FEDERAL BUREAU OF INVESTIGATION FOI/PA
DELETED PAGE INFORMATION SHEET
10th Interim Release
Civil Action# 18-cv-1833, FOIA 1404359-0

Total Withheld Page(s) = 26

Bates Page Reference	**Reason for Withholding** (i.e., exemptions with coded rationale, duplicate, sealed by order of court, etc.)
18-cv-1833-4522-4523	Referral/Consult
18-cv-1833-4525	Referral/Consult
18-cv-1833-4527-4545	Referral/Consult
18-cv-1833-4548-4551	Referral/Consult

XXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXX

Daniel Charles Richman

From: Daniel Charles Richman
Sent: Tuesday, December 06, 2016 3:51 PM
To: [redacted](DO) (OGA); Oconnell, Sasha C. (DO) (FBI)
Subject: NITs for child exploitation
Attachments: [redacted] Paper Version 2.docx

b6 -1,2
b7C -1,2

Dear Sasha and [redacted] Attached is a draft paper by [redacted] on vulnerability exploitation in child exploitation cases. It brackets the encryption issue but may still be very useful. [redacted] said I could share it.
d

---------- Forwarded message ----------
From: [redacted]
Date: Mon, Dec 5, 2016 at 10:27 PM
Subject: Re: 12/9 cypto discussion at CLS
To: Daniel Charles Richman [redacted]

b6 -2,4
b7C -2,4

Thanks Dan, this is really helpful. I've taken a machete to the introduction, which was far too meandering, and eliminated the parts trying to convince people they should care about this. The facts speak for themselves on that. The result is much shorter and hopefully clearer. I incorporated your minor notes quickly, and will sit down with the bigger ones tomorrow. New version is attached, feel free to share it at your discretion.

Unfortunately, I can't make the Friday meeting. I'll spare you the details but [redacted] and I need to be here to cover. I'm sorry to miss it. I'd love to hear how it went and catch up sometime soon. Any plans to be in DC? I should be in New York sometime in February.

[redacted]

Spam
Not spam
Forget previous vote

--

Daniel Charles Richman

From:	Daniel Charles Richman
Sent:	Saturday, December 10, 2016 3:53 PM
To:	Oconnell, Sasha C. (DO) (FBI); [redacted] (DO) (OGA)
Subject:	Fwd: Thanks and a request
Attachments:	FBI-Columbia-Dec2016.pdf

b6 -1,2
b7C -1,2

missed [redacted] slides
d

---------- Forwarded message ----------
From: [redacted]
Date: Sat, Dec 10, 2016 at 2:32 PM
Subject: Thanks and a request
To: Daniel Charles Richman [redacted]

b6 -2,4
b7C -2,4

Dear Dan,

Thanks again for hosting the event yesterday and for inviting me.

I think that in the end it was absolutely ok that I didnt present the slides, essentially all the points were said. Still, can I ask you to forward it to the FBI people that were present in the meeting? I dont have their contact information.

I slightly shortened and made it more concise. I also added a more "high level" recommendation, that the meeting yesterday helped me crystallize: that the design of the system should consider the case where the secret/priviledged keys and other info that allows LE to obtain what is legitimately needs leaks out to bad guys. The system should be such that the damage caused in such a case does not outweigh the benefits that the system provides to begin with.

Many thanks,

[redacted]

--
BEGIN-ANTISPAM-VOTING-LINKS

Teach Email if this mail (ID 01SikqPJQ) is spam:
Spam: https://antispam.law.columbia.edu/canit/b.php?i=01SikqPJQ&m=53da38999a22&t=20161210&c=s
Not spam: https://antispam.law.columbia.edu/canit/b.php?i=01SikqPJQ&m=53da38999a22&t=20161210&c=n
Forget vote: https://antispam.law.columbia.edu/canit/b.php?i=01SikqPJQ&m=

53da38999a22&t=20161210&c=f

END-ANTISPAM-VOTING-LINKS

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office [redacted] b6 -4
cellphone [redacted] b7C -4
You can download my papers at http://ssrn.com/author=937729

Daniel Charles Richman

From: Daniel Charles Richman
Sent: Thursday, December 15, 2016 6:07 PM
To: [redacted] (DO) (OGA); Oconnell, Sasha C. (DO) (FBI)
Subject: Fwd: continuing thread

b6 -1,2,4
b7C -1,2,4

I want to keep you posted on my long exchange with [redacted] on GD
Interesting :)

Daniel Richman
Paul J. Kellner Professor of Law
Columbia Law School
Office: [redacted]
Cell: [redacted]

Begin forwarded message:

> **From:** [redacted]
> **Date:** December 15, 2016 at 5:17:04 PM EST
> **To:** Daniel Charles Richman [redacted]
> **Cc:** [redacted]
> **Subject: Re: continuing thread**

b6 -2,4
b7C -2,4

> Hi Dan, see inline:
>
> On 12/13/2016 3:34 PM, Daniel Charles Richman wrote:
>
>> More questions/comments, if you don't mind
>>
>> 1. On the argument that a master key in govt hands creates the risk of system failure, and that mandating a set of master keys in govt hands is marginally but not a lot better: I wonder whether we might be more granular on what failure looks like. Does it necessarily mean that every device can be hacked and turned into a zombie that would kill us all? Or that the contents of everyone's devices become accessible to an evil genius? Must the conversation stop at failure, or are there variants of system failure that can be baked in -- variants that, to various degrees, we could tolerate as a society, in exchange for ?
>
> Yes, this is indeed the goal. But need to be very cautious about it. You read the newspaper just like I do and you see how porous all our security measures are. How anything can be hacked. You dont need to be an expert to see that computer security is not anything that you would want to trust. How we got to where we are is a great question, but perhaps a bit out of scope for this immediate discussion.
>
> So one starting point of the discussion should be that no computer security system can be really trusted long-term, not even if the FBI or the CIA or the NSA or all together design it. So

any system whose security relies solely on the long term secrecy of some smallish set of keys is a bad idea.

And one should bake into the system measures that will bound the damage in case security is compromised. Once this is acknowledged then one can start discussing specifics.

> 2. I understand that we don't want to leave things to chance in the "non-master-key(s) but instead multiple schemes" scenario. Employers/device manufacters/ etc, each setting up access in some coordinated way. But is anyone looking it that as a matter of theory? If not, I'll bet a government mandate would jump start that work. This wouldn't be the first time that a regulatory mandate sparked innovation that no saw in their self-interest beforehand.

There are many papers that solve this in principle. (I have written some myself.) The problem is the interfaces and the implementations and the "what ifs".

