● (0905)

[English]

The government can also exercise various legislative authorities to enhance the security of the rail transportation system in certain circumstances. For example, to enhance security during the 2010 Vancouver Olympics and the G-8 and G-20 in 2010 in Toronto, Transport Canada used security authorities under the Railway Safety Act.

From 2006 to 2009, Transport Canada also managed the Transit-Secure program. This program provided financial assistance on a cost-shared basis to both small and large commuter rail and public transit operators throughout Canada to further enhance their security measures for addressing potential threats of terrorism.

Industry and government also collaborate on the development of voluntary codes of practice on such matters as conducting security risk assessments, developing and maintaining security plans, conducting security exercises, and training and awareness. Transport Canada officials also participate in workshops with rail and transit associations to promote rail security. We have also collaborated with industry in the creation of an intelligence network for the sharing of security intelligence and incident reporting.

[Translation]

In conclusion, I want to reiterate that security is of the utmost importance to the Government of Canada. Security of the transportation system is also everyone's business and is enhanced through partnerships, the promotion of a security culture and awareness across all jurisdictions and sectors.

Thank you again for offering Transport Canada the opportunity to present how it is working to enhance the security of Canada's rail transportation system.

[English]

I would welcome any questions you may have on the work we do in this regard.

Thank you, Mr. Chair.

The Chair: Thank you very much, Mr. McDonald.

We will now move to Montreal to VIA Rail.

I'm not certain whether there is one statement or two. Monsieur Beaulieu, the floor is yours.

Mr. Marc Beaulieu (Regional General Manager, East and Chief of Transporation, Customer Experience, VIA Rail Canada Inc.): Good morning.

My name is Marc Beaulieu. I'm regional general manager and chief of transportation for VIA Rail. I'm happy to be joined today by Marc Tessier, our director of security and regulatory affairs, as well as by Jacques Gagnon, our VIA spokesperson.

[*Translation*]

Mr. Chair, members of the committee, we are pleased to be participating in this meeting by videoconference.

[*English*]

On behalf of VIA Rail Canada, I wish to thank you, Mr. Chair, for our invitation to appear before this committee.

[*Translation*]

VIA Rail's safety and security policies are rigorous and strictly applied. We have high training standards for our employees who work on board trains and those who serve passengers. Our mechanisms for reporting any kind of risk to police authorities are very effective.

[*English*]

Safety and security are paramount at VIA Rail. We recognize and salute the work of law enforcement. Passenger train travel is among the safest and we work diligently to keep it that way. As a member of the Railway Association of Canada, VIA Rail is signatory to the memorandum of understanding on railway security between the Railway Association of Canada and Transport Canada. The memorandum of understanding covers the following essential elements: security plans, training and awareness, exercises, and incident reporting. In compliance with the above, VIA Rail has submitted a security plan that reflects our current security model. The plan is risk-based, using Transport Canada's threat context statements as a basis for risk assessment.

As part of its security plan, VIA Rail has implemented the following programs and procedures. Security awareness training is mandatory for all employees. This training was developed in consultation with the RCMP. A group of front-line employees have also received face-to-face training by members of the RCMP. Management employees with security responsibilities have received training given by the RCMP officers, in conjunction with the Canadian Police College in Ottawa. Intelligence training and certification were also obtained through the Privy Council Office.

VIA Rail routinely conducts security exercises to ensure that programs and procedures are functioning as designed. Part of this process relies on participation of various police forces, including the RCMP, on training exercises that focus on familiarizing officers with VIA Rail operations and equipment, and synchronizing our respective responses. VIA Rail also has procedures in place to ensure the reporting of incidents with a nexus to terrorism to the appropriate authorities. This includes partnership with the RCMP in the suspicious incident reporting initiative and notification to Transport Canada.

Above and beyond these requirements, VIA's security plan also establishes our letter of understanding program, which involves authorizing law enforcement agencies full access to our properties. This empowers the law enforcement agencies to act on our behalf. The RCMP is signatory on several letters of understanding. It enables us to establish strong partnerships and facilitates intelligence gathering and sharing.

VIA partners with host railway police who are responsible for infrastructure protection over a significant portion of the track that VIA Rail operates. VIA also works closely with Transport Canada to participate on various initiatives, committees, and working groups. This work has led to the establishment of the codes of practice that outline industry best practices related to security, security plans, threat and risk assessment, security awareness training, and public awareness.

In conclusion, I would like to thank our law enforcement partners and Transport Canada for continuously helping us improve and be more effective in terms of security. We deliver on our promise to keep the travelling public safe.

● (0910)

[*Translation*]

In closing, I would like to thank law enforcement agencies and Transport Canada for their ongoing support. It allows us to keep our promise to provide secure service for our passengers.

Thank you.

[*English*]

The Chair: Thank you very much, Monsieur Beaulieu.

We will move into the first round of questioning. It's a seven-minute round.

We'll go to Mr. Hawn, please, for seven minutes.

Hon. Laurie Hawn (Edmonton Centre, CPC): Thank you, Mr. Chair.

Thank you to all our witnesses for appearing on pretty short notice.

I'd like to start with Public Safety Canada, Mr. Davies. You talked about the continuum of prevent, detect, deny, and respond. Obviously we'd like to not get to the respond part. We'd like to stop it earlier. I think the key to that is obviously detection, and to me a key to that is having access to the information that's out there. There's a lot of information out there on the Internet and in other sources.

Do you think we need some kind of legislation that would permit lawful access, under appropriate supervision, to the Internet to detect the kind of activity that leads to what we've just witnessed?

Mr. John Davies: In broad terms, access to information is intelligence. They're synonyms. They go together. Any kind of policy program or legislative improvement that helps law enforcement, our intelligence agencies, access more information to make it lawful to lower risk to Canadians, that's obviously something you want to consider. You want to consider all the pros and cons of doing that and the best way to legislate it, for sure. Obviously information sharing with the private sector, with other parts of government, anything we can do to facilitate that is a good thing in my view.

Hon. Laurie Hawn: I'm guessing that none of the other panellists would disagree with that. I'm not seeing any disagreement, thank you.

I'd like to stick with Public Safety, Mr. Davies, for a second. One of my other jobs is as the Canadian co-chair of the Canada-U.S. Permanent Joint Board on Defence. As I'm sure you know, there's a lot of cooperation on that between Public Safety and the Homeland Security side. Could you talk a little bit about...?

We've kind of talked about the Canadian side of this, which obviously ultimately is the most important to us. Can you talk a little bit about the coordination with the U.S. in general terms, or if there is anything sort of specific to rail safety that you could talk about?

● (0915)

Mr. John Davies: Just maybe in general terms and my colleagues can talk about a more specific link to rail. The beyond the border initiative agreement between President Obama and Prime Minister Harper is a big driver of a lot of security-related investments and efforts over the last few years. Of course, one aspect of that is information sharing, working together also on different threat assessments, investments to make the border safer, to push the border out from a permanent perspective.

So a lot of the work we're doing with the U.S. is sort of driven by very concrete objectives linked to the border action plan. The action plan has a number of specific metrics, deliverable dates, and so on. It has really helped energize and open a lot of doors for us with the U. S. and I think vice versa. So that's a big part at least from the national security policy and information-sharing point of view. That's a big piece of the puzzle for us.

Hon. Laurie Hawn: Thank you.

I'd like to turn to VIA Rail now along that same line with respect to MOUs or agreements you have with other rail companies, specifically cross-border. What kinds of arrangements do you have for information sharing, intelligence-sharing cooperation, with other operators, specifically Amtrak?

Mr. Marc Beaulieu: We have a very close relationship with Amtrak. We value our partnership with them. We're in constant communication whether it be operational or security wise. We certainly share information extremely well. As I said, it's an extension. We keep them informed as much as required to make sure that our mutual networks are well informed of any threats.

Hon. Laurie Hawn: Thank you.

To the RCMP now, Superintendent Tremblay, I was lucky enough to be in Edmonton to help announce the integrated national security enforcement teams. So it's a relatively new concept, although I know you've been collaborating forever in these areas, and this has formalized it.

Is that working as planned and is there an international component to that or could you describe at least in broad terms the international component of that with agencies south of the border?

C/Supt Larry Tremblay: Obviously the RCMP works very closely with our U.S. law enforcement partners. The INSETs here in Canada are just a formalized version of the level of cooperation amongst the agencies. Even where we don't have an INSET, there's a high level of collaboration throughout. The INSETs allow us to formalize that and work closely together. The level of sharing at the provincial, federal, and municipal levels is outstanding.

Hon. Laurie Hawn: For CSIS, events change. Things can unfold fairly quickly. I know how you're going to answer this, but I'm going to ask it anyway. How quickly can CSIS adapt? I guess I just want some level of comfort that CSIS is manned and equipped, etc., to adapt fairly quickly when new threats arise or when the landscape changes.

Mr. Michel Coulombe: We are a very nimble organization. That's the nature of the work we do, so we have to adapt all the time. If you go back to moving from more of a CI priority during the Cold War to more of a CT environment today.... The emergence of cyber was also another issue we had to adapt to. So we have the analytical capability and the operational capability to adapt to the emergence of new threats and environments.

Hon. Laurie Hawn: For Transport Canada—because I don't want to leave anybody out—Mr. McDonald, you obviously have Transport Canada's responsibility for transportation, safety, and security. What mechanisms do you use to ensure that operators—whether it's on the rail side or the air transport side, whatever—are in fact fulfilling their obligations?

Mr. Gerard McDonald: We have a number of mechanisms. First and foremost, we conduct oversight of the operators to make sure that they're living up either to our regulatory framework or to the MOUs that we have in place. We've also established security networks in each of the modes where we ensure that operators have people cleared at the appropriate level, at the secret level, so that we can share any information with them that might become available to us in the event that there is a threat to the system. It allows us in concert with them to raise vigilance as appropriate.

● (0920)

Hon. Laurie Hawn: What kind of inspections do you conduct? Do you do things like what we in the air force would call a "no-notice Tac Eval"? Do you do those kinds of exercises?

Mr. Gerard McDonald: We might do that.

In many cases what we'll do, specifically with respect to the rail industry—all of the rail industry has security plans in place—is go in and verify that they are living up to what they say they are going to do in those security plans. We'll also consult with them on the development of their plans, and if required, if we see that something is not there, we may do surprise inspections. It's more often announced, quite frankly.

Hon. Laurie Hawn: Okay.

Going back to the RCMP, Chief Superintendent Tremblay, recently the government's Combating Terrorism Act was passed, giving police new tools and powers to address the threat posed by terrorism. As much as you can say, politically, what is your view of Bill S-7? Is it going to give you some more tools in your tool belt?

The Chair: Go ahead.

C/Supt Larry Tremblay: Thank you.

Obviously I cannot comment on pending legislation, but I can say that we will make use of all tools that are made available to us for law enforcement purposes.

The Chair: Thank you very much.

We'll move to Mr. Garrison, please, for seven minutes.

Mr. Randall Garrison (Esquimalt—Juan de Fuca, NDP): Thank you, Mr. Chair.

I too would like to thank all the witnesses for appearing at short notice.

In particular I extend thanks to VIA Rail and the RCMP for their very quick action on the most recent anti-terrorism case, which of course on our side we believe demonstrates that the tool box is probably full and being made good use of.

I want to start with a question to VIA Rail about how VIA Rail is treated by the government, in terms of anti-terrorism strategies and activities. Are you at VIA Rail treated solely in the same manner as any other private institution, despite the fact that you're a crown corporation?

Mr. Marc Beaulieu: I'll defer that to our director of security.

Mr. Marc Tessier (Director, Corporate Security and Regulatory Affairs, Safety, Security and Risk Management, VIA Rail Canada Inc.): Thank you.

We work very closely with the industry and with the governing agencies, such as Transport Canada. Because of the nature of our business, we have very customer-focused and passenger-focused inspection criteria with Transport Canada. I would say that it is mostly due to the nature of our business, rather than to the fact that we are a crown corporation, that we enjoy that closer relationship.

Mr. Randall Garrison: When it came to something such as the government's anti-terrorism initiative, which started in late 2001 or early 2002, would VIA Rail have been invited to submit proposals for funding for anti-terrorism initiatives under the proposal, or were you simply left with the other, private sector groups to take care of those security things with your own resources?

Mr. Marc Beaulieu: We rely on our own operating budgets to put these plans in place.

Mr. Randall Garrison: What that would indicate is that, under the national strategy and action plan for critical infrastructure, we would find VIA Rail in the transportation sector, under that strategy in 2011. Would that be a good understanding of where you're participating in these initiatives?

Mr. Marc Beaulieu: That's correct.

Mr. Randall Garrison: I'll turn to Mr. Davies from Public Safety.

Was any of the money from the anti-terrorism initiative allocated to critical infrastructure projects?

Mr. John Davies: Are you talking about the PSAT money?

Mr. Randall Garrison: That's right.

Mr. John Davies: I don't have knowledge of the way that money was broken down.

Mr. Randall Garrison: We've had the recent report from the Auditor General that expressed concerns about identifying where the money was spent. One area in which I still have a question concerns whether you would be able, at a later date, to tell us whether any of that money was allocated to national critical infrastructure such as VIA Rail.

Mr. John Davies: I'm certain that some was allocated to the transport sector.

The Chair: Yes, Mr. McDonald?

Mr. Gerard McDonald: Mr. Chair, I may be able to provide a bit of clarification.

One of the programs under that rubric was, as I alluded to earlier, the Transit-Secure program, which identified roughly $115 million to be spent to enhance the security of rail and urban infrastructure.