> 3. On the technical slowdown approach: I've assumed (perhaps wrongly) that those suggesting this approach were just arguing for more govt computer power and not suggesting that there be any mandated route that would accommodate a set amount of govt power. Are you suggesting that we could really have a "master key that works intentionally slowly"?

yes, absolutely. The system can have a baked in mechanism that slows down the response in case that the "special LE access" is requested.

> Also, as your lawyer, let me counsel you not to make the "need to wait for a warrant" analogy. Fourth Amendment doctrine has developed a robust "exigent circumstances" exception to the warrant rule. Law enforcement doesn't have to wait when there is good reason not to - as there regularly is.

thx :)

But let me push back on this a bit: as far as I understand, one of the premises of these "exigent circumstances" exceptions is that the dangers of denying justified warrant far exceeds the dangers of granting an unjustified warrant.
I claim that our case is different: The dangers of immediate access far outweigh the dangers of delayed access. It's a harder argument to make, since the danger of immediate access is the danger of an event that happens with some very small probability. but the weight of the bad event is so large that even this small probability should not be tolerable. This is especially so since, over time, the probability of the bad event happening just increases, until it becomes a certainty that the event will happen *some time* in the next, say, 50 years.
Compare eg to nuclear power plant failure or to, say a Snowden event.
So maybe not such a bad comparison after all...

Best, [redacted]

b6 -2
b7C -2

dan r

On Mon, Dec 12, 2016 at 8:59 PM, [redacted] wrote: b6 -2 b7C -2

> Dan,
>
> Having multiple schemes/ algorithm/vendors might help, but it might also create more havoc and confusion for system designers and and the system's users. And certainly one cannot afford to leave things to chance, hoping that multiple schemes will somehow increase security.
>
> Indeed, it is not only the FBI that cannot be trusted to keep keys secret for a long time, nobody is...
>
> In other words - the only way to make sure that the master key that allows breaking into people's devices will not end up in the wrong hands is to *not have that master key in the first place*.
>
> Your suggestion reads to me akin to "let's restrict the number of devices that each master key can open". Now, whether that is better than a single master key depends on how these semi-master keys are kept. If they are held by the FBI then we're back to the same problem, since as soon as FBI is compromised everyone is. If these keys are held by different entities then the bad guys would have to compromise these entities, perhaps one by one, perhaps all at once, depending on what vulnerabilities the bad guys find.
>
> Either way, this is significantly worse than having no master key, or alternatively making sure that the master key words intentionally slowly.
>
> Regarding the infeasibility of time delay: I completely understand that the FBI dont like it. But perhaps they can understand that they will better serve the citizens of the US by taking a delay hit - in the same way that they better serve the citizens of the US by waiting for a warrant before searching, even though waiting for a warrant sometimes allows criminals to escape.
>
> For instance, if what they want is those pictures to convince the jury, then this is not time sensitive. If they want some specific information that's time sensitive then perhaps they can specify what it is and different delays can apply to different types of information.
>
> Best, [redacted] b6 -2 b7C -2
>
> One might set a limit on how many devices can a single key open. And then force the
>
> Allowing for multiple mechanisms and implementations is certainly a very good thing. But one must not leave things for chance and make sure that no matter what happens, there is no situation that allows for a massive break of security

for all - even if FBI's internal security is compromised.

one way to do that is to have the device vendors be responsible for the security of the devices, and hand over the keys to LE upon request.

On 12/11/2016 2:33 PM, Daniel Charles Richman wrote:

[redacted] - I really appreciate your willingness to engage on this in practical terms.

b6 -2
b7C -2

So the way I read your last two messages, the problem lies in a "single mechanism" regime of universal access. (The "golden key" that is so scorned:)). That's the single basket waiting for trouble. But what is the problem with a "single" principle of access -- where the mechanisms of that access are to be selected by a myriad of decisionmakers (like the many enterprises making those decisions today about the devices used by their employees etc.)? Why should we expect that the mechanisms will all be same, particularly in a world -- like the one that a government mandate would create -- in which innovation and diversity would be financially rewarded?

When it comes to the slow/resource intensive proposal, here's where my own "systems expertise" kicks it: Between the kidnapped child and loose terrorist scenarios, the time delay is not acceptable. And even putting time aside, the decentralized nature of the US police system, and the political complexities of deciding which small number of cases are "worth it," vastly reduces the promise of this proposal.

best
d

On Sun, Dec 11, 2016 at 11:27 AM, [redacted] wrote:

b6 -2
b7C -2

Sorry, let me fix that:

> That is, such systems would force everyone, by law, to put all their eggs in a single communal basket. But the RBI tells us not to worry since its a really really good basket which will never break.

What I meant it: The FBI comes the to the academic community in a request to design such a really really good basket that will never break.

So the answer that I heard in the room is that we cannot design such a basket, and furthermore we believe that anyone that claims they can design such a basket is selling snake oil...

The one reasonable suggestion that I heard (mentioned by [redacted] [redacted] in the meeting) is to make sure that even legitimate LE access will be slow, and require much resources on a per device basis. At least this way when the basket breaks, the eggs will not break all at once.

b6 -2
b7C -2

Note that this does not restrict the court-order solution where the owner of the device is ordered by court to disclose the contents of the device. It only limits the "FBI does it by itself given court order" path.

(Of course, then there are the 4th-am issues, but these live in a different layer of the solution space, ie when to grant access, and what types of access to grant.)

Best, [redacted]

On 12/11/2016 1:01 AM, [redacted] wrote:

b6 -2
b7C -2

> Please feel free to share this discussion with the FBI (except for the strong language in prior notes, that was for academic consumption only...)
>
> Re your question: The difference is scale.
>
> Right now each company has its own structure and mechanisms. So the bad guys would need to use different methodologies/techniques/manpower to obtain the secret information of each individual company. (True, some "zero days" might be useful for multiple companies/individuals, but still.)
>
> Furthermore, each company/individual decides which pieces of data to protect more and which to protect less. They decide among how many baskets they split their eggs.
>
> systems like the ones you describe (such as Tait etc) require all companies to use a single mechanism that will allow lawful access by LE. this means that a failure of this single mechanism will compromise everyone.
>
> That is, such systems would force everyone, by law, to put all their eggs in a single communal basket. But the RBI tells us not to worry since its a really really

good basket which will never break.

So there is a big difference between having a court order the owner of a device to expose its contents to LE, and giving LE the technical ability to do it themselves, once court order is issued. The first one does not have the vulnerabilities I discussed, the second one does. Hope this makes sense.

[redacted]

b6 -2
b7C -2

On 12/10/2016 10:38 PM, Daniel Charles Richman wrote:

> Not sure I follow. Right now we live in a world in which innumerable enterprises - firms etc - have not given the govt keys at all. There is no LE key at all; no envelopes. But all those enterprises are or can in be in a position to comply with a Search warrant for devices in their domain, right?. I guess you can still worry about a failure across every enterprise. But we already have that and for enterprise reasons it won't change. Why would the risk be qualitatively different if every device had such an available warrant addressee?
>
> Also please note that my musings are in my academic capacity (tho i keep the bureau posted).
>
> Daniel Richman
> Paul J. Kellner Professor of Law
> Columbia Law School
> Office:[redacted]
> Cell:[redacted]
>
> b6 -4
> b7C -4
>
> On Dec 10, 2016, at 9:51 PM, [redacted] wrote:
>
> b6 -2
> b7C -2
>
>> ok, now we're talking business :)
>>
>> the point is that this idea of distributing/sharing the keys among several entities is not that helpful here.

this sharing business (via onion encryption or shamir secret sharing or whatever) is mainly helpful when the entities dont trust each other, or different people trust different entities - in other words when what you try to defend against is these entities themselves going rogue.

when you're trying to protect against external attackers that try to hack their way in by finding vulnerabilities such as zero-days, human enginering , physical side channel attacks etc etc, such distribution provides only limited additional protection. Indeed, most entities use similar systems, have similar vulnerabilities, etc. so breaking into 5 is not that much harder than breaking into 1. after all, it;s all software agents so doing 5 times the work in parallel has the same cost as doing it once.

and note that here you painted a target around yourself, and you give the attackers infinite time to work. so the question is now not whether your system will be compromised, but rather how long it will take the attackers to break the system.

And recall that there is not recourse - once the system is broken, all secrets of all citizens are exposed.

And I didnt even take into consideration the possibilities that keys or algorithms will need to be updated, or the case where some computer doesnt work right now and you really need that key now so you send it over by fax...

remember, one false move and game over....

bottom line: even with distribution, onions, etc, one has to consider the case that one day the bad guys will be in possession of all of LE keys. And the FBI needs to acknowledge that in order to move forward.

Best,

[redacted]

b6 -2
b7C -2

On 12/10/2016 5:07 PM, Daniel Charles Richman wrote:

> Fair point about keeping a "master" secret actually secret. And fair point that the Bureau people didn't answer it. But of course, there needn't be a master and needed even be a set of multiple keys. All that is needed is that there be, at least for devices, a place that the govt can go for compliance. That can be an

enterprise (employer etc), a manufacturer or any number of possibilities.
d

On Sat, Dec 10, 2016 at 4:40 PM, [redacted]
> wrote:

b6 -2
b7C -2

> Dan,
>
> I agree that there was a lot lost in translation here. But I wouldnt put the blame only, or even mainly, the academic side. I think the other side was as equally wrapped in their own nest.
>
> For instance, I didnt hear them even once acknowledge the fact that there is danger in putting so many eggs in one basket. I only heard them say "we feel confident about our ability to keep our secret information secret"

and "of course we wouldnt want the security of regular phones compromised. after all our own agents are using the same phones". They lost me - and probably the rest of the techy side of the room- right there. Obviously, someone who says these words either doent know what they are talking about, or is trying to con you.

On the other hand, the academic side was very good about putting aside the "4th am" issues, as you rightly suggested. indeed, this is a whole other wasp nest that would need to be sorted out later on.

Going forward, perhaps the first step, before trying to propose and shoot down specific solutions, is to try to agree on a set of criteria and desiderata. This is perhaps the most important (and perhaps the hardest) step, and also the step where the "non-techies" can contribute and weigh-in the most.

And I dont agree with [redacted] that we need "very precise problem specification" to get going. Part of our job is to be able to turn English desiderata to technical specifications that make mathematical sense. But we need to agree on the English desiderata first.

b6 -2
b7C -2

I would like to start with the following requirement, that I kept repeating like a broken record in the meeting:

* Even if all the secrets of LE get exposed, or hacked, then the damage caused to the common citizens, the organizations, to the economy, and to national infrastructures is limited, and furthermore we have a contigency plan as to how we recover from such damage.

Best

[redacted]

b6 -2
b7C -2

On 12/10/2016 3:52 PM, Daniel Charles Richman wrote:

I'm really gl

			ad you came and I will forward these materials and your message right now. In my odd status as observer/participant,

			I have to say that yesterday left me wondering about the troubling intellectual/policy gap between the Bureau and th

			e academic community. I give you enormous credit for getting beyond the (to my mind) unproductive talking points

			about "the golden age of surveillance" and "vulnerabilities are the answer" and getting to the heart of the design issues.

			The problem comes when thinking about next steps. Even as the academic community (understandably) points to the pr

			oblems with the "clipper chip," it seems to be sitting back and waiting for some other "top-down" proposal from the govern

		ment that invariably will raise concerns about system failure and that will invariably (if not so limited as to be of little us

			e to the govt) have weaknesses. To it's credit, the govt has made no such proposal. In the face of public safety conc

erns that, again to your credit, you truly recognize, my overly optimistic hope has been that others, like [redacted] ,

b6 -2
b7C -2

			would at least take a stab at the problem, instead of waiting for some global government solution. That this has not be

			en happening strengthens the need, in my personal opinion, for legislative moves that will just start the innovational on

			g the lines that you suggest. Unless, of course, you and [redacted] present your design requirements to your students and have

b6 -2
b7C -2

			them (not the government) propose some ideas:) let's keep in touch best dan richman On Sat, Dec 10, 2016 at

2:32 PM, [redacted] > wrote:

> Dear Dan,
>
> Thanks again for hosting t

b6 -2
b7C -2

			he event yesterday and for inviting me. I think that in the end

				itwasabsolutelyokthatIdidntpresenttheslides,essenti

				allyallthepointsweresaid.Still,canIaskyoutoforwardit

				to the FBI people that were present in the meeting? I dont have

				their contact information. I slightly shortened and made i

				t more concise. I also added a more "high level" recommendatio

			n, that the meeting yesterday helped me crystallize: that t

			he design of the system should co ment that invariably will raise concerns about system fai

			lure and that will invariably (if not so limited as to be of little use to the govt) have weaknesses. To it's credit, the govt ha

			s made no such proposal. In the face of public safety concerns that, again to your credit, you truly recognize, my overl

			y optimistic hope has been that others, like [redacted], would at least take a stab at the problem, instead of waiting

b6 -2
b7C -2

			for some global government solution. That this has not been happening strengthens the need, in my personal opinion

, for legislative moves that will just start the innovation along the lines that you suggest. Unless, of course, you and [redacted]

b6 -2
b7C -2

b6 -2
b7C -2

[redacted]

present your design requirements to your students and have them (not the government) propose some ideas:)

let

's keep in touch
best
dan richman

On Sat, Dec 10, 2016 at 2:32 PM, [redacted] > wrote:

> Dear D

b6 -2
b7C -2

				an, Thanks again for hosting the event yesterday and for inv

				iting me. I think that in the end it was absolutely ok that I did

			nt present the slides, essentially all the points were said.