Under that program, all rail and urban transit operators were eligible to apply. VIA Rail did not apply under that particular program, but they did benefit from security enhancements that were made under the program to Toronto's Union Station and to *gare Centrale* in Montreal.

● (0925)

Mr. Randall Garrison: Going back again to the Auditor General's recent reports, one of the things they identified was some gaps in overall coordination. We have the public safety anti-terrorism initiative in 2001. We have the building resilience against terrorism, Canada's counterterrorism strategy, 2012. We have a national strategy and action plan for critical infrastructure. We have Canada's cyber-security strategy. We have Canada's counterterrorism strategy.

Who is actually coordinating all of the work on the anti-terrorism strategy? How is that coordination done? I know it is officially assigned to Public Safety, but we have this whole set of strategies covering various things. Where does that coordination occur?

Mr. John Davies: For the counterterrorism strategy, Public Safety Canada coordinates, on behalf of the security intelligence community, the implementation of that strategy, likewise for the strategy on critical infrastructure, and it is the same thing for the cyber-strategy.

I'm sorry, I've forgotten the others you mentioned, but at Public Safety, as I mentioned at the beginning of my remarks, we develop policy with the community. We put things together with them and we implement with them as well. It's our job to work with the community, document what has been going on, create the action plans, and report to ministers and to cabinet about how things are going in terms of progress.

Mr. Randall Garrison: If this coordination is going on at Public Safety, how is that related to the coordination of spending on the anti-terrorism initiatives? In other words, you have the coordination of policy aspects, but who is coordinating the assignment of resources to these anti-terrorism things?

Mr. John Davies: Again, if you're talking about the PSAT money, I think that money has run out some time ago. Most resources for departments and agencies are called A-base or normal core funding of these departments.

Are you asking if there are additional resources and who designs where incremental dollars go? Is that what you're asking?

Mr. Randall Garrison: One of the concerns the Auditor General identified was that there was a lack of evidence that proposals for spending under anti-terrorism initiatives were clearly based on threat and risk assessments. So I'm trying to determine who would be responsible for making sure that the money we're spending, whether it's department by department or overall in government, is based, as the Auditor General said, on national threat and risk assessments.

Is that the responsibility of your coordinating groups? Is that the responsibility of Treasury Board?

Mr. John Davies: Again I think you're talking about discrete initiatives of some years ago. Obviously for core spending now, there are departmental performance reports. There are various reports that are public and discussed. Whether it's the estimates, the public accounts, all that kind of normal corporate reporting, that's when those issues are discussed and debated amongst parliamentarians.

The Chair: Thank you, Mr. Garrison. We're out of time.

We'll now move back to Mr. Leef, please.

Mr. Ryan Leef (Yukon, CPC): Thank you, Mr. Chair.

Thank you to all our witnesses.

Since we did really come today to talk about rail security, I'll direct some of my questions to the folks at VIA Rail.

We've heard about partnerships and integrated work and education. I'm just wondering, when we get down to the client level for identifying threats, what kind of work is VIA Rail doing to ensure the passengers and clients of rail services receive the information and education they need to be vigilant?

We heard the RCMP talk about detachment-level work. We heard CSIS talk about how difficult it is to identify lone operators, and if we have threats around the rail sector, obviously we rely heavily on the general public to be aware of these threats.

How well versed do you think Canadians are right now on the actual threat of terrorism? What kind of work does VIA Rail do to encourage vigilance and encourage reporting from the client level?

● (0930)

Mr. Marc Beaulieu: We certainly have some programs that are very effective at increasing employee vigilance. Our locomotive engineers are extremely familiar with their territory, and our front-line employees who deal with our customers, either on our trains or in our stations, are very well trained and experienced at observing and identifying any dangerous situations or suspicious behaviours.

We have technology in place in our stations and facilities with many features, such as cameras, access control, remote locking systems. We have security personnel from VIA Rail and station owners to provide security guards in many locations, and we use contracted security inspectors who are former police officers who travel under cover on some of our trains.

There is no doubt in our minds that our customers are a big part of our solution. Anything that is brought forth to our attention is acted upon very rigorously and very effectively. To answer your question, I'm very confident that people who travel in our mode of transport feel safe, are safe, and we do everything possible to continuously improve our mitigations that are in place.

Mr. Ryan Leef: Thank you.

When you're using any form of public transportation or when you're in any public space generally, you just want to be able to operate, to feel safe, let your guard down, and not be constantly on the lookout. But obviously we've reached a different day. As we heard from CSIS, there are people in groups here and now that are seeking to do us harm.

I was just in Boston a few weeks ago when the attacks occurred there. I'd be the first to admit that in a venue like that, you certainly let your guard down. I'm not sure we ever want to see the day when we're inundated with warning signs. Obviously sometimes the best security is the security you don't see. But we as everyday citizens and people utilizing public transportation for this topic have a role to play.

How do you strike a balance between letting people know where and how to report or educating with signage or with security things, and at the same time, allowing people to exist in an environment where they're not on that proverbial edge of their seat all the time? How do you strike that balance appropriately with VIA Rail?

Mr. Marc Beaulieu: It's through constant training and awareness. We use every opportunity available to us to make sure that the message is clear. Our "keep an eye open" approach and training for our employees is very clear. The first skill that they use is diffusing. Suspicious issues are to be reported immediately. Our operations control centre is directly linked to whatever police forces or support that we require in any event. We test those measures regularly. We use the feedback from our front-line employees and our managers to consistently review any of our processes and procedures to ensure that a balance is reached. When in doubt, always err on the side of safety.

Mr. Ryan Leef: Chief Superintendent Tremblay, the NDP suggested the tool box is full. Would you say that today the tool box for law enforcement is full and that we are on par with terrorism organizations? Are we behind them slightly? Are there things we need to do to make sure that we continually add to that tool box? How are we keeping pace right now?

C/Supt Larry Tremblay: What I can comment on is that the complexity of the threat continues to evolve. It's critical that we reposition to deal with that evolving threat. Again, without being in a position to comment on the proposed legislation, we will make use of all tools available. If tools become available, we will put them to good use.

Mr. Ryan Leef: Thank you.

The Chair: One minute.

Mr. Ryan Leef: One minute? Thank you, Mr. Chair.

You described work at the detachment levels. How important do you think the work at the detachment level is in terms of community education and engagement, in contrast to the work at the more discreet levels of enforcement?

● (0935)

C/Supt Larry Tremblay: It's absolutely critical. I think the recent arrests, and the more public recent arrests, show the level of collaboration among the various agencies and collaboration with the private sector. But prevention of terrorist-related activity is very much a shared responsibility. It can't be left to the police alone or to the agency alone. The engagement of community leaders and the engagement of the public is absolutely critical in the detect, deny, and prevent phase.

The Chair: Thank you very much.

We'll move to Mr. Scarpaleggia, please, for seven minutes.

Mr. Francis Scarpaleggia (Lac-Saint-Louis, Lib.): Thank you very much, Chair, and thank you to all the witnesses for being here. Thank you to the committee for agreeing to our Liberal motion to have this hearing. We also would have liked to have had some outside experts, not because we don't have faith in the work that you're all doing, but just to test the resilience of your responses perhaps.

I'd like to get down to a little bit of a more specific level. We've heard about strategies, coordination, and memoranda of understanding. But I was wondering, Mr. Beaulieu, if you could tell me or the committee how many incidents there have been on the VIA Rail train service in the last year. You say there are people trained to respond to incidents. Obviously we're not talking about terrorist attacks here. We're just talking about incidents on trains where the porters or someone else—one of your plainclothes marshals—would have to intervene in some way. From something very simple to something like, for example, a passenger needing to be taken off the train.

Mr. Marc Beaulieu: To the exact number of incidents, I would not be able to answer that, but I could certainly recover it from our database as required and get you that information later. I can tell you that our employees are extremely vigilant, and they apply the processes extremely well.

Police forces across the country, when required, respond extremely effectively. To my knowledge, never have we contacted any police force for support that didn't respond swiftly and effectively to our needs. Yes, we have detrained customers on occasion, unfortunately, because it was our only option at that time.

We also are extremely well skilled at identifying any suspicious baggage, and again, the police forces respond extremely effectively to all those needs. I can say that, to my knowledge, it has happened at least eight to 10 times this year, without being too specific, because I don't have the database in front of me, but numerous times. Each was responded to extremely effectively by all involved on every occasion.

Mr. Francis Scarpaleggia: You're telling me there have been incidents and people have been taken off the train and baggage has been taken off the train. So, yes, we would appreciate getting information on the number of times this has occurred, and perhaps on an annual basis for the last three to five years. That would be helpful.

You say you have security cameras in the stations. What do these security cameras tell you? As you know, there's a debate in the United States as to whether security cameras are an effective deterrent. We know they obviously help in apprehending those who've committed offences, but there's a big debate as to whether they are a deterrent.

So I'm just wondering, have your security cameras been helpful in terms of perhaps preventing someone from boarding a train who, based on a security camera, was exhibiting maybe odd behaviour or something like that?

Mr. Marc Beaulieu: I can't answer that specific question of somebody having odd behaviour. I know that we have used our security cameras to recover stolen items and identify a perpetrator of a crime, but I don't have a specific example of having detected somebody with suspicious behaviour with our camera systems per se.

● (0940)

Mr. Francis Scarpaleggia: I would also like to, at this point, follow up on something that came out of the Auditor General's report and that Mr. Garrison raised, which is that nobody seems to be able to tell us how much is being spent on anti-terrorism or cyber-security in this country.

I remember when the minister appeared. I think it was either last month or two months ago. We asked him if he could give us a number for how much the Government of Canada spends on the fight for cyber-security, and the only answer we got from the minister was, well, consult the estimates in all the different departments that are involved. I think this is something that is concerning, not only to the Auditor General but to members of Parliament and to the public.

Mr. McDonald, in your department, in your unit, will there be any diminution of resources in the coming years, maybe next year or the year after, as a result of budget cutting, for example? Would you be considered front line or back room? If you're front line, we've been told by the government that there will be no reductions in expenditures or manpower, but we've been told that back office services could see some cuts.

I'd like to know if you're being squeezed, or if your budget is being squeezed, to the extent that you may not be able to do the fine work that you do as well in the future. Are you being asked to come up with efficiencies that maybe, quite frankly, are not there to be had?

Mr. Gerard McDonald: In response to your question of whether we're front line or back room, in fact we're both. We exercise the functional responsibility for our safety and security programs. Then we also deliver those programs on the front line through our inspectors and what have you in the regions and at headquarters.

Our programs have been subject to the same reductions that have been absorbed by other departments around the country. But that being said, we made a specific effort not to cut any front-line resources, not to reduce any of our inspectors out in the field, but to look more at administrative, organization, and overhead-type expenses in order to meet the budget reductions that have been imposed on us.

Mr. Francis Scarpaleggia: Thank you.

Mr. Beaulieu, if somebody comes to buy a ticket at the local train station and they want to pay cash, do you just take the cash and give them a ticket, or does that raise a red flag?

Mr. Marc Beaulieu: All purchases paid with cash raise a red flag. There are other indicators, such as one-way trips, nervousness, other behaviours that are communicated through training and awareness to our employees. Any such incidents can be easily reported and followed up on.

The Chair: Thank you very much, Mr. Scarpaleggia.

We'll now move to Madame Michaud for five minutes. The second round is a five-minute round.

[*Translation*]

Ms. Élaine Michaud (Portneuf—Jacques-Cartier, NDP): I would like to thank you for being here today.

I would like to build on the questions asked by my colleague, Mr. Garrison.

You mentioned that many departments and agencies, including yours, experienced budget cuts. This began with budget 2012, when the Canada Border Services Agency absorbed cuts of $143 million, which resulted in the elimination of 325 jobs at border crossings across the country. The Canadian Security Intelligence Service will have its budget cut by almost $24.5 million in 2015. This is going to happen. The RCMP has been subjected to reductions of $195.2 million and more cuts are expected in budget 2013. It is expected that spending will be slashed by 29.8% in 2013-14 compared to 2012-13.

Cuts are being made in different departments and the work is being done in silos. However, is there a global assessment of how every cut and every new measure implemented affects the capacity of various departments and agencies to counter terrorism and protect Canada's national security?

Mr. John Davies: Thank you for your question.

● (0945)

[*English*]

Is it an overall analysis, from a national security point of view, of what the totality of cuts has meant to the community across the board that you're asking for?

[*Translation*]

Ms. Élaine Michaud: Yes, exactly. I want to know if the cumulative effect of all the cuts has been assessed. Different human resources are being eliminated. What are the effects on the ground of all these initiatives?

[*English*]

Mr. Ryan Leef: I have a point of order.

The Chair: I'll hear Mr. Leef on a point of order.

Mr. Ryan Leef: Mr. Chair, I think, in fairness to our witnesses, that these broad-based questions about departmental cuts and across the spectrum cuts are not fair. We asked them to come here to answer questions about the safety of Canada's rail system. If the members opposite have direct questions about budgetary measures that would directly impact transport or rail safety, I think it might be fair for the witnesses to answer, but I don't think to ask them on a completely departmental level is fair.

The Chair: Thank you, Mr. Leef. In fact I asked our clerk for the motion that we've asked them to appear on, and I should remind the committee that we have asked them to appear at a meeting to brief the committee on current modes, systems, and procedures for protecting rail transport in Canada, passengers, and freight against terrorism.