				Still, can I ask you to forward it to the FBI people that were pre

				sent in the meeting? I dont have their contact information.

				I slightly shortened and made it more concise. I also added am

			ore" high level" recommendation, that the meeting yesterday

				helped me crystallize: that the design of the system should

				consider the case where these secret/privileged keys and othe

			r info that allows LE to obtain what is legitimately needs lea

			ks out to bad guys. The system should be such that the damage c

			used in such a case does not outweigh the benefits that the sys

temprovidestobeginwith. Manythanks,

[redacted]

b6 -2
b7C -2

..BEGIN.

				ANTISPAM.VOTING.LINKS...............................

TeachEmaiIIfthismail(IDO1S

			kqpjQ)isspam.spam. https://antispam.law.columbia

			.edu/canit/b.php?i=01SikgPJQ&m=53da3899a22&t=201612

				10&c=sNot spam: https://antispam.law.columbia.edu/c

anit/b.php?i=015ikgpjQ&m=53da38999a22&t=20161210&c=

			nForsetvote: https://antispam.law.columbia.edu/canit/

b:php?i=015ikgPJQ&m=53da38999a22&t=20161210&c=f....

D-ANTISPAM.VOTING-LINKS

-- Daniel Richman Paul J. Kellner Professor of Law, Columbia Law School offi ce [redacted]

cellphone [redacted]

You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

Spam
Not spam
Forget previous vote

--
Daniel Richman
Paul J. Kellner Professor of Law, Columbia Law School

office [redacted]
[redacted]
cellphone [redacted]
[redacted]
You can download
my papers
at http://ssrn.com/
author=937729

b6 -4
b7C -4

Spam
Not spam
Forget previous vote

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office [redacted]
cellphone [redacted]
You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

Spam
Not spam
Forget previous vote

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office [redacted]
cellphone [redacted]
You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

Spam
Not spam
Forget previous vote

Daniel Charles Richman

From: Daniel Charles Richman
Sent: Friday, December 16, 2016 12:53 PM
To: [redacted](DO) (OGA)
Subject: are you available to chat later today?

b6 -1
b7C -1

Daniel Charles Richman

From: Daniel Charles Richman
Sent: Tuesday, December 20, 2016 4:53 PM
To: [redacted] (DO) (OGA)
Subject: Re: FW: Encryption Working Group Releases Year-End Report

b6 -1
b7C -1

thanks for this.
Did they outsource the job to the Berkman people, or just do the same thing on their own?
Metadata + loose data + vulnerability exploitation = good enough

On Tue, Dec 20, 2016 at 4:47 PM, [redacted] (DO) (OGA) [redacted] wrote:

> **From:** Herring, Jason V. (CD) (FBI)
> **Sent:** Tuesday, December 20, 2016 4:39 PM
> **To:** Beers, Elizabeth R. (DO) (FBI) [redacted] (DO) (FBI)
> [redacted] (DO) (FBI) [redacted] (DO) (FBI)
> [redacted] (DO) (FBI [redacted] (DO) (FBI)
> [redacted] (DO) (FBI) [redacted] (DO) (FBI)
> [redacted] (DO) (OGA [redacted] (DO)
> (FBI) [redacted] (DO) (FBI) [redacted] (CTD)
> (FBI [redacted] Baker, James A. (OGC) (FBI) [redacted] Anderson, Trisha B. (OGC)
> (FBI [redacted] Mcnally, Richard (OGC) (FBI) [redacted] (OGC)
> (FBI) [redacted]
> **Subject:** FW: Encryption Working Group Releases Year-End Report
>
> b6 -1
> b7C -1
> b7E -3
>
> The House Judiciary Committee released its year-end encryption working group report.
>
> Please share with anyone I may have missed who has an interest in encryption matters...
>
> Thanks. Jason
>
> **From:** Hiller, Aaron [mailto: [redacted]
> **Sent:** Tuesday, December 20, 2016 4:26 PM
> **To:** Herring, Jason V. (CD) (FBI) [redacted]
> **Subject:** Fwd: Encryption Working Group Releases Year-End Report
>
> b6 -5
> b7C -5
> b7E -3
>
> Flagging this for you, Mr. Herring. Hope you are well.

Begin forwarded message:

From: "Rexrode, Kathryn" [redacted] b6 -5
Date: December 20, 2016 at 4:20:19 PM EST b7C -5
To: "Rexrode, Kathryn" [redacted]
Subject: Encryption Working Group Releases Year-End Report

FOR IMMEDIATE RELEASE: December 20, 2016

CONTACT: Jessica Collins (Goodlatte), (202) 225-3951
[redacted] (Upton) [redacted] b6 -5
Shadawn Reddick-Smith (Conyers) [redacted] b7C -5
[redacted] Pallone) [redacted]

Encryption Working Group Releases Year-End Report

The report contains key observations and opportunities for progress

Washington, D.C. –Members of the bipartisan encryption working group – established in March 2016 by House Judiciary Committee Chairman Bob Goodlatte (R-VA), Ranking Member John Conyers, Jr. (D-MI), House Energy and Commerce Committee Chairman Fred Upton (R-MI), and Ranking Member Frank Pallone, Jr. (D-NJ) – today released a year-end report laying out key observations and next steps.

For nearly a year, the Encryption Working Group has held numerous meetings with a variety of federal, state, and local government entities, former government officials, private industry and trade associations, civil society organizations, consultants and legal experts, academia, and cryptographers. These meetings have produced critical information, culminating in a year-end report that lays out four key observations and identifies several areas for future discussion next Congress.

The report concludes:

"Encryption is inexorably tied to our national interests. It is a safeguard for our personal secrets and economic prosperity. It helps to prevent crime and protect national security. The widespread use of encryption technologies also complicates the missions of the law enforcement and intelligence communities. As described in this report, those complications cannot be ignored. This is the reality of modern society. We must strive to find common ground in our collective responsibility: to prevent crime, protect national security, and provide the best possible conditions for peace and prosperity.

"That is why this can no longer be an isolated or binary debate. There is no 'us versus them,' or 'pro-

encryption versus law enforcement." This conversation implicates everyone and everything that depends on connected technologies—including our law enforcement and intelligence communities. This is a complex challenge that will take time, patience, and cooperation to resolve. The potential consequences of inaction—or overreaction—are too important to allow historical or ideological perspectives to stand in the way of progress."

Below are key observations of the report.

1. Any measure that weakens encryption works against the national interest.

2. Encryption technology is a global technology that is widely and increasingly available around the world.

3. The variety of stakeholders, technologies, and other factors create different and divergent challenges with respect to encryption and the "going dark" phenomenon, and therefore there is no one-size-fits-all solution to the encryption challenge.