I think what Mr. Leef says is probably correct. I would encourage you.... The broad question of whether there have been cuts that have affected the safety of rail...but we're more specifically looking into the procedures for protecting rail transport in Canada: the systems, the modes, not the overall question of budgetary....

Go ahead.

Ms. Élaine Michaud: If it's going to be a point of order and not on my time, I want to answer to that.

The Chair: It's definitely not on your time. We haven't taken your time off.

[*Translation*]

Ms. Élaine Michaud: All right, that is perfect.

In fact, in the presentations, some witnesses told us that they wanted to look at the broader issues. Thus, I am responding to the presentations made here. The witnesses themselves wanted to address these broader issues. Therefore, in that context, I believe that my questions are in keeping with the rules.

[*English*]

The Chair: I'll watch it. I hadn't interjected myself yet, because I think your questioning was getting close to the edge here. We want a briefing on the systems, the procedures, and the modes of security on transport.

Continue, please.

[*Translation*]

Ms. Élaine Michaud: I will.

Mr. Davies, could you speak to that?

[*English*]

Mr. John Davies: In very broad terms, during the deficit reduction action plan discussions, the national security advisor, together with other deputies from the community, met consistently to discuss the impact of cuts on national security. There was an ongoing dialogue among deputies during that time.

[*Translation*]

Ms. Élaine Michaud: Thank you very much.

I will now ask Mr. Tremblay a question that addresses the concerns of my colleagues opposite, I believe.

I referred to the cuts at the RCMP. Does this have a direct effect on your ability to work with VIA Rail to protect the security of railways and counter possible terrorist attacks?

C/Supt Larry Tremblay: Thank you for your question.

[*English*]

Mr. Chair, in very broad terms we believe that the recent arrests have demonstrated that we do possess the ability, in close collaboration with the S and I community and various departments within the GOC, to work with the private sector to counter what was a very serious terrorist threat to the rail system.

I'm not sure that I can go into more detail than that.

[*Translation*]

Ms. Élaine Michaud: Thank you very much.

My next question is for Mr. McDonald.

Earlier, you started talking about certain programs of the public security and anti-terrorism initiative, which allowed Transport Canada, among others, to collaborate with VIA Rail on railway security.

Could you expand on what you said? We know that there are a lot of programs in this initiative, and that it is difficult to track where the money was invested, the results and where any residual money went.

Could you tell us more about certain other initiatives you used to ensure the security of our railways?

Mr. Gerard McDonald: Thank you for your question.

[*English*]

As I indicated earlier, we've had two major initiatives. One is the Transit-Secure program that ran from 2006 to 2009, I believe. That was to improve security at railway stations and operations, and urban transit operations. That provided funding for our organizations to improve what they had.

● (0950)

[*Translation*]

Ms. Élaine Michaud: Allow me to clarify something about this program.

[*English*]

The Chair: Just let him finish. We're out of time.

Mr. Gerard McDonald: It funded things such as construction equipment, training, public awareness, signage, internal assessments, surveillance technologies, infrastructure in these locations, security centres, and access control measures.

As I indicated, we also have the MOU with the railways. We work regularly with the railways to enhance the MOU, make sure that it's lived up to, and ensure that the railways are meeting their obligations in that regard.

The Chair: Thank you very much, Mr. McDonald.

We'll now move back to the government, to Mr. Norlock, please.

Mr. Rick Norlock (Northumberland—Quinte West, CPC): Thank you very much, Mr. Chair.

Through you to the witnesses, thank you for appearing today.

Just to set the record straight, the Auditor General said that we didn't find anything that gave us concern that the money was used in any way it should not have been. Then when he appeared before committee—

Mr. John Rafferty (Thunder Bay—Rainy River, NDP): On a point of order. I don't think that we're talking about that anymore.

Mr. Rick Norlock: Absolutely, Mr. Chair, they're not going to get away with misinformation. I'm speaking to my constituents at home. They've been somewhat misled by the type of questioning that goes on here. There has been no misappropriation and at the department —

The Chair: Go ahead.

Mr. John Rafferty: It's exactly the same as Mr. Leef's point. We've left that line of questioning. I will certainly return to that if you wish, when it's my turn.

The Chair: Mr. Norlock, maybe word it in a way or—

Mr. Rick Norlock: Let me go to another issue.

One of the questions had to do with CBSA and cuts. If I remember correctly, Mr. Chair, looking at some of our past budgets—and if any of the witnesses who may be directly responsible for CBSA want to confirm this—we've increased front-line.... Number one, because terrorists are not nice people, we've armed our border guards for their safety and the safety of Canadians. Number two, we've increased front-line CBSA officers to 26%.

But if I might go to the VIA Rail folks and the RCMP with regard to security cameras, based on my 30 years of policing, security cameras have in the past and continue.... I'll go right to the RCMP. Wouldn't the proof of the pudding with regard to security cameras in areas of concern and in our cities and towns, in your opinion and based on the Boston experience.... Security cameras significantly reduced the investigation time in order to catch the bad guys. Wouldn't that be true, Chief Superintendent?

C/Supt Larry Tremblay: Thank you.

I think security cameras have been used by law enforcement in order to bring facts within the evidence chain. So we have made use of security cameras for law enforcement purposes. It has been extensively used for evidence purposes in court.

Mr. Rick Norlock: Thank you very much.

This question is for Mr. Coulombe. Can you describe the role CSIS has in the counterterrorism strategy that was announced by this government in 2012?

Mr. Michel Coulombe: If you look at our mandate, we obviously have a role in all four phases—detect, prevent, deny, response—but to different degrees.

I think it's pretty obvious in terms of detect and prevent what our role would be, and response also. If there is an incident or an investigation we will collaborate with the RCMP, so we would also have a role in the response phase. We do have a role in all four phases to different degrees.

Mr. Rick Norlock: Thank you very much.

I have a question again for the RCMP and perhaps our folks at VIA Rail. Can you describe specifically the collaboration between the RCMP and rail operators? I'm thinking of the CN and CP police who provide a vital function along those lines used by VIA. Perhaps the VIA folks can chime in if they see an area they want to talk about with regard to collaboration with those two police services, vis-à-vis their rail operations.

C/Supt Larry Tremblay: Because of the ongoing case, I can't go into detail now, but I can easily say that we have, from the onset of this investigation, been working hand in hand with VIA and CN police in order to assist in the investigation and ensure public safety. The collaboration was seamless. It was an open door both ways into how we can work together to prevent this threat. This relationship is established and ongoing.

● (0955)

Mr. Rick Norlock: Thank you.

Mr. Beaulieu, any comments with regard to—

Mr. Marc Beaulieu: Yes, I completely concur with that statement. The collaboration and cooperation is second to none. Whether it be with the RCMP, local law enforcement agencies, CN and CP, our network is very rigorous and we communicate extremely well.

The Chair: Very quickly, Mr. Norlock, you have 30 seconds.

Mr. Rick Norlock: I have a quick question for CSIS. The possibility of a terrorist threat is on many people's minds, given recent events. Have these events dramatically changed anything in regard to the standard operating procedures of CSIS?

Mr. Michel Coulombe: My quick response is no.

Mr. Rick Norlock: Great. Thank you.

The Chair: Thank you very much.

We'll now move back to the opposition and Monsieur Rousseau.

[*Translation*]

Mr. Jean Rousseau (Compton—Stanstead, NDP): Thank you very much, Mr. Chair.

With respect to operations, there are six border crossings in my riding. Some of them, like Chartierville, Stanhope and Saint-Herménégilde are fairly isolated. In the region, there are sometimes hundreds of kilometres of forest between different border crossings. Let us be frank. In outlying areas of the Eastern Townships, people have crossed the border and been found wandering in different municipalities. There have even been cases of mischief committed in my riding by people who simply crossed the border through the forest.

Every time that we speak to people at the Canada Border Services Agency, the RCMP, or the Sûreté du Québec—the Sûreté du Québec patrols certain areas of Quebec because other border services lack the resources to do so—they tell us that information sharing between the various services is difficult and ineffective, that there is information, but that they cannot use it.

My question is for Mr. Davies and also Mr. Tremblay, or Mr. McDonald, to whom I will address another question a little later.

Why am I hearing about those kinds of situations, when you are telling me that everything is going relatively well and that operations are very successful and very effective?

I will give you an example. Although very effective operations have been conducted in Stanstead, there have been unfortunate situations in the past, and they continue to occur, because of the fact that hundreds of kilometres of forest are wide open.

How is the surveillance carried out? How can we reassure people, tell them that there is security and, above all, that there are patrols?

[*English*]

Mr. John Davies: Unfortunately I don't have a great answer for you. The CBSA would be well placed to give you a bit more detail, operationally, on how things are working at the border and what their efforts are for interoperability, dealing with local communities, and any posts that would be isolated and the challenges they face.

I'm not sure if others have any....

The Chair: Mr. Rousseau, could you again be more specific to rail, perhaps? I appreciate you have those.... Yes, go ahead.

[*Translation*]

Mr. Jean Rousseau: All right.

In my riding, there is a small railway service that belongs to the St. Lawrence and Atlantic Railroad, which only ships freight. Two railway lines cross the border in my area, the Eastern Townships. This company is owned by Genesee & Wyoming Inc., which manages the shipping. It seems that it also owns railway cars.

How does the information sharing and training that you mentioned take place? You say that communications and training keep people up-to-date on rail security. This small line only carries freight, but at least one or two trains cross the border every day. Are these trains searched. How are searches conducted?

Furthermore, there are level crossings that are in a poor state of repair. Traffic has been tied up for days because the St. Lawrence and Atlantic Railroad has not assumed responsibility for repairing and upgrading these level crossings. The Department of Transport officials say that the municipality should have that responsibility. Therefore, who is responsible for what? It seems to me that there are holes in the system.

● (1000)

[*English*]

Mr. Gerard McDonald: Mr. Chair, I think that falls into my capacity. I'm not sure if I understand all the questions.

In terms of searching these trains when they're crossing the border, that's a CBSA responsibility. I can't respond to that.

With respect to the security of the operations of an organization like the St. Lawrence and Atlantic Railroad, they're part of the MOU with the Railway Association of Canada, so they have a responsibility to have a security plan. They have to assess what their risks are and have a plan to be able to respond to mitigate those risks.

Obviously a short-line railway, with the type of merchandise it's carrying, is not going to have as detailed a plan as VIA Rail, which is carrying passengers across the country. So they have that plan. They work with us. They work with the Railway Association of Canada. We assess their plan to make sure that it meets the requirements, that they have adequately assessed the risks, and that they have mitigation measures in place to address them.

Finally, with respect to level crossings and how they get funded, as you may be aware, we do have a grade-crossing contribution program to which all railways can apply. It's funded on a 50-50 basis between the federal government, and the municipalities and the railways. The federal government is one side; the municipalities and railways are on the other. That is one way to get funding to improve level crossings.

Yes, there is a jurisdictional issue, obviously, between railways and municipalities. It exists everywhere in the country. We try to work through it as best we can. In many cases we are successful in doing that and in improving the safety of those level crossings.

The Chair: Thank you, Mr. McDonald.

We'll now move to Mr. Payne, please, for five minutes.

Mr. LaVar Payne (Medicine Hat, CPC): Thank you, Chair.

Thank you to all the witnesses for coming in. It's certainly important to talk about some of the issues we've heard already.

Mr. McDonald, just on your point, I actually just recently announced a number of dollars that went into funding right across my riding. There are probably at least a half-dozen different crossings that are being upgraded for safety purposes, which is extremely important, I think, for the communities, for the citizens who might be using those roadways. That's an important aspect.

Mr. Davies, in your comments you talked about how we have infrastructure in place to communicate with government at all levels, private sector, and operators of critical infrastructure—obviously including transportation. Could you maybe give us a little better feel for what "critical infrastructure" might be?

Mr. John Davies: Do you mean what the 10 sectors are, how the plan worked, and so on?

Mr. LaVar Payne: Yes.

Mr. John Davies: I'll do my best. Critical infrastructure is not my direct responsibility, but in 2010 the Minister of Public Safety, together with his counterparts in the provinces, announced the national strategy for critical infrastructure. Essentially this is a plan to address threats to vital assets in systems, like financial systems, transport networks, electricity grids, and so on. It's more or less a vision for building public-private partnerships, improving information sharing among levels of government with the private sector on risks and threats, and conducting risk management activities and exercises.

The chief superintendent talked a bit about those kinds of exercises, but there are a number of working groups by sector, and those sectors roll up once a year into a national forum. They receive classified briefings on threats and risks, exchange information on building risk methodologies, and so on. There's also, in a sense, a counterpart to that of work with the United States, given how our critical infrastructure entwines with theirs to some degree.

Mr. LaVar Payne: Okay. Thank you.

Mr. McDonald, I just wanted to touch a bit more on the railway. I'm from western Canada, and in my riding I have a couple of major petrochemical or fertilizer producers. Of course, they do ship a lot of goods such as ammonia and methanol, and they do travel across the border. That's done through CPR because that's the only railway we have. I'm just wondering what the communication is between Transport Canada and CPR, their plans, particularly with carrying these types of products. Obviously when you think about it, certainly terrorism could be a major issue.

If anyone else has a comment on that, I'd certainly appreciate that as well.

● (1005)

Mr. Gerard McDonald: With respect to that, those are goods we would classify as dangerous goods. They are covered under the Transportation of Dangerous Goods Act. First and foremost, they have to have an appropriate means of containment to transport those goods. They also have to have what we call an ERAP, an emergency response activation plan, so that if anything goes wrong, they have a plan in place and they can activate that plan should it be necessary.

We also have provisions now within the TDG Act for security measures for goods that could be considered for the use of terrorism or what have you. We're in the process of developing regulations in that regard as to what measures we might want to use should a security situation arise.

Mr. LaVar Payne: Is there anyone who wants to comment on those? No?

Certainly we want to commend the RCMP on their recent performance in stopping the potential terrorism act. I'm wondering if you could describe what work or collaboration occurred to make those arrests possible, without, obviously, divulging sensitive information.

C/Supt Larry Tremblay: Thank you, sir, for your comment.

I think it's critical. We all recognize that terrorism is a global phenomenon, so the response must be in line with that reality. Any terrorism-related investigation will activate cooperation not only within the Canadian government but with partners and allies, most often with our U.S. ally's law enforcement agency. This project was just another example of that.

Mr. LaVar Payne: Okay.

How much time do I have?

The Chair: You have five seconds. We'll just maybe credit you with that until the next meeting.

We'll go to Mr. Rafferty, please.

Mr. John Rafferty: Thank you very much, Chair.

I do appreciate Mr. Leef's point of order because we've already heard in this committee previously from the RCMP that their cuts to 2015 of $195.2 million are not going to impact public safety, and also from CSIS that a $24.5 million cut is not going to affect public safety. We don't need to talk about budget cuts anymore. Thank you, Mr. Leef, for that point of order.

I guess it's good because you were just wasting that money before.

Let me ask a question about who's in charge. You talk about building resilience against terrorism, about the 15-plus members of the security network, and about shared responsibilities. We've heard that a couple of times. Where does the buck stop? Who is actually coordinating that? Is there a pyramid there, or is everybody sort of acting independently and helping each other whenever they need some help?

Yes, Mr. Davies, please.

Mr. John Davies: The Prime Minister, I think, is where the buck stops. Under him is the Minister of Public Safety, and obviously the counterterrorism strategy is something that he released, but it was done in cooperation with the Minister of Foreign Affairs, the Minister of Justice, the Minister of Transport, and so on.

In terms of the kind of binding leadership role, the Minister of Public Safety plays a big part in that, given his portfolio includes CSIS, the RCMP, and CBSA, and those are three core members of the security intelligence community.

Mr. John Rafferty: Is there a coordinating body that sort of keeps an eye on all those agencies, that sort of gives direction?

Mr. John Davies: Certainly there's a series of deputy-level committees that meet frequently, almost weekly, to talk about emerging issues, whether those are threat issues or new policy or legislation. Those committees advise ministers, right up to the Cabinet Committee on National Security, which is a new creation of the Prime Minister. I believe it's two years old now.

● (1010)

Mr. John Rafferty: I guess I'm just trying to get a sense of the relationship between the agencies and then maybe the Prime Minister, who, as you say, is the boss.

This is a question for VIA Rail. Let's say you call in a police service and the incident is resolved. Do you get billed for that? How does that work? Let's say you're using the RCMP services, or in Ontario, the OPP. Do they send you a bill later for the help they gave you?

Mr. Marc Beaulieu: No. We don't get billed for such incidents. If the police are called in for dangerous situations that threaten security or safety and take whatever action is necessary according to their experience, they do not invoice us for that.

Mr. John Rafferty: Okay. That doesn't happen anywhere in the system, right? There's no cost recovery there anywhere. Everybody just sort of helps when they're called upon.

This is also a question for VIA Rail. As you know, you have kilometres and kilometres of track that is unsupervised—

Mr. Marc Beaulieu: It's 46,000.

Mr. John Rafferty: It's 46,000? Really, no one can police that; it's so huge. I know that in northern Ontario, where VIA Rail is not, but CN and CP are, just stopping people from trespassing is almost an impossible task. How does VIA Rail monitor that, to the best of your ability? How does that happen?

Mr. Marc Beaulieu: We rely heavily on the experience of our locomotive engineers and on-train employees, who are well trained in identifying any areas of concern. They immediately report any incidents to the rail traffic controllers, who then in turn immediately contact police for intervention. They are of course very skilled individuals who operate over this territory for a living, and they know every turn and switch along the way. They are very good at immediately reporting any incident or behaviour that needs to be reported.

The Chair: Thank you very much.

We'll now move back to Mr. Gill, please, for five minutes.

Mr. Parm Gill (Brampton—Springdale, CPC): Thank you, Mr. Chair.

I also want to thank all the witnesses for their time. I know that it was short notice, so we appreciate you appearing before the committee.

My question is first for VIA Rail. Obviously, this is basically related to your clients, your customers, who take the rail on a regular basis. What sort of cooperation do you get from them in terms of any concerns or any issues they may have or may be concerned about? Do you regularly get any sort of reporting from individuals, just your customers, such as, "Hey, we're concerned about a certain individual", or a package, say, or just on general safety concerns?

Mr. Marc Beaulieu: Yes, we certainly receive such information, and we act upon it quickly. We regularly call upon local law enforcement, or whatever enforcement we need, to further those investigations. They're acted upon very promptly and effectively whenever they're brought to our attention by a customer or one of our employees using our "keep an eye open" approach.

Mr. Parm Gill: How would they normally contact you? What's the method used most often?

Mr. Marc Beaulieu: Usually through contact with our employees, or I suppose they would call 911. All the police forces can get a hold of us very quickly. The network works extremely well. We rely heavily on our infrastructure owners as well, who do an extremely good job of having track forces out there and signaling any incidents to us. Our primary contact is our employees, our operations control centre, or simply by calling the local police.

● (1015)

Mr. Parm Gill: Are there any educational components available to your passengers, to the general public, any sort of signage—be it on the rail itself, or in the waiting areas, and so on—of what to look for if they feel unsafe, or if there's any sort of suspicious activity or a suspicious person? Are there telephone numbers of a law enforcement agency posted, or is it just 911?

Mr. Marc Beaulieu: My understanding is that the best way to alert somebody of a dangerous or suspicious situation quickly is to dial 911. We rely heavily on our partnerships with all the police forces, and CN and CP police forces, and our operating partners, to respond quickly and effectively.

Mr. Parm Gill: But is there actual signage available or an educational component of what to look for and who to call in case?

Mr. Marc Beaulieu: We have "travelling better together" programs to inform passengers of behaviours that are and are not tolerated. Again, we don't have a public awareness campaign with the number to reach us if there's a security threat. They're to use the quickest means to alert the proper authorities.

Mr. Parm Gill: The other question I have is, when it comes to railway security, how well equipped would you say we are here in Canada in comparison to some of the other countries that have a similar railway system in place?

How would you rate us, as a country, in being prepared to tackle any of these threats—safety, security?

Mr. Gerard McDonald: I'll try to answer that.

Obviously, it's very different. Probably the biggest similarity to the rail structure we have in Canada is that of the States. With Europe and the Asian countries, their systems operate in a highly urbanized environment, which is much different from how we operate in Canada. Given the threats we have in the system, we feel we have adequate response plans prepared to address the risks we perceive to be there.

The Chair: Thank you, Mr. Gill.

It's still another government-round question. I'll ask one quick question and then we'll go to Mr. Leef.

After asking all of you not to give away any operational type of issues that might hinder security, I guess I would ask this. How often do you meet with the RCMP? For example, in the last event, I take it that you didn't just wake up one morning and see that VIA Rail was in the news. You obviously must have been aware of some ongoing investigation.

Is this a natural thing, where you meet with them once a week or they'll give you a heads-up that there may be an investigation under way and to tighten up some of your security? Does that type of thing happen, Mr. Tessier or Mr. Beaulieu?

Mr. Tessier, go ahead.

Mr. Marc Tessier: Yes, thank you.

We have regular contacts with the RCMP. As far as the recent event, yes, we had received previous notification. As I said, we have ongoing communication between VIA Rail security and the RCMP, as well as other law enforcement agencies, and Transport Canada.

The Chair: In terms of notification, then, are there certain steps you take immediately, based on that, which your locomotive engineers, or your porters or conductors, would realize are out of the norm?

Mr. Marc Tessier: As far as the last incident is concerned, VIA Rail was notified, and we were under the guidance of the RCMP. That's all I can say about that.

● (1020)

The Chair: Whatever process or whatever strategy you took, it obviously worked, so we're very pleased. I think we all have confidence that.... Obviously, the communication, then, between the RCMP and VIA Rail was very good. You were able, in whatever way you did it, to contact your conductors without giving away anything. I think Canadians can be confident in that.

We'll go to Mr. Leef, please.

Mr. Ryan Leef: Thank you, Mr. Chair.

This is another question for VIA Rail. We have talked a lot about the prevention strategies that are in place. Of course, it's a priority for our government, and I think obviously a priority for you at VIA Rail, to make sure that incidents don't happen in the first place. But maybe we can move to the response end of it, because I don't think we've touched on that a lot.

It is recognized a lot of times that when disaster strikes, your survivability of an incident, or the mitigation of harm, has as much to do with your response to it as it does the event itself. On that end, what kind of work is VIA Rail doing with integrated partnerships to ensure a safe and appropriate response to anything that might occur on a medium or larger scale?

Mr. Marc Beaulieu: We've participated in exercises with local police and the RCMP to develop our skills and knowledge on first response. Depending on the location, the site could be taken control of by the infrastructure owner themselves. We work very well in partnership with the infrastructure owners, with the RCMP, and with Transport Canada to coordinate these exercises, to practise how they go.

We have an operations control centre that is open 24 hours a day, seven days a week, in constant communication with whatever governing bodies we require, or infrastructure owners, to keep an eye. For anything that is signalled to us, we have identified an appropriate response per type of occurrence. We use it efficiently whenever required.

Mr. Ryan Leef: Do you engage other emergency services, such as local fire and ambulance or other emergency responders, in that training?

Mr. Marc Beaulieu: We would contact any agency required, depending on the type of emergency it is, whether it be fire, ambulance, police, or Transport Canada. For any means that we need to mitigate the risk that has been identified to us, we have an appropriate response plan.

Mr. Ryan Leef: Thank you.

Mr. McDonald, we're focused on rail, of course, but does Transport have similar plans with other public safety transport, and does that include appropriate legislation for public transport? Some of these transport systems are integrated. You take a bus to take a train to take a plane.

Maybe you could just touch on that a bit.

Mr. Gerard McDonald: Sure. It really depends on the type of mode. Some of the requirements we have are legislated, and we do have regulations in that regard. With others, as with the rail industry, we work through a memorandum of agreement.

The objective for us is to achieve a certain behaviour as opposed to passing laws and regulations. It's making sure that the industry's prepared, that they've assessed the risk, and that they know what they're doing and how to respond to it.

Mr. Ryan Leef: Great. Thank you.

I'll go back to VIA Rail again. Obviously, with the security market nowadays, there's a host of products, programs, and systems available to choose from. When you're making decisions about the suite of security programs and security measures that you buy or integrate into your system, at even the smallest of levels, how do you go about making those decisions? Are they evidence-based, operationally appropriate decisions, keeping in mind sound financial management, or do you just try to invest in everything going and see what works?

Mr. Marc Beaulieu: We rely on our partnerships with experts in the field, whether it be Transport Canada, the RCMP, or other railways. We seek whatever expertise required.

All of our risk assessments are done using proven models to make sure that the mitigation we're aiming for is properly considered in our assessments. We get full cooperation from everybody and anybody who is involved in our safety and security network.

● (1025)

Mr. Ryan Leef: Thank you.

The Chair: Thank you very much, Mr. Leef.

We'll now move back to Mr. Garrison.

Mr. Randall Garrison: Thank you very much, Mr. Chair.

Let me assure everybody that I'm going to have a very specific question for VIA Rail, but given some of the interventions from the other side, I just want to step back for a minute.

The terms of reference for today are fairly narrow, but we on this side think it's important to set the rail transport question of national security in the larger context. It was implied, for instance, that the audit of the Auditor General didn't really apply to what we're talking about today, and I just want to point to two of the objectives of that audit.

The Auditor General said that their audit was to "determine whether the management framework for the Public Security and Anti-Terrorism initiative was adequate to ensure that funding decisions reduced risks to Canadians by the maximum extent possible". For that reason, we've asked a number of more general questions, because that audit I think is relevant to determining where our resources are going, and whether rail is one of the places it needs to go.

Second was to "determine whether intelligence services work efficiently together and provide enforcement personnel with adequate information". Again, I'm going to have a very specific question about that with regard to VIA Rail.

We've asked the question on the overall impact of cuts being made in various departments, and whether anybody is examining the coordination of this to make sure that those individual cuts don't have an unintended impact on national security. We've asked about the allocation of resources to try to make sure that they're clearly based on threat and risk assessment. We've asked some questions about the coordination of those activities.

Finally, I think one of our perspectives has been that there seems to be, in the strategy, the treatment of VIA Rail as just another railway, when clearly VIA Rail, both as a crown corporation and as a passenger carrier, probably needs some special treatment in these areas.

With that in mind, I'm going to ask about—again from the Auditor General's report—a question that was raised. My question is to VIA Rail. When you sell tickets to people, do you check ID? What kind of ID would be checked?

Mr. Marc Beaulieu: We only check ID when necessary, in other words, if we have a doubt as to the transaction that is going on. We do not as a rule ask all of our customers for ID.

Mr. Randall Garrison: Has that policy been evaluated in a threat and risk assessment? I'm not arguing that it's necessary. I'm just asking the question of whether that policy was viewed through that lens of risk and threat assessment.