4. Congress should foster cooperation between the law enforcement community and technology companies.

Based on these observations, the report has identified several areas for future discussion by the committees next Congress, such as exploring opportunities to help law enforcement agencies navigate the process of accessing information from private companies; examining options to improve law enforcement's ability to leverage metadata; reviewing the circumstances, resources and legal framework necessary to help law enforcement agencies exploit existing flaws in digital products; considering the implications of alternative legal strategies such as compelling individual consumers to decrypt their devices, and the role of encryption in fostering greater data security and privacy.

The full report can be viewed here.

The members of the working group issuing the report are House Judiciary Committee Chairman Bob Goodlatte (R-VA), House Energy and Commerce Chairman Fred Upton (R-Mich.), Ranking Member John Conyers, Jr. (D-Mich.), Ranking Member Frank Pallone, Jr. (D-N.J.), and Representatives Jim Sensenbrenner (R-WI), Darrell Issa (R-CA), Zoe Lofgren (D-CA), Suzan DelBene (D-WA), Bill Johnson (R-OH), and Yvette D. Clarke (D-NY).

###

Spam
Not spam
Forget previous vote

--
Daniel Richman
Paul J. Kellner Professor of Law,

Columbia Law School
office [redacted]
cellphone [redacted]
You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

Daniel Charles Richman

From: Daniel Charles Richman
Sent: Friday, December 16, 2016 1:24 PM
To: [redacted] (DO) (OGA) b6 -1 b7C -1
Subject: Re: are you available to chat later today?

3 would be great. thx

On Fri, Dec 16, 2016 at 1:09 PM, [redacted] (DO) (OGA) [redacted] wrote: b6 -1 b7C -1 b7E -3

> How about around 3?
>
> **From:** Daniel Charles Richman [mailto: [redacted] b6 -1,4 b7C -1,4 b7E -3
> **Sent:** Friday, December 16, 2016 12:53 PM
> **To:** [redacted] (DO) (OGA) [redacted]
> **Subject:** are you available to chat later today?
>
> ---
>
> Spam
> Not spam
> Forget previous vote

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office [redacted] b6 -4
cellphone [redacted] b7C -4
You can download my papers at http://ssrn.com/author=937729

Daniel Charles Richman

From: Daniel Charles Richman
Sent: Wednesday, December 28, 2016 11:05 AM
To: [redacted](DO) (OGA)
Subject: Re: DC visit on Jan 3

b6 -1,4
b7C -1,4

No, I havent
Thx

Daniel Richman
Paul J. Kellner Professor of Law
Columbia Law School
Office:[redacted]
Cel[redacted]

On Dec 28, 2016, at 10:53 AM, [redacted](DO) (OGA) [redacted] wrote:

b6 -1
b7C -1
b7E -3

> Thanks Dan—heard back from Rybicki? (He's been out of the office the past few days, but I can follow up if necessary.)
>
> I should be around the 3rd and happy to meet.
>
> **From:** Daniel Charles Richman [mailto[redacted]
> **Sent:** Monday, December 26, 2016 7:02 PM
> **To**[redacted](DO) (OGA)[redacted] Rybicki, James E. (DO) (FBI)
> [redacted]
> **Subject:** DC visit on Jan 3
>
> Dear Jim &[redacted] Hope you guys had a lovely Christmas. I'm planning to be in DC Jan 2-4. Mostly for fun, but the D said I should come his office Jan 3. I figure I should coordinate this with one or both of you & maybe even get to see you when I'm there
> thx
> dan richman
>
> --
> Daniel Richman
> Paul J. Kellner Professor of Law,
> Columbia Law School
> office[redacted]
> cellphone[redacted]
> You can download my papers at http://ssrn.com/author=937729
>
> Spam
> Not spam
> Forget previous vote

b6 -1,4
b7C -1,4
b7E -3

[redacted] (DO) (FBI)

b6 -1
b7C -1

From: [redacted] (DO) (FBI)
Sent: Wednesday, December 28, 2016 1:59 PM
To: [redacted] (DO) (OGA)
Subject: RE: DC visit on Jan 3

Thank you! The boss sent me an email regarding Mr. Richman. I will find a time, respond to Dan, and cc you.

...

-------- Original message --------
From: [redacted] (DO) (OGA)" [redacted]
Date: 12/28/2016 1:46 PM (GMT-05:00)
To: [redacted] (DO) (FBI)" [redacted]
Subject: FW: DC visit on Jan 3

b6 -1
b7C -1
b7E -3

[redacted]

Hope you had a Merry Xmas!

Please see the note below from Dan Richman—Jim said to work with you to hold a time for Dan to meet the Boss on the 3rd.

[redacted]

From: Daniel Charles Richman [mailto: [redacted]]
Sent: Monday, December 26, 2016 7:02 PM
To: [redacted] (DO) (OGA) [redacted]; Rybicki, James E. (DO) (FBI)
[redacted]
Subject: DC visit on Jan 3

b6 -1,4
b7C -1,4
b7E -3

Dear Jim & [redacted] Hope you guys had a lovely Christmas. I'm planning to be in DC Jan 2-4. Mostly for fun, but the D said I should come his office Jan 3. I figure I should coordinate this with one or both of you & maybe even get to see you when I'm there
thx
dan richman

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office [redacted]
cellphone [redacted]
You can download my papers at: http://ssrn.com/author=937729

Daniel Charles Richman

From: Daniel Charles Richman
Sent: Thursday, December 29, 2016 11:08 AM
To: [redacted](DO) (OGA) b6 -1,4 b7C -1,4
Subject: Re: DC visit on Jan 3

Excellent. Unless my hang with d runs a bit over, but you'll know that
Please remind me of his office number ?
D

Daniel Richman
Paul J. Kellner Professor of Law
Columbia Law School
Office[redacted]
Cell:[redacted]

On Dec 29, 2016, at 9:49 AM,[redacted](DO) (OGA)[redacted]wrote: b6 -1,4 b7C -1,4 b7E -3

> Sure—I'll pencil you in for 11:30? (I actually had a Going Dark idea to run by you.)
>
> **From:** Daniel Charles Richman [mailto[redacted]
> **Sent:** Wednesday, December 28, 2016 2:31 PM
> **To**[redacted](DO) (OGA)[redacted]
> **Cc:** Rybicki, James E. (DO) (FBI)[redacted]
> **Subject:** Re: DC visit on Jan 3
>
> Thx. I just heard from her & will see the D at 11:00. Maybe I can catch you afterward?
>
> On Wed, Dec 28, 2016 at 2:29 PM,[redacted](DO) (OGA)
> [redacted]wrote: b6 -1 b7C -1 b7E -3
>
>> Dan,
>>
>> Hope you had a nice Christmas too[redacted]is looking into scheduling for the 3rd and will be in touch soon.
>>
>> Thanks,
>> [redacted]
>>
>> **From:** Daniel Charles Richman [mailto[redacted] b6 -1,4 b7C -1,4 b7E -3
>> **Sent:** Monday, December 26, 2016 7:02 PM
>> **To:**[redacted](DO) (OGA)[redacted]Rybicki, James E. (DO) (FBI)
>> [redacted]
>> **Subject:** DC visit on Jan 3
>>
>> Dear Jim &[redacted]- Hope you guys had a lovely Christmas. I'm planning to be in DC Jan 2-4. Mostly for fun, but the D said I should come his office Jan 3. I figure I should coordinate