Mr. Marc Beaulieu: Well, as part of our ongoing review of our security plans, we're always exploring further risk mitigation in consultation with our partners, and law enforcement, and Transport Canada. We're constantly assessing further controls. That is one of the controls being assessed.

Mr. Randall Garrison: It seems to me this might be a good example of where, by VIA Rail perhaps checking ID, it might be of assistance to law enforcement officials by flagging people who are otherwise on watch lists in other places. So here's one of my questions, then, very specifically: does VIA Rail have access to the information on lost and stolen passports?

If someone were to use a lost or stolen passport at VIA Rail, would you know that it's a lost or stolen passport? Because one of the concerns raised by the Auditor General was that this information isn't getting to front-line people.

Mr. Marc Beaulieu: No, I'm not aware of receiving any information on lost or stolen passports.

Mr. Randall Garrison: My follow-up question, then, would be to Mr. Tremblay.

In the Auditor General's report, he points to what he considers serious delays in processing information on lost and stolen passports, from the passport office to the RCMP. He was talking about delays of over a month in processing that information. Can you make any comment about that?

C/Supt Larry Tremblay: I'm sorry. I'm just not personally aware of the specificity of your question.

Mr. Randall Garrison: His concern was that obviously if we're dealing with terrorism factors, the timeliness is important, and that the information needs to pass quickly from Citizenship and Immigration Canada to the law enforcement authorities so that the information is out there.

One of the things he does say is that he suspects that a lack of resources for what is considered sometimes a routine operation is one of the reasons for that delay. I wonder if maybe Mr. Davies or anyone else has any comment on that.

● (1030)

Mr. John Davies: We certainly have to talk to Passport Canada about what information they push out now. Obviously, they would be looking at what's lawful to push out—if they had information—to make sure there's a lawful basis for that information to move.

I haven't heard the concern that there's an issue. Usually if a passport's stolen or lost, my understanding is that information goes to the security agencies and so on. But I think we'd have to talk to them to get more details on what constraints they may be under. I don't think the constraint would be a resource constraint. I think it would be an issue on whether it's lawful to push that information, to whom, and when.

The Chair: Thank you.

We'll now go back to Mr. Del Mastro.

Welcome to our committee, Mr. Del Mastro.

Mr. Dean Del Mastro (Peterborough, CPC): Thank you, Mr. Chairman.

I have a couple of questions for the witnesses.

First of all, I think certainly what we've witnessed—and I've just talked to my colleague as well—we seem to have very good collaboration with the United States. We seem to have very good collaboration between agencies, and indeed, with VIA Rail. I think that's very encouraging to everyone hearing the testimony here today.

Mr. Rafferty pointed out that there are, in fact, thousands of miles of track—in the railway industry, we do still talk miles—and it seems to me that most of it is not of great concern. Where we do have greater concerns seems to be in urbanized areas. Threats are exposed or highlighted when we see people gaining access to tracks in areas where they shouldn't be. We had an unfortunate incident just a couple of years ago in Montreal, for example, where some younger folks got down there with spray-paint cans or what have you. But it demonstrates that access to the tracks is still perhaps too easy.

What are we doing, specifically, to eliminate that kind of access to what is really a very dangerous area? If you can get down there with a spray-paint can, you can get down there with just about anything else. What are we doing to secure the tracks in urbanized areas, not only from a public safety perspective for the people who might access it, but also for the people on the trains?

Mr. Gerard McDonald: Mr. Chair, obviously, as the member points out, access to tracks is a very big concern for us, on both the safety side and the security side. What we expect each railway organization to do is to conduct an appropriate threat and risk assessment of all their infrastructure, identify those areas requiring the highest need of improvement, and develop the appropriate mitigation measures to address those.

We're working with the railways, on both the safety and the security side, to help them identify those areas where there are specific instances—such as in Montreal where access to the tracks was a concern—then we work with them to see what can be done. It's my understanding that changes have been made to that particular area to make it more secure.

Mr. Dean Del Mastro: When we look at VIA, for example, they tend to operate at speeds faster than freight trains. That's expected. It's part of their business plan. These specific areas become of greater concern. If people can access the tracks, they don't have a lot of warning. People often, frankly, mistake the speed of trains. They don't have a lot of warning, specifically with passenger trains and the speed they're travelling at.

Has there been consideration given—and, again, it speaks to all aspects of rail security—to greater mitigation efforts, such as fencing and so forth, that would really block access to railway yards in urban areas?

Mr. Gerard McDonald: It's not an area that we regulate specifically in a general sense. But if there is a specific area of concern, we can work with the railway to look at where further mitigation measures might be necessary, and if necessary, try to come to an agreement with the railways. That is what we do to address those.

Mr. Dean Del Mastro: At this point, it's optional whether the railways may choose or not—

● (1035)

Mr. Gerard McDonald: It's the railway's responsibility.

We work with them. If we find an area that is a continuing concern, we can bring more force to bear on finding a potential solution.

Mr. Dean Del Mastro: Okay.

To VIA Rail, as I said, we've seen some incidents where there have been concerns about access to the tracks. I know CN is a principal railway whose tracks you operate on in the corridor. There's also some interaction with CP.

Are you working with those railways specifically to enhance security to prevent access along those tracks?

Mr. Marc Beaulieu: We rely strongly on the infrastructure owners to provide that safety. We report very quickly and efficiently to them whenever we find there's a risk area that needs to be addressed.

We work very closely with Operation Lifesaver, which obviously creates awareness campaigns on the dangers of being on or near infrastructure. We work very closely with Transport Canada. In fact, we've had a very successful private-crossing closure program that was funded by Transport Canada to improve rail security on the short distance of infrastructure that we own. All incidents and reasons for suspicion are quickly reported to the infrastructure owner for their information and furtherance.

Mr. Dean Del Mastro: Thank you.

The Chair: We'll move to Mr. Scarpaleggia, please, for five minutes.

Mr. Francis Scarpaleggia: Mr. McDonald, I'm looking at a newspaper article from a couple of weeks ago. It says:

> In its latest plans and priorities report, Transport Canada noted that security "systems and processes in place may not be sufficiently robust to respond" to a major incident.

Perhaps you could comment on that. Is it a misquote?

Mr. Gerard McDonald: No, I don't believe it's a misquote. It's from our report on plans and priorities. Part of that is that you outline what some of the risks in the system are and how you might mitigate them. One of the risks identified in that report is that our plans aren't robust enough. Obviously, to mitigate it we're going to ensure that we enhance those plans to ensure their robustness.

Mr. Francis Scarpaleggia: Okay.

Mr. Beaulieu, just to come back to the marshals, you have plainclothes marshals on VIA Rail trains in Canada. You did say that, correct?

Mr. Marc Beaulieu: I did.

Mr. Francis Scarpaleggia: Okay. I don't know if you can answer this, but on what percentage of trains would you have them? Is it 5%, 10%, 20%?

Mr. Marc Beaulieu: To reveal more information about some of our measures would defeat the purpose of the measures that are in place, so I'm going to choose not to answer that.

Mr. Francis Scarpaleggia: Understood.

That's why, actually, Liberals more and more are calling for the establishment of a public safety and national security committee that would meet in camera. As you know, Senator Dallaire has been discussing this, and I brought it up a couple times at this committee. That's precisely why—so we can get some of these answers.

On the issue of passenger lists, when it comes to air travel, Mr. McDonald, correct me if I'm wrong, but every time someone gets on a plane in Canada, their name is checked against an RCMP list or some kind of list to see if they're a person of interest. Or is it just people travelling in and out of Canada, especially to the United States?

Mr. Gerard McDonald: Their names are checked against what is called a specified persons list.

Mr. Francis Scarpaleggia: Is that done for people getting on VIA trains? If not, would it be very expensive and complicated to do it for VIA passenger lists as well?

Mr. Gerard McDonald: It is not done for VIA trains. One would have to assess what the value of that would be before determining whether it would be a worthwhile exercise and whether it would mitigate any security risks.

Mr. Francis Scarpaleggia: Well, I would think that if it mitigates security risks in one area, it would mitigate them in another. We're talking in both cases about mass transit. Obviously, in some ways, I suppose, there's more concern about air travel, but we're talking about probably the same passenger loads, and so on and so forth. Given that there's no screening of baggage that gets on a VIA Rail train, probably there's a good reason to screen the lists.

I would suggest that this is something that VIA Rail and the government might want to look at, Mr. Chair.

I'd like to turn to the big issue, I guess, Mr. Beaulieu and Mr. Tessier, as representatives of the government. Is anyone in a position to compare and contrast our rail security here, especially in the busy Montreal-Quebec City-Windsor corridor, with how Amtrak tackles security in the busy New York-Boston-Washington corridor? Apparently all their baggage has to go through sniffer dogs and so on.

I'm not suggesting that this is what we should look at, but are you regularly comparing and contrasting, and maybe sharing best practices? Or are they out of the picture, in some way, from your concerns?

● (1040)

The Chair: I think that was, perhaps, to Mr. Beaulieu.

Mr. Marc Beaulieu: We constantly review safety and security measures by other railways, whether it be Amtrak or Europe or Australia, to see what their best practices are. Based on our risk assessments, we determine what actions we should take.

If I may, I'm going to go back to your passenger list question, just for a clarification. Every person who gets on our trains has their ticket scanned so we know exactly how many people and what people are aboard our trains. This is consistent with the safety and security plans we submit to Transport Canada. We know who is on our trains based on ticket scanning, and we've implemented that technology.

The Chair: Your time is just up, very quickly, please.

Mr. Francis Scarpaleggia: Are you comparing that with a police list? For example, he may not be a terrorist. It could be somebody who's known to have a firearm and has threatened someone in the past.

The Chair: Thank you, Mr. Scarpaleggia.

We'll now move to Mr. Rafferty.

Mr. John Rafferty: Thank you very much, Mr. Chair.

If we have a little bit of time, Mr. Beaulieu might be interested in answering that question.

I have a question for you, Mr. Davies, but you may find that it's better answered by Mr. Coulombe or Mr. Tremblay. In your opening remarks, you talked about terrorist-related incidents. That got me thinking that we have a number of incidents of civil unrest or civil disobedience. I'm just wondering, what is the definition of a terrorist, in relation to public safety, that you use in Transport, in the government, and in the agencies? What distinguishes a terrorist from someone who is blocking a railway line, for example?

Mr. John Davies: I'm referring to the CT, counterterrorism, strategy. We tend to not define terrorism directly. We talk about the terrorist activities that you see described in the Criminal Code. That's an act or omission undertaken inside or outside Canada for a political, religious, or ideological purpose, which is intended to intimidate the public.

Mr. John Rafferty: So that would include first nations blocking a rail line, for example?

Mr. John Davies: Ahh...

Mr. John Rafferty: Under that definition....

Mr. John Davies: I think there's an element of subjectivity in how you look at this.

Mr. John Rafferty: I have a second question for you.

It's about the INSETs, which I didn't know about until your opening remarks. They sound like a good idea but I didn't see the railroads represented. Are railways represented on INSETs?

C/Supt Larry Tremblay: We have a member of the CN police on secondment to national security here at headquarters for that specific purpose.

Mr. John Rafferty: I'm curious as to what the response has been to INSETs. The RCMP, and maybe Mr. Coulombe, might want to answer also. You're also part of that group. Perhaps if we have time, Mr. Tessier might want to respond as well.

How are they working?

● (1045)

C/Supt Larry Tremblay: They're in Montreal, Toronto, Ottawa, Vancouver, and now Edmonton. They are an extremely efficient and effective way to pull multi-agencies together. They are very focused and ensure timely information sharing. They also ensure that there's notification. Overall, they make investigation of terrorist-related activity far more efficient and timely.

Mr. John Rafferty: Mr. Coulombe, would you care to comment on that, or agree with Chief Tremblay?

Mr. Michel Coulombe: I can only echo Mr. Tremblay. When I was in Montreal, in charge of Quebec, we had a member of CSIS seconded to INSET at C Division. This facilitated the exchange of information. The CSIS member had access to her own database. INSETs facilitate liaison and are a good approach to counterterrorism.

Mr. John Rafferty: Mr. Tessier, do you care to make a comment, or Mr. Beaulieu?

Mr. Marc Beaulieu: We're not members of INSET, but we certainly receive information from them. I echo the comments of the RCMP and CSIS that it's a very effective way of receiving the information.

Mr. John Rafferty: Thank you.

The Chair: Thank you very much, everyone, for appearing and helping the public safety and national security committee understand a little more about rail safety and security.

Mr. Del Mastro asked the question about young people and paint cans. I guess different people view different things in different ways. Many aspiring young artists see a canvas every time they see a grain car, so they're down there. Terrorists may very well see potential for a terrorist act.

Different people have different roles. Your role is to protect Canada, to protect the security of Canadians. We thank you very much for the very important work you're doing, seemingly in an organized fashion, where issues of the past—turf wars and things like that—don't seem to be as present today as maybe 20 years ago. So thank you very much.

We are adjourned.

Published under the authority of the Speaker of the House of Commons

SPEAKER'S PERMISSION

Also available on the Parliament of Canada Web Site at the following address: http://www.parl.gc.ca

Publié en conformité de l'autorité du Président de la Chambre des communes

PERMISSION DU PRÉSIDENT

Aussi disponible sur le site Web du Parlement du Canada à l'adresse suivante : http://www.parl.gc.ca

Determining IP addresses and tracking individuals by their IP address

What is an IP address?

The Internet Protocol (IP) is the system that routes information (broken up into data packets) on the Internet from one computer to another. Every computer or Internet-enabled device is given a unique numerical address (such as 123.145.167.189). In order to exchange information between two computers over the Internet, they must know each other's IP address.