> this with one or both of you & maybe even get to see you when I'm there
> thx
> dan richman
>
> --
> Daniel Richman
> Paul J. Kellner Professor of Law,
> Columbia Law School
> office [redacted]
> cellphone [redacted]
> You can download my papers at http://ssrn.com/author=937729
>
> Spam
> Not spam
> Forget previous vote

b6 -4
b7C -4

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office [redacted]
cellphone [redacted]
You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

Spam
Not spam
Forget previous vote

From: Daniel Charles Richman
Sent: Friday, December 30, 2016 11:27 AM
To: [redacted](DO) (OGA)
Subject: Re: DC visit on Jan 3

b6 -1,4
b7C -1,4

Perfect. See you tues
And have a wonder new year

Daniel Richman
Paul J. Kellner Professor of Law
Columbia Law School
Office:[redacted]
Cell:[redacted]

On Dec 30, 2016, at 11:19 AM[redacted](DO) (OGA)[redacted] wrote:

b6 -1
b7C -1
b7E -3

> The room number? 7162
>
> **From:** Daniel Charles Richman [mailto[redacted]
> **Sent:** Thursday, December 29, 2016 11:08 AM
> **To:** [redacted](DO) (OGA)[redacted]
> **Subject:** Re: DC visit on Jan 3
>
> b6 -1,4
> b7C -1,4
> b7E -3
>
> Excellent. Unless my hang with d runs a bit over, but you'll know that
> Please remind me of his office number ?
> D
>
> Daniel Richman
> Paul J. Kellner Professor of Law
> Columbia Law School
> Office:[redacted]
> Cell:[redacted]
>
> On Dec 29, 2016, at 9:49 AM,[redacted](DO) (OGA)[redacted]
> wrote:
>
> b6 -1
> b7C -1
> b7E -3
>
>> Sure—I'll pencil you in for 11:30? (I actually had a Going Dark idea to run by you.)
>>
>> **From:** Daniel Charles Richman [mailto[redacted]
>> **Sent:** Wednesday, December 28, 2016 2:31 PM
>> **To:** [redacted](DO) (OGA)[redacted]
>> **Cc:** Rybicki, James E. (DO) (FBI)[redacted]
>> **Subject:** Re: DC visit on Jan 3
>>
>> b6 -1,4
>> b7C -1,4
>> b7E -3
>>
>> Thx. I just heard from her & will see the D at 11:00. Maybe I can catch you afterward?

On Wed, Dec 28, 2016 at 2:29 PM, [redacted](DO) (OGA) [redacted] wrote:

b6 -1
b7C -1
b7E -3

> Dan,
>
> Hope you had a nice Christmas too. [redacted] is looking into scheduling for the 3rd and will be in touch soon.
>
> Thanks,
> [redacted]
>
> **From:** Daniel Charles Richman [mailto:[redacted]
> **Sent:** Monday, December 26, 2016 7:02 PM
> **To:** [redacted](DO) (OGA)[redacted]; Rybicki, James E. (DO) (FBI)[redacted]
> **Subject:** DC visit on Jan 3
>
> Dear Jim &[redacted] Hope you guys had a lovely Christmas. I'm planning to be in DC Jan 2-4. Mostly for fun, but the D said I should come his office Jan 3. I figure I should coordinate this with one or both of you & maybe even get to see you when I'm there
> thx
> dan richman
>
> --
> Daniel Richman
> Paul J. Kellner Professor of Law,
> Columbia Law School
> office[redacted]
> cellphone[redacted]
> You can download my papers at http://ssrn.com/author=937729
>
> Spam
> Not spam
> Forget previous vote

b6 -1,4
b7C -1,4
b7E -3

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office[redacted]
cellphone[redacted]
You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

Spam
Not spam
Forget previous vote

Daniel Charles Richman

From: Daniel Charles Richman
Sent: Friday, December 30, 2016 11:30 AM
To: [redacted] (DO) (OGA) b6 -1,4 b7C -1,4
Subject: Re: DC visit on Jan 3

Sure. Ok to call my cell in 10 mins?
Daniel Richman
Paul J. Kellner Professor of Law
Columbia Law School
Office: [redacted]
Cell: [redacted]

On Dec 30, 2016, at 11:28 AM, [redacted] (DO) (OGA) [redacted] wrote: b6 -1 b7C -1 b7E -3

> Got a sec to chat?
>
> **From:** Daniel Charles Richman [mailto: [redacted] b6 -1,4 b7C -1,4 b7E -3
> **Sent:** Friday, December 30, 2016 11:27 AM
> **To:** [redacted] (DO) (OGA) [redacted]
> **Subject:** Re: DC visit on Jan 3
>
> Perfect. See you tues
> And have a wonder new year
>
> Daniel Richman
> Paul J. Kellner Professor of Law
> Columbia Law School
> Office: [redacted]
> Cell: [redacted]
>
> On Dec 30, 2016, at 11:19 AM, [redacted] (DO) (OGA) [redacted] wrote: b6 -1 b7C -1 b7E -3
>
> > The room number? 7162
> >
> > **From:** Daniel Charles Richman [mailto: [redacted] b6 -1,4 b7C -1,4 b7E -3
> > **Sent:** Thursday, December 29, 2016 11:08 AM
> > **To:** [redacted] (DO) (OGA) [redacted]
> > **Subject:** Re: DC visit on Jan 3
> >
> > Excellent. Unless my hang with d runs a bit over, but you'll know that
> > Please remind me of his office number ?
> > D
> >
> > Daniel Richman
> > Paul J. Kellner Professor of Law

Columbia Law School
Office: [redacted]
Cell: [redacted]

b6 -1,4
b7C -1,4
b7E -3

On Dec 29, 2016, at 9:49 AM, [redacted] (DO) (OGA) [redacted] wrote:

> Sure—I'll pencil you in for 11:30? (I actually had a Going Dark idea to run by you.)
>
> **From:** Daniel Charles Richman [mailto: [redacted]
> **Sent:** Wednesday, December 28, 2016 2:31 PM
> **To:** [redacted] (DO) (OGA) [redacted]
> **Cc:** Rybicki, James E. (DO) (FBI) [redacted]
> **Subject:** Re: DC visit on Jan 3
>
> b6 -1,4
> b7C -1,4
> b7E -3
>
> Thx. I just heard from her & will see the D at 11:00. Maybe I can catch you afterward?
>
> On Wed, Dec 28, 2016 at 2:29 PM, [redacted] (DO) (OGA) [redacted] wrote:
>
> b6 -1
> b7C -1
> b7E -3
>
>> Dan,
>>
>> Hope you had a nice Christmas too. [redacted] is looking into scheduling for the 3rd and will be in touch soon.
>>
>> Thanks,
>> [redacted]
>>
>> **From:** Daniel Charles Richman [mailto: [redacted]
>> **Sent:** Monday, December 26, 2016 7:02 PM
>> **To** [redacted] (DO) (OGA) [redacted]
>> Rybicki, James E. (DO) (FBI) [redacted]
>> **Subject:** DC visit on Jan 3
>>
>> b6 -1,4
>> b7C -1,4
>> b7E -3
>>
>> Dear Jim & [redacted] - Hope you guys had a lovely Christmas. I'm planning to be in DC Jan 2-4. Mostly for fun, but the D said I should come his office Jan 3. I figure I should coordinate this with one or both of you & maybe even get to see you when I'm there
>> thx
>> dan richman
>>
>> --
>> Daniel Richman
>> Paul J. Kellner Professor of Law,
>> Columbia Law School
>> office [redacted]
>> cellphone [redacted]
>> You can download my papers at http://ssrn.com/author=937729
>>
>> Spam

Not spam
Forget previous vote

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office [redacted]
cellphone [redacted]
You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

Spam
Not spam
Forget previous vote

[redacted] (DO) (OGA)

b6 -1
b7C -1

From: [redacted] (DO) (OGA)
Sent: Friday, January 06, 2017 12:12 PM
To: Daniel Charles Richman
Subject: RE: Going Dark Comparative Approaches

Thanks—I'll share the letter with the wider DOJ group to make sure they know. Do you happen to know if there is already Bu coverage for the Feb. 7th meeting? If not, I'm happy to make sure its staffed appropriately.

2. That's nice of you. When you have a moment sometime let's chat about it?

From: Daniel Charles Richman [mailto [redacted]
Sent: Friday, January 06, 2017 12:04 PM
To [redacted] (DO) (OGA) [redacted]
Subject: Re: Going Dark Comparative Approaches

b6 -1,4
b7C -1,4
b7E -3

Thanks. Just looking at it. Also
1. I was in touch with Kenn Kern, at DANY who says "The state and local law enforcement community is convening in DC on Feb 7 on encryption. There is a real sense of momentum." He also send me a recent letter to House Judiciary Committee in opposition to their recent Report. See attached.
2. I checked with Jim Rybicki on your detail status. He said that they "can definitely reup" you. You and I should make sure this doesn't fall thru the cracks
d

On Fri, Jan 6, 2017 at 11:59 AM, [redacted] (DO) (OGA) [redacted] wrote:

b6 -1,4
b7C -1,4
b7E -3

We received the international GD legal piece from CRM. I forwarded to you on your FBI email account.

----- Original Message-----
From: Daniel Charles Richman [mailto: [redacted]
Sent: Tuesday, January 03, 2017 4:50 PM
To: [redacted] (DO) (OGA) [redacted]
Subject: Re: Going Dark Comparative Approaches

Thx. It's a start. And it's been out since may :(Lovely seeing you

Daniel Richman
Paul J. Kellner Professor of Law
Columbia Law School
Office: [redacted]
Cell: [redacted]

b6 -1,4
b7C -1,4
b7E -3

> On Jan 3, 2017, at 4:28 PM, [redacted] (DO) (OGA) [redacted] wrote:
>

>
>
> ----- Original Message -----
> From: [redacted] (DO) (OGA)
> Sent: Tuesday, January 03, 2017 4:28 PM
> To: [redacted] (ODAG) (JMD) [redacted]
> Subject: Going Dark Comparative Approaches
>
> You may have already seen this comparative GD report, but featured on USAbook today.
>
> [redacted]
>
>
>
> --
> BEGIN-ANTISPAM-VOTING-LINKS
> --
>
> Teach Email if this mail (ID 01SrVvCfP) is spam:
> Spam: https://antispam.law.columbia.edu/canit/b.php?i=01SrVvCfP&m=6947e7738b93&t=20170103&c=s
> Not spam: https://antispam.law.columbia.edu/canit/b.php?i=01SrVvCfP&m=6947e7738b93&t=20170103&c=n
> Forget vote:
> https://antispam.law.columbia.edu/canit/b.php?i=01SrVvCfP&m=6947e7738b
> 93&t=20170103&c=f
> --
> END-ANTISPAM-VOTING-LINKS
>
> <GD Comparative Approaches.pdf>

b6 -1,5
b7C -1,5

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office [redacted]
cellphone [redacted]
You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

[redacted] (DO) (OGA) b6 -1 b7C -1

From: [redacted] (DO) (OGA)
Sent: Tuesday, January 03, 2017 4:29 PM
To: Daniel Charles Richman
Subject: FW: Going Dark Comparative Approaches
Attachments: GD Comparative Approaches.pdf

-----Original Message-----
From: [redacted] (DO) (OGA) b6 -1,5
Sent: Tuesday, January 03, 2017 4:28 PM b7C -1,5
To: [redacted] (ODAG) (JMD) [redacted]
Subject: Going Dark Comparative Approaches

You may have already seen this comparative GD report, but featured on USAbook today.

[redacted]

Government Access to Encrypted Communications

Australia · Belgium · Brazil · Canada · European Union
France · Germany · Israel · Japan · South Africa
Sweden · Taiwan · United Kingdom

May 2016

The Law Library of Congress, Global Legal Research Center
(202) 707-6462 (phone) · (866) 550-0442 (fax) · law@loc.gov · http://www.law.gov

This report is provided for reference purposes only.
It does not constitute legal advice and does not represent the official opinion of the United States Government. The information provided reflects research undertaken as of the date of writing.
It has not been updated.

Contents

Comparative Summary

Luis Acosta
Chief, Foreign, Comparative, and International Law Division II

This report describes the law of twelve nations and the European Union on whether the government, pursuant to a court order or other government process, can require companies to decrypt encrypted communications or provide the government with the means to do so. Some of the surveys provide additional information on related surveillance issues like the law on monitoring and intercepting communications.

The report finds that while there is a range of approaches among the surveyed countries, a majority make provision for specified intelligence or law enforcement agencies to obtain access to encrypted communications or the means of decryption under certain circumstances.

In France, national intelligence and security services may obtain authorization from the Prime Minister or his delegate, upon the written request of a senior minister, to intercept and read private communications for specifically enumerated purposes, and may request from providers of cryptology services the means to decipher encrypted communications. French law also provides for investigative judges to order the interception, recording, and transcription of private telecommunications in criminal investigations, and law enforcement authorities may obtain authorization to ask any qualified person to perform the technical operations that would allow access to this information.

In Belgium, the intelligence services may obtain authorization from a special independent commission to secretly access, listen to, or recording private communications, and can serve a written demand to the network operator or the service provider for technical assistance; such providers are required to have the technical ability to provide decrypted copies of communications when requested by Belgian intelligence. Also, investigative judges may authorize communication interception operations under certain legally-defined circumstances, and may order anyone who has a particular knowledge of a relevant encryption service to help access communications in a readable format.

Under current law in the UK, specified law enforcement and intelligence officials under certain circumstances may serve written notice on persons or bodies requiring them to disclose encrypted information in intelligible form. A draft revision of the relevant UK law is being considered.

In Australia, under some circumstances, the police may obtain an order from a court requiring certain persons to provide information or assistance to enable the police to unlock a computer or digital storage device that is subject to a warrant, or to provide information on the decryption of data on such a device in order to make it intelligible to the police.

In Japan, law enforcement officials may request the courts to order the decryption of encrypted information during criminal investigations, and courts may also order the decryption of encrypted information during trials.

In South Africa, a law enforcement officer may apply for a "decryption direction" from a court requiring a decryption key holder to disclose the key or provide decryption assistance.

In some countries, such as Canada and Taiwan, the relevant law does not explicitly address decryption, but does provide a framework under which telecommunications companies are required to assist with government surveillance of communications, and the framework would appear to permit orders requiring them to assist with decryption, at least subject to reasonable technological feasibility.

Similarly, in Brazil, while the relevant law does not make direct reference to decryption pursuant to a warrant, the federal telecommunications agency has provided in regulations that communications providers must make available to certain authorities the technological resources and data relating to the suspension of telecommunications confidentiality. Two known cases apparently involving judicial enforcement of decryption orders (albeit subject to judicial secrecy) suggest that companies may be considered obligated to provide decryption assistance to the government.

In Israel, the law does not specifically address orders for decryption. However, encryption activities are regulated and licensed by the Ministry of Defense, and officials of that Ministry may enter any place where an encryption-related activity is being conducted and request information at any time regarding the subject of an encryption license.

In Germany, certain intelligence and law enforcement agencies have authority to access and intercept communications. While they may use whatever technologies they have at their disposal to unlock encrypted communications, and they may demand telecommunications providers to remove encryption put in place by such providers, there is no legal basis in Germany to compel end users to turn over encryption keys they have used, on the principle that suspects cannot be compelled to cooperate in investigations that would incriminate themselves.

Under current Swedish law, it appears unlikely that a Swedish court would force an ISP, encryption firm, or other entity to decrypt data, because warrants must satisfy a proportionality test, and an order of decryption would not likely be considered proportional. There have been some calls and proposals for legislative changes.

At the European Union level, there is no EU legislation that requires tech companies to disclose the keys to encrypted materials to law enforcement authorities, or to decrypt communications upon the request of a government. Relevant agencies on cybersecurity, organized crime, and terrorism have not reached a uniform position on this issue.

Australia

Kelly Buchanan
Chief, Foreign, Comparative, and
International Law Division I

SUMMARY Various federal statutes in Australia relate to the ability of government agencies to intercept and access communications and other data for law enforcement and national security purposes. In terms of requirements for persons to assist in decrypting information, under the Crimes Act 1914 (Cth) federal and state police may obtain an order for certain persons to provide "any information and assistance" necessary to enable an officer to access data in a computer or digital storage device that is subject to a warrant and to make that data intelligible. Such orders can only be made with respect to a "person under investigation, an owner of the device, an employee of the owner, a relevant contractor, a person who has used the device, or a systems administrator."

The Telecommunications (Interception and Access) Act 1979 (Cth) (TIA Act), which provides a warrant system for intercepting communications and accessing stored communications, does not include a specific requirement for service providers to assist in making encrypted communications or other data intelligible. Under that Act and the Telecommunications Act 1997 (Cth), carriers and carriage service providers are required to provide assistance to officials, including by giving effect to stored communications warrants, providing interception services, and providing "relevant information" about communications.

There have been multiple reviews of the TIA Act and related legislation over the years. Following a report by the Australian Law Reform Commission on privacy issues and recommendations by a parliamentary committee on reforming national security legislation, another parliamentary committee examined the need for a comprehensive revision of the TIA Act. The government has indicated that it will consider possible changes to the Act, including consulting with the telecommunications industry and relevant agencies on the development of appropriate legislative provisions to address issues related to accessing encrypted information.

I. Introduction

There are several federal statutes relevant to the ability of Australian law enforcement and intelligence agencies to access and intercept electronic communications and other data:[1]

- Telecommunications (Interception and Access) Act 1979 (Cth) (TIA Act):[2] This Act provides for various federal and state agencies to obtain interception warrants and stored communications warrants for law enforcement and national security purposes.

[1] *See generally Telecommunications Interception and Surveillance: Overview of Legislation*, ATTORNEY-GENERAL'S DEPARTMENT, https://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Pages/Overviewoflegislation.aspx (last visited Apr. 8, 2016), *archived at* https://perma.cc/CRE2-EZZF.

- Surveillance Devices Act 2004 (Cth):[3] This Act provides for eligible federal agencies to obtain warrants to install and use surveillance devices, including data surveillance devices.
- Telecommunications Act 1997 (Cth):[4] This Act requires that carriers and carriage service providers provide assistance to relevant agencies for the purposes of law enforcement and safeguarding national security.
- Australian Security Intelligence Organisation Act 1979 (Cth) (ASIO Act): This Act provides the Australian Security Intelligence Organisation (ASIO) with various powers, including the ability to obtain computer access warrants and surveillance device warrants.
- Crimes Act 1914 (Cth):[5] This Act includes various search and information-gathering powers of law enforcement officers, including the ability to access data held in a computer or other data storage device.

The powers and procedures in these laws related to electronic communications and data have been the subject of several reviews, with the discussion encompassing the impact of new technologies (including encryption technologies) and the need to balance privacy considerations with national security and law enforcement interests.[6] The most recent change that has resulted from these reviews was the amendment of the TIA Act in 2015 to put in place a data retention system that requires service providers to retain certain data related to communications (i.e., "metadata" rather than content) for a set period of time.[7]

II. Access to Information Held in a Computer

A. Order to Assist Law Enforcement Officer to Access Data

Section 3LA of the Crimes Act 1914 enables a member of the Australian Federal Police (AFP) or a state police force[8] to