Who determines how IP addresses are assigned?

Internet Service Providers (ISPs) are given blocks of IP addresses by regional internet governance bodies, and they usually assign IP addresses dynamically from within one block to subscribers. These dynamically assigned addresses are only valid for a specific lease time. Lease times vary greatly from one ISP to another because the optimal duration depends on several factors such as the number of IP addresses and subscribers an ISP possesses, and how much traffic a network can handle. So even if police are able to obtain someone's IP address, as described below, it is unlikely to be that person's IP address over a long period of time.

How easily can police find someone's IP address?

In all but a few cases, police would not be able to obtain someone's IP address without the assistance of that person's ISP. When a user passively browses websites (e.g. reading an online newspaper article), that IP address is only known by the user's ISP and the website he or she is visiting. Even if the user leaves a comment at the bottom of the article, for example, the user's IP address is rarely visible to users other than the site's administrators, though a user name (real or fictional) may be visible to others.

If instead of browsing the Internet, the user is interacting with people – such as by sending emails or instant messaging – then the user's IP address is generally available to the other person's computer (since the recipient needs to know where to send a response back). Some webmail services make finding the IP address fairly simple by including it in the email header, while others do not.

Determining someone's IP address can be made more difficult if that person uses a proxy server (essentially, people send their requests for webpages to a middleman, which uses its IP address to ask for the webpage, and then returns it to the requestor) or if that person attempts to spoof their IP address (replace their IP address with a fake one, though this is used less frequently because people who spoof addresses do not receive any reply back since their real IP address has been replaced).

In short, unless police are provided with someone's IP (e.g. a crime victim forwards a harassing email to police) or are able to engage someone online directly, they must request assistance from an ISP to determine who a particular IP address belongs to. Police may only ask an ISP to identify who was using a particular IP address at a given point in time if they suspect the information is needed to administer, enforce or investigate the enforcement of a law, or relates to national security.

How much can police learn about someone from their IP address?

Numerous tools are available to the public to help determine the approximate geographical location of an IP address. Sites such as Whatismyip.com allow users to enter IP addresses and get approximate locations down to the city or in some cases neighbourhood level, though accuracy can vary significantly. These sites do not actually know where the subscriber lives. Instead, the location represents an area served by a specific block of IP addresses owned by a particular ISP. For example, a given ISP could assign addresses from within the block 123.145.167.0 to 123.145.171.0 (approximately 1,000 addresses) to a particular neighbourhood in a given city. A person checking to see where address 123.145.167.1 was, for example, would see the same city or neighbourhood as the rest of the numbers in the block.

Police could not learn what websites a particular IP address had visited over time without judicial authorization.

Police could request that the person's ISP voluntarily provide such identifiers as the person's name, address, and email addresses tied to the account. Again, police would be permitted to make such a request only if they suspect the information is needed to administer, enforce or investigate the enforcement of a law, or relates to national security. Police could also request similar identifying information from a number of popular webmail and social media providers, such as Gmail, Facebook, and Twitter. In cases where the person has accounts with these providers, and the companies voluntarily provide this information, police could obtain the account names. However, police would have no access to the content of these accounts, unless they were open to the general public (such as an open Twitter account), in which case police and everybody else could receive content information.

In short, police would only be able to obtain identifying information without a warrant, and would still need to suspect the information is needed to administer, enforce or investigate the enforcement of a law, or relates to national security, to make the request. Obtaining the actual private communications of a person would require judicial authorization.

Department of Justice
Canada

Ministère de la Justice
Canada

Security classification -- Côte de sécurité

Protected B

File number -- Numéro de dossier

Date

April 15, 2013

Telephone / FAX -- Téléphone / Télécopieur

(613) 991-4364

MEMORANDUM / NOTE DE SERVICE

TO / DEST: Maciek Hawrylak
National Security Operations Directorate

s.23

FROM / ORIG: Claude Pilon,
Counsel, Public Safety Legal Services

[redacted]

Pages 397 to / à 401

are withheld pursuant to section

sont retenues en vertu de l'article

23

of the Access to Information

de la Loi sur l'accès à l'information

Emmett, Jamie

From:	Plunkett, Shawn
Sent:	April-05-13 1:49 PM
To:	Chayer, Marie-Helene
Cc:	Emmett, Jamie
Subject:	FW: Lawful Interception

Just confirmed with Caroline that they are looking for the rationale piece we had previously discussed (I was slightly confused by the term 'text').

She did raise the issue of how to transmit this info to Vancouver, as her director will need to see this information.

From: Caroline.Kennedy@ic.gc.ca [mailto:Caroline.Kennedy@ic.gc.ca]
Sent: April-05-13 1:36 PM
To: Plunkett, Shawn
Cc: Emmett, Jamie; Philip.Fleming@ic.gc.ca; Stephen.Nolan@ic.gc.ca s.19(1)
Subject: Lawful Interception

Good afternoon Shawn,

[redacted] I've had wind from my director that PS was to provide us with some text on Lawful Intercept later this afternoon. If you are to send it to us electronically, could you please make sure that both Philip Fleming and Stephen Nolan are both in CC. Should you not be able to send it via email, please contact Steve Nolan (613-993-2602) to make arrangements.

Thanks and have a great week-end.

Caroline
Industry Canada Industrie Canada
Canada

s.19(1)

Chayer, Marie-Helene

From: [redacted]
Sent: March-15-13 9:09 AM
To: Chayer, Marie-Helene
Subject: RE: [redacted] - M.A. research on lawful access

Good morning Marie-Hélène,
Thank you for the email and your consideration of the request. I understand fully the constraints and difficulties related to the file, so I'm grateful for the consideration of the request.
My best regards

[redacted]

From: Chayer, Marie-Helene [mailto:Marie-Helene.Chayer@ps-sp.gc.ca]
Sent: Friday, March 15, 2013 8:59 AM
To: [redacted]
Subject: RE: [redacted] - M.A. research on lawful access

Good morning Professor [redacted]

I wish I could help your student, but unfortunately, I'm afraid it will not be possible for me to meet with [redacted] at this point. As you may know, in February 2012, the Government introduced Bill C-30, the *Protecting Children from Internet Predators Act*, which pertains to lawful access. The Bill included provisions related to authorities' access to basic subscriber information and related privacy safeguards, and to telecommunications service providers' obligations regarding the lawful interception of communications. The Government, however, recently announced that these elements of Bill C-30 would not be going forward. As such, there is very little I can say on the subject.

Again, my apologies for being more helpful.

Have a nice day,

Marie-Hélène

Marie-Hélène Chayer
Director – Investigative Technology and Telecommunications Policy /
Directrice – Politique sur les technologies d'enquête et les télécommunications
National Security Operations Division / Division des Opérations de sécurité nationale
Public Safety Canada / Sécurité Publique Canada

(613)949-3181

s.19(1)

From: Banerjee, Ritu
Sent: March-14-13 5:03 PM
To: [redacted]
Cc: Chayer, Marie-Helene
Subject: RE: [redacted] - M.A. research on lawful access

Hi [redacted]

I have copied my colleague Marie-Helene Chayer, who handles the lawful access file. She would be pleased to follow-up with you on your request.

Ritu

From: [redacted]
Sent: Thursday, March 07, 2013 3:21 PM
To: Banerjee, Ritu
Subject: [redacted] - M.A. research on lawful access

Dear Ritu,

I write with a request which you may be able to assist me with.

I have [redacted] student undertaking research on lawful access and its national security implications. I write to see if I can open the door for [redacted] to the national security community.

[redacted] underlying assumption is that (a) there will be lawful access legislation at some point in time and (b) the subscriber information will be part of that package. [redacted] is specifically interested in the possibility of safeguards and/or accountability mechanisms that might be added to any legislation in order to assuage privacy concerns but still allow the national security community to access information.

To date [redacted] has conducted a solid literature review on the issue and conducted close to 20 interviews with individuals knowledgeable about lawful access from the following communities: academic, legal, private sector (communications companies), privacy associations/ groups and law enforcement. The interviews have been non-attributable – unless specifically requested by the interviewee for acknowledgement - , cleared by ethics protocols here at the University, and taken place with both pro and anti lawful access proponents. [redacted] I do not know who [redacted] has interviewed or who [redacted] plans to interview before the end of April.

[redacted] is establishing the national security case for subscriber information; most of it available in the public domain is second-hand or inferred and lacks concrete national security examples for why the changes in the last lawful access bill were being requested. [redacted] is hoping that non-attributable interviews with members of the national security community might go some way to filling that gap, without, of course, posing any risk to any on-going court cases, investigations, or sources, targets, and methods information.

The interviews would take place before the end of April, 2013 if possible.

If you think it is possible for [redacted] to conduct interviews on this issue – and I note that the legislation is now shelved so there may be less sensitivity about the subject at this juncture – I would like to provide you with [redacted] contact details or, if you prefer, for me to provide your details to [redacted] so contact can be established.

Once contact is established I remain outside of the process; any discussion you have with [redacted] to assess if interviews are possible, or interviews and contacts you might be able to facilitate, would be strictly between you and the student. (You would only need to be in contact with me if you were concerned about professional misconduct or breach of ethics by the student).

[redacted] and knowing the individual quite well, I can vouch for her approach and professional attitude and I would not be willing to reach out to the national security community on [redacted] behalf if I did not have confidence in [redacted] conduct and [redacted] abilities.

I'm happy to discuss any aspect of this with you at your convenience if you have questions. I'm also, of course, cognizant of the fact that this is a sensitive area and it may not be possible to talk to the community.

Grateful for your consideration of the request in advance, and don't hesitate to contact me if you have any questions or concerns,

Best regards,

[redacted]

s.19(1)

Emmett, Jamie

From:	Plunkett, Shawn
Sent:	March-01-13 11:58 AM
To:	Emmett, Jamie
Cc:	Hawrylak, Maciek; Thompson, Julie
Subject:	FW: Public enquiry re: Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications
Attachments:	FW: Media Call: SolGen Standards
Categories:	Blue Category

Jamie, thanks for your help on this one.

Maciek/Julie FYI.

From: Plunkett, Shawn
Sent: March-01-13 11:57 AM
To: Communications_
Cc: Picard, Josée; Chayer, Marie-Helene
Subject: RE: Public enquiry re: Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications

Hi Zarah,
Apologies for the delay. Following discussions with senior management we request that this document not/not be provided to the requester and propose the following response.

Proposed Response:

We respectfully decline your request for the document entitled *Solicitor General Enforcement Standards for Lawful Interception of Telecommunications*, and we would note that this document is provided to radio and spectrum licence holders only to assist them in complying with their lawful interception condition of licence. This document contains sensitive content and is not publicly available.

This proposed response is line with previous comms requests for the SolGen Standards (Please see attached).

Should you have any further questions, please do not hesitate to contact myself or my director Marie-Helene Chayer at (613)-949-3181.

Thank you.

Shawn Plunkett
Senior Policy Advisor / Conseiller principal en politiques
Investigative Technologies and Telecommunications Policy (ITTP) /
Technologies d'enquêtes et politiques des télécommunications (TEPT)
National Security Operations Directorate / Direction des opérations de sécurité nationale
Public Safety Canada / Sécurité Publique Canada
Tel: (613) 990-7066
Email: shawn.plunkett@ps.gc.ca

From: Communications_
Sent: February-28-13 11:57 AM
To: Plunkett, Shawn

Cc: Picard, Josée; Hawrylak, Maciek; Communications_
Subject: RE: Public enquiry re: Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications

Good morning,
Just following up on this. Thank you.

Zarah Malik
613-949-5536

From: Hawrylak, Maciek
Sent: Tuesday, February 26, 2013 2:56 PM
To: Communications_; Day, Liliane
Cc: Picard, Josée; Plunkett, Shawn
Subject: Re: Public enquiry re: Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications

Hello Zarah,

Liliane may have already responded, but my colleague Shawn Plunkett handles the SolGen standards.

Best,
Maciek

From: Communications_
Sent: Tuesday, February 26, 2013 01:27 PM
To: Day, Liliane
Cc: Communications_; Hawrylak, Maciek; Picard, Josée
Subject: FW: Public enquiry re: Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications

Hello Ms. Day,
As Maciek is away, would you be able to help with the enquiry below?
We would be grateful for any direction you could provide.
Thank you for your time.

Zarah Malik
613-949-5536

From: Communications_
Sent: Tuesday, February 26, 2013 1:26 PM
To: Hawrylak, Maciek
Cc: Communications_; Picard, Josée
Subject: Public enquiry re: Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications

Hello Maciek,

I was referred to you by my colleague at NS, Chris Willey.
I'm hoping that you might be able to help respond to the public enquiry below.
Would you know where we might be able to retrieve a copy of the Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications?
We would appreciate any direction you could provide, thank you.

s.19(1)

Name	[redacted]
Enquiry Date	2/14/2013
Language	English
Phone #	
Location	Ontario
E-mail	[redacted]@gmail.com
Type of Enquiry	Related to Public Safety
Method of Enquiry	E-mail
Organization	
PS Branch	
Program	
Portfolio Agency/Review Bodies	
Questions	Hello, I would like to obtain a copy of the Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications, along with any proposed changes. It says at http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf10473.html " For further information on proposed changes to the Solicitor General's Enforcement Standards, please contact Public Safety Canada via the General Enquiries line at 1-800-830-3118." I decided to try to contact you by electronic means first but will telephone if necessary.

Zarah Malik

Agente des communications | Communications Officer
Gestion des enjeux, Affaires publiques | Issues Management Team, Public Affairs Division
Ministère de la sécurité publique | Department of Public Safety
T : 613-949-5536 | F : 613-954-4779

Emmett, Jamie

From:	Plunkett, Shawn
Sent:	January-03-13 12:14 PM
To:	Duval, Jean Paul
Cc:	MacDonald, Michael; Chayer, Marie-Helene; Champoux, Martin
Subject:	FW: Media Call: SolGen Standards

JP, please find below the proposed response to the applicant, regarding the media request from the G&M. These lines have been DG approved.

Please advise should comms seek any additional changes.

Proposed Response:

We respectfully decline your request for an interview and would note that the document entitled *Solicitor General Enforcement Standards for Lawful Interception of Telecommunications*, is provided to radio and spectrum licence holders to assist them in complying with their lawful interception condition of licence. This document contains sensitive content and is not publicly available.

Should you have any questions, please let me know.

Thanks.

Shawn Plunkett
Senior Policy Advisor / Conseiller principal en politiques
Investigative Technologies and Telecommunications Policy (ITTP) /
Technologies d'enquêtes et politiques des télécommunications (TEPT)
National Security Operations Directorate / Direction des opérations de sécurité nationale
Public Safety Canada / Sécurité Publique Canada
Tel: (613) 990-7066
Email: shawn.plunkett@ps.gc.ca

From: Duval, Jean Paul
Sent: January-03-13 10:35 AM
To: Plunkett, Shawn
Subject: Media Call: SolGen Standards

Good morning Shawn,

Based on our conversation yesterday, here is the proposed response for your review. Please advise if you have any concerns as I would like to discuss potential issues before proceeding with DG level approvals.

Proposed response:

- We respectfully decline your request for an interview and would note that the document in question is intended as a compliance reference for industry officials, and not for public distribution.

Many thanks,
JP

s.19(1)

Title	[redacted]
Media Outlet	Globe and Mail

s.19(1)

Call Date	12/31/2012 3:00 PM
Telephone	[redacted]
E-mail address	[redacted]@globeandmail.com
Deadline	
Status	Consulting
Branch	NS
Subject	Lawful Interception Enforcement Standards (re: Lawful Access)
Questions	I am reviewing a document put together by Public Safety Canada's National Security Technology Division regarding 22 specific interception standards that telecom carriers were asked to provide police circa 2008. I am seeking a discussion with someone in the division to discuss these specific 22 measures. Would that be possible? Document info: - "Solicitor General's Enforcement Standards for the Lawful Interception of Telecommunications -- Compliance Table." - said to be "current as of Nov. 17 2008" - 22 standards make explicit what the government is seeking from telecom networks and carriers - Annotated with italics further explaining the standards - Among measures made explicit are needs for intercepting various modalities (call forwarding / real-time audio / data-voice correlation accuracy measures / encryption algorithms, etc etc etc) - Prepared by Public Safety's National Security Technology Division

Jean Paul Duval
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-1689
Cell | Portable: [redacted]
Email | Courriel : jeanpaul.duval@ps-sp.gc.ca

Carignan, Joëlle

From: Miller, Kevin
Sent: Wednesday, September 18, 2013 4:10 PM
To: deleRue, Jean-Christophe
Cc: Tomlinson, Jamie
Subject: RE: Hill Times - Lawful Access

Merci, on va le contacter...

KM

From: deleRue, Jean-Christophe
Sent: Wednesday, September 18, 2013 4:09 PM
To: Miller, Kevin
Cc: Tomlinson, Jamie
Subject: FW: Hill Times - Lawful Access

s.19(1)

Kevin,

Pour suivi du ministère. Merci.

From: [redacted] [mailto:[redacted]@hilltimes.com]
Sent: September-18-13 11:58 AM
To: deleRue, Jean-Christophe
Subject: Hill Times - Lawful Access

Hi Jean-Christophe,

I'm following the issue of lawful access and telecommunications surveillance this week and I am looking for some response to the following questions.

My questions are:
1. Will the government reintroduce lawful access legislation when Parliament returns?
2. What checks are in place to protect citizens' privacy from unwarranted surveillance?
3. Some critics say that the government has approved expanded telecomms surveillance without legislation, through spectrum licensing for example. How does your office respond to this claim?

I'm putting these questions to your office as it was the previous Public Safety Minister who previously introduced lawful access legislation. My deadline is tomorrow at 5, please let me know who the response are attributable to.

Thanks for your help,

[redacted]

[redacted]

The Hill Times
Office: [redacted]
Cell: [redacted]

s.19(1)

Carignan, Joëlle

From:	Boisvert, Frederik
Sent:	Friday, September 13, 2013 5:39 PM
To:	Picard, Josée; deleRue, Jean-Christophe; Tamming, Jason; Johnson, Mark
Cc:	Carta, John; Tomlinson, Jamie; Miller, Kevin; Filipps, Lisa
Subject:	Re: For Approval: Media Request: Lawful Interception Enforcement Standards

Approved.

From: Picard, Josée
Sent: Friday, September 13, 2013 05:36 PM
To: Boisvert, Frederik; deleRue, Jean-Christophe; Tamming, Jason; Johnson, Mark
Cc: Carta, John; Tomlinson, Jamie; Miller, Kevin; Filipps, Lisa
Subject: For Approval: Media Request: Lawful Interception Enforcement Standards

s.19(1)

Jean-Christophe, Frederik,

We received a second follow-up request from [redacted] (Globe and Mail) today on a Lawful Interception Enforcement Standards request [redacted] made back in December 2012 (please see call summaries below). [redacted] is looking to know if we have anything more to say at this time.

Do you have any concerns with the following response?:

- "Further to your follow-up request today, we have nothing further to add at this time."

Many thanks,
Josée

Previous Calls (2):

Title	[redacted]
Media Outlet	Globe and Mail
Call Date	6/10/2013 4:00 PM
Telephone	[redacted]
E-mail address	[redacted]@globeandmail.com
Deadline	
Status	Final
Branch	NS
Subject	Lawful Interception Enforcement Standards
Questions	The reporter is following up on a request he had sent us this winter, see summary below. He wants to see if there is anything more that can be said on this at this time.

****

PREVIOUS REQUEST

Title: [redacted]
Media Outlet: Globe and Mail
Call Date: 12/31/2012 3:00 PM
Telephone: [redacted]
E-mail address: [redacted]@globeandmail.com

Status: Response sent to the reporter
Branch: NS
Subject: Lawful Interception Enforcement Standards (re:Lawful Access)
Questions:
I am reviewing a document put together by Public Safety Canada's National Security Technology Division regarding 22 specific interception standards that telecom carriers were asked to provide police circa 2008.

I am seeking a discussion with someone in the division to discuss these specific 22 measures. Would that be possible?

Document info:
- "Solicitor General's Enforcement Standards for the Lawful Interception of Telecommunications -- Compliance Table."
- said to be "current as of Nov. 17 2008"
- 22 standards make explicit what the government is seeking from telecom networks and carriers
- Annotated with italics further explaining the standards
- Among measures made explicit are needs for intercepting various modalities (call forwarding / real-time audio / data-voice correlation accuracy measures / encryption algorithms, etc etc etc)
- Prepared by Public Safety's National Security Technology Division

Final Response:
We respectfully decline your request for an interview and would note that the document entitled Solicitor General Enforcement Standards for Lawful Interception of Telecommunications, is provided to radio and spectrum licence holders to assist them in complying with their lawful interception condition of licence. This document contains sensitive content and is not publicly available.

Reporter and Outlet	[redacted] - Globe and Mail	s.19(1)
Actions Taken	No existing entries.	
Draft Response	Further to your follow-up request today, we have nothing further to add at this time.	

Title	[redacted]
Media Outlet	Globe and Mail
Call Date	12/31/2012 3:00 PM
Telephone	[redacted]
E-mail address	[redacted]@globeandmail.com
Deadline	
Status	Final
Branch	NS
Subject	Lawful Interception Enforcement Standards (re:Lawful Access)
Questions	I am reviewing a document put together by Public Safety Canada's National Security Technology Division regarding 22 specific interception standards that telecom carriers were asked to provide police circa 2008. I am seeking a discussion with someone in the division to discuss these specific 22 measures. Would that be possible? Document info: - "Solicitor General's Enforcement Standards for the Lawful Interception of Telecommunications -- Compliance Table." - said to be "current as of Nov. 17 2008" - 22 standards make explicit what the government is seeking from telecom networks and carriers - Annotated with italics further explaining the standards - Among measures made explicit are needs for intercepting various modalities (call forwarding / real-time audio / data-voice correlation accuracy measures / encryption algorithms, etc etc etc)

		- Prepared by Public Safety's National Security Technology Division
Reporter and Outlet	s.19(1)	[redacted] - Globe and Mail
Actions Taken		No existing entries.
Draft Response		
Approvals		Shawn Plunkett Michael MacDonald Andrew Swift Stéphanie Durand MO
Final Response		We respectfully decline your request for an interview and would note that the document entitled Solicitor General Enforcement Standards for Lawful Interception of Telecommunications, is provided to radio and spectrum licence holders to assist them in complying with their lawful interception condition of licence. This document contains sensitive content and is not publicly available.

Carignan, Joëlle

From:	Tomlinson, Jamie
Sent:	Friday, September 13, 2013 5:33 PM
To:	Picard, Josée
Cc:	Filipps, Lisa; Miller, Kevin; Carta, John
Subject:	Re: For DG Approval: Media Request: Lawful Interception Enforcement Standards

No concerns

Thanks

s.19(1)

From: Picard, Josée
Sent: Friday, September 13, 2013 05:32 PM
To: Tomlinson, Jamie
Cc: Filipps, Lisa; Miller, Kevin; Carta, John
Subject: For DG Approval: Media Request: Lawful Interception Enforcement Standards

Jamie,

We received another follow-up request from [redacted] (Globe and Mail) today on a Lawful Interception Enforcement Standards request [redacted] made back in December 2012. [redacted] is looking to know if we have anything more to say at this time.

Do you have any concerns with the following response?:

- "Further to your follow-up request today, we have nothing further to add at this time."

Approved by:
Marie-Helene Chayer
Mike MacDonald

Many thanks,
Josée

Josée Picard
Media Relations / Relations avec les médias
Ministère de la sécurité publique | Department of Public Safety
T : 613-949-4288 | F : 613-954-4779
josee.picard@ps-sp.gc.ca

Previous Calls (2):

Title	[redacted]
Media Outlet	Globe and Mail
Call Date	6/10/2013 4:00 PM
Telephone	[redacted]
E-mail address	[redacted]@globeandmail.com

Deadline

Status
Final

Branch
NS

Subject
Lawful Interception Enforcement Standards

Questions
The reporter is following up on a request [redacted] had sent us this winter, see summary below. [redacted] wants to see if there is anything more that can be said on this at this time.

****

PREVIOUS REQUEST

s.19(1)

Title: [redacted]
Media Outlet: Globe and Mail
Call Date: 12/31/2012 3:00 PM
Telephone: [redacted]
E-mail address: [redacted]@globeandmail.com
Status: Response sent to the reporter
Branch: NS
Subject: Lawful Interception Enforcement Standards (re:Lawful Access)
Questions:
I am reviewing a document put together by Public Safety Canada's National Security Technology Division regarding 22 specific interception standards that telecom carriers were asked to provide police circa 2008.

I am seeking a discussion with someone in the division to discuss these specific 22 measures. Would that be possible?

Document info:
- "Solicitor General's Enforcement Standards for the Lawful Interception of Telecommunications -- Compliance Table."
- said to be "current as of Nov. 17 2008"
- 22 standards make explicit what the government is seeking from telecom networks and carriers
- Annotated with italics further explaining the standards
- Among measures made explicit are needs for intercepting various modalities (call forwarding / real-time audio / data-voice correlation accuracy measures / encryption algorithms, etc etc etc)
- Prepared by Public Safety's National Security Technology Division

Final Response:
We respectfully decline your request for an interview and would note that the document entitled Solicitor General Enforcement Standards for Lawful Interception of Telecommunications, is provided to radio and spectrum licence holders to assist them in complying with their lawful interception condition of licence. This document contains sensitive content and is not publicly available.

Reporter and Outlet
[redacted] - Globe and Mail

Actions Taken
No existing entries.

Draft Response
Further to your follow-up request today, we have nothing further to add at this time.

Title	[redacted]
Media Outlet	Globe and Mail
Call Date	12/31/2012 3:00 PM
Telephone	[redacted]
E-mail address	[redacted]@globeandmail.com
Deadline	
Status	Final
Branch	NS

Subject	Lawful Interception Enforcement Standards (re:Lawful Access)
Questions	I am reviewing a document put together by Public Safety Canada's National Security Technology Division regarding 22 specific interception standards that telecom carriers were asked to provide police circa 2008. I am seeking a discussion with someone in the division to discuss these specific 22 measures. Would that be possible?
s.19(1)	Document info: - "Solicitor General's Enforcement Standards for the Lawful Interception of Telecommunications -- Compliance Table." - said to be "current as of Nov. 17 2008" - 22 standards make explicit what the government is seeking from telecom networks and carriers - Annotated with italics further explaining the standards - Among measures made explicit are needs for intercepting various modalities (call forwarding / real-time audio / data-voice correlation accuracy measures / encryption algorithms, etc etc etc) - Prepared by Public Safety's National Security Technology Division
Reporter and Outlet	[redacted] Globe and Mail
Actions Taken	No existing entries.
Draft Response	
Approvals	Shawn Plunkett Michael MacDonald Andrew Swift Stéphanie Durand MO
Final Response	We respectfully decline your request for an interview and would note that the document entitled Solicitor General Enforcement Standards for Lawful Interception of Telecommunications, is provided to radio and spectrum licence holders to assist them in complying with their lawful interception condition of licence. This document contains sensitive content and is not publicly available.

Willey, Chris

From:	Carta, John
Sent:	Friday, September 13, 2013 5:05 PM
To:	Picard, Josée; Willey, Chris
Cc:	Miller, Kevin
Subject:	RE: Media Request: Lawful Interception Enforcement Standards

Your response looks right to me, but I'd confirm with Shawn Plunkett & Marie-Helene Chayer. Let me know if you need a hand.

Thanks Josée

John

From: Picard, Josée
Sent: September-13-13 5:01 PM
To: Carta, John; Willey, Chris
Cc: Miller, Kevin
Subject: Media Request: Lawful Interception Enforcement Standards

John and Chris,

We received another follow-up request from [redacted] today on a Lawful Interception Enforcement Standards request [redacted] made back in December 2012. [redacted] is looking to know if we have anything more to say at this time.

Unless you know something I don`t, do you have any concerns with the following response?:

- "Further to your follow-up request today, we have nothing further to add at this time."

Many thanks,
Josée

s.19(1)

Previous Calls:

Title	[redacted]
Media Outlet	Globe and Mail
Call Date	6/10/2013 4:00 PM
Telephone	[redacted]
E-mail address	[redacted]@globeandmail.com
Deadline	
Status	Final
Branch	NS
Subject	Lawful Interception Enforcement Standards
Questions	The reporter is following up on a request he had sent us this winter, see summary below. He wants to see if there is anything more that can be said on this at this time. **************************

PREVIOUS REQUEST

s.19(1)

Title: [redacted]
Media Outlet: Globe and Mail
Call Date: 12/31/2012 3:00 PM
Telephone: [redacted]
E-mail address: [redacted]@globeandmail.com
Status: Response sent to the reporter
Branch: NS
Subject: Lawful Interception Enforcement Standards (re:Lawful Access)
Questions:
I am reviewing a document put together by Public Safety Canada's National Security Technology Division regarding 22 specific interception standards that telecom carriers were asked to provide police circa 2008.

I am seeking a discussion with someone in the division to discuss these specific 22 measures. Would that be possible?

Document info:
- "Solicitor General's Enforcement Standards for the Lawful Interception of Telecommunications -- Compliance Table."
- said to be "current as of Nov. 17 2008"
- 22 standards make explicit what the government is seeking from telecom networks and carriers
- Annotated with italics further explaining the standards
- Among measures made explicit are needs for intercepting various modalities (call forwarding / real-time audio / data-voice correlation accuracy measures / encryption algorithms, etc etc etc)
- Prepared by Public Safety's National Security Technology Division

Final Response:
We respectfully decline your request for an interview and would note that the document entitled Solicitor General Enforcement Standards for Lawful Interception of Telecommunications, is provided to radio and spectrum licence holders to assist them in complying with their lawful interception condition of licence. This document contains sensitive content and is not publicly available.

Reporter and Outlet	[redacted] Globe and Mail
Actions Taken	No existing entries.
Draft Response	Further to your follow-up request today, we have nothing further to add at this time.

Title	[redacted]
Media Outlet	Globe and Mail
Call Date	12/31/2012 3:00 PM
Telephone	[redacted]
E-mail address	[redacted]@globeandmail.com
Deadline	
Status	Final
Branch	NS
Subject	Lawful Interception Enforcement Standards (re:Lawful Access)
Questions	I am reviewing a document put together by Public Safety Canada's National Security Technology Division regarding 22 specific interception standards that telecom carriers were asked to provide police circa 2008. I am seeking a discussion with someone in the division to discuss these specific 22 measures. Would that be possible? Document info: - "Solicitor General's Enforcement Standards for the Lawful Interception of Telecommunications -- Compliance Table."

		- said to be "current as of Nov. 17 2008" - 22 standards make explicit what the government is seeking from telecom networks and carriers - Annotated with italics further explaining the standards - Among measures made explicit are needs for intercepting various modalities (call forwarding / real-time audio / data-voice correlation accuracy measures / encryption algorithms, etc etc etc) - Prepared by Public Safety's National Security Technology Division
Reporter and Outlet	s.19(1)	[redacted] Globe and Mail
Actions Taken		No existing entries.
Draft Response		
Approvals		Shawn Plunkett Michael MacDonald Andrew Swift Stéphanie Durand MO
Final Response		We respectfully decline your request for an interview and would note that the document entitled Solicitor General Enforcement Standards for Lawful Interception of Telecommunications, is provided to radio and spectrum licence holders to assist them in complying with their lawful interception condition of licence. This document contains sensitive content and is not publicly available.

Wilson, Barbara

From:	Carta, John
Sent:	Wednesday, April 24, 2013 5:28 PM
To:	Duval, Jean Paul; Nadon, Marc
Cc:	Wilson, Barbara; Slack, Jessica; LeSage, Lynn; Paulson, Erika; Austria, Jamela
Subject:	RE: Info derived from torture
Attachments:	130211 - Tse SCC Compliance ML E - FINAL.DOCX

No worries. Jamela just tracked down the products from DOJ.

Attached are DoJ's lines regarding the Government's February introduction of amendments in response to the ruling of the Supreme Court of Canada in the case of R. v. Tse. It contains language on Bill C-30. I believe the only line we would use is:

- The Government has listened to the concerns raised by Canadians in regards to Bill C-30, which will not be proceeding further.

But DOJ should likely be referred calls on C30 at this point.

I'll get back to Jean.

From: Duval, Jean Paul
Sent: April-24-13 5:25 PM
To: Nadon, Marc; Carta, John
Cc: Wilson, Barbara; Slack, Jessica; LeSage, Lynn; Paulson, Erika
Subject: RE: Info derived from torture

Marc, John,

FYI - Mr. Cintra has just dropped by my desk asking for the C-30 lines as well on behalf of ADM MacKinnon. I told him to contact either of you for the these lines.

Sorry to pass the buck on providing these lines, but I prefer to defer to your expertise on this as I'm not sure if the lines I provided are ready for use in Geneva as is.

Cheers,
JP

From: Nadon, Marc
Sent: Wednesday, April 24, 2013 5:15 PM
To: Carta, John; Paulson, Erika; Duval, Jean Paul
Cc: Wilson, Barbara; Slack, Jessica; LeSage, Lynn
Subject: Re: Info derived from torture

Ok - thanks

From: Carta, John
Sent: Wednesday, April 24, 2013 05:01 PM
To: Nadon, Marc; Paulson, Erika; Duval, Jean Paul; Paulson, Erika

Cc: Wilson, Barbara; Slack, Jessica; LeSage, Lynn
Subject: RE: Info derived from torture

There's only one line on C30... just trying to track it down.

From: Nadon, Marc
Sent: April-24-13 4:58 PM
To: Paulson, Erika; Duval, Jean Paul
Cc: Wilson, Barbara; Slack, Jessica; LeSage, Lynn; Carta, John
Subject: Re: Info derived from torture

Ok thanks - anything on Bill C-30?

From: Paulson, Erika
Sent: Wednesday, April 24, 2013 04:56 PM
To: Duval, Jean Paul; Nadon, Marc
Cc: Wilson, Barbara; Slack, Jessica; LeSage, Lynn; Carta, John
Subject: RE: Info derived from torture

Thanks, JP. Marc, pls see below

From: Duval, Jean Paul
Sent: Wednesday, April 24, 2013 4:53 PM
To: Paulson, Erika
Cc: Wilson, Barbara; Slack, Jessica
Subject: Info derived from torture

Erika,

Below is the last I have on this. Jessica will be in tomorrow and may have more background to offer.

Provided to CBSA on Feb 13 -11:33 by Jessica.
-The Government of Canada opposes in the strongest possible terms the mistreatment of any individual by any foreign state or agency for any purpose.

Cheers,
JP

Media Lines:
Government response to Supreme Court of Canada decision in *R v. Tse*

ISSUE:

On February 11, 2013 the Government will introduce amendments in response to the ruling of the Supreme Court of Canada in the case of *R. v. Tse*. In that case, the Court found that section 184.4 of the Criminal Code, which was enacted in 1993 and allows for the use of wiretapping without a judicial authorization when there is imminent harm, was unconstitutional. The Court gave Parliament until April 13, 2013, to amend the provision to make it constitutionally compliant. These amendments comply with the Supreme Court of Canada ruling.

KEY MESSAGES:

Compliance with the Supreme Court of Canada

- The Supreme Court of Canada recently found that section 184.4 of the *Criminal Code* (interception in exceptional circumstances), which was enacted in 1993, was unconstitutional but gave Parliament until April 13, 2013 to amend the provision to make it constitutionally compliant.

- The proposed reforms will add important privacy safeguards to the *Criminal Code's* provision for wiretaps in situations of imminent harm (section 184.4). This provision deals with situations of imminent harm, such as kidnappings or bomb threats.

- The Government will continue to work hard to safeguard Canadians, while ensuring that their privacy is also protected.

If pressed re: Bill C-30

- The Government has listened to the concerns raised by Canadians in regards to Bill C-30, which will not be proceeding further.

- The Government of Canada has no plans to move forward with the measures contained in Bill C-30 related to the warrantless mandatory disclosure of basic subscriber information or the requirement for telecommunications service providers to build intercept capability within their systems.

- The Government will continue to review the other components of Bill C-30 which aimed at modernizing the *Criminal Code* and its related statutes.

Prepared by:

Andrew Gowing
Communications Advisor
(613) 948-5913

Wilson, Barbara

From: Carta, John
Sent: Wednesday, April 24, 2013 5:25 PM
To: Wilson, Barbara
Subject: RE: Info derived from torture
Attachments: 130211 - Tse SCC Compliance ML E - FINAL.DOCX

Here are the Justice lines, from which we would take our C30 line. Basically:

- The Government has listened to the concerns raised by Canadians in regards to Bill C-30, which will not be proceeding further.

From: Wilson, Barbara
Sent: April-24-13 5:23 PM
To: Carta, John
Subject: Re: Info derived from torture

If you get that one line, can you share? Not sure if it's in our stuff or not

From: Carta, John
Sent: Wednesday, April 24, 2013 05:01 PM
To: Nadon, Marc; Paulson, Erika; Duval, Jean Paul; Paulson, Erika
Cc: Wilson, Barbara; Slack, Jessica; LeSage, Lynn
Subject: RE: Info derived from torture

There's only one line on C30... just trying to track it down.

From: Nadon, Marc
Sent: April-24-13 4:58 PM
To: Paulson, Erika; Duval, Jean Paul
Cc: Wilson, Barbara; Slack, Jessica; LeSage, Lynn; Carta, John
Subject: Re: Info derived from torture

Ok thanks - anything on Bill C-30?

From: Paulson, Erika
Sent: Wednesday, April 24, 2013 04:56 PM
To: Duval, Jean Paul; Nadon, Marc
Cc: Wilson, Barbara; Slack, Jessica; LeSage, Lynn; Carta, John
Subject: RE: Info derived from torture

Thanks, JP. Marc, pls see below

From: Duval, Jean Paul
Sent: Wednesday, April 24, 2013 4:53 PM
To: Paulson, Erika
Cc: Wilson, Barbara; Slack, Jessica
Subject: Info derived from torture

Erika,

Below is the last I have on this. Jessica will be in tomorrow and may have more background to offer.

Provided to CBSA on Feb 13 -11:33 by Jessica.
-The Government of Canada opposes in the strongest possible terms the mistreatment of any individual by any foreign state or agency for any purpose.

Cheers,
JP

Media Lines:
Government response to Supreme Court of Canada decision in *R v. Tse*

ISSUE:

On February 11, 2013 the Government will introduce amendments in response to the ruling of the Supreme Court of Canada in the case of *R. v. Tse*. In that case, the Court found that section 184.4 of the Criminal Code, which was enacted in 1993 and allows for the use of wiretapping without a judicial authorization when there is imminent harm, was unconstitutional. The Court gave Parliament until April 13, 2013, to amend the provision to make it constitutionally compliant. These amendments comply with the Supreme Court of Canada ruling.

KEY MESSAGES:

Compliance with the Supreme Court of Canada

- The Supreme Court of Canada recently found that section 184.4 of the *Criminal Code* (interception in exceptional circumstances), which was enacted in 1993, was unconstitutional but gave Parliament until April 13, 2013 to amend the provision to make it constitutionally compliant.

- The proposed reforms will add important privacy safeguards to the *Criminal Code's* provision for wiretaps in situations of imminent harm (section 184.4). This provision deals with situations of imminent harm, such as kidnappings or bomb threats.

- The Government will continue to work hard to safeguard Canadians, while ensuring that their privacy is also protected.

If pressed re: Bill C-30

- The Government has listened to the concerns raised by Canadians in regards to Bill C-30, which will not be proceeding further.

- The Government of Canada has no plans to move forward with the measures contained in Bill C-30 related to the warrantless mandatory disclosure of basic subscriber information or the requirement for telecommunications service providers to build intercept capability within their systems.

- The Government will continue to review the other components of Bill C-30 which aimed at modernizing the *Criminal Code* and its related statutes.

Prepared by:

Andrew Gowing
Communications Advisor
(613) 948-5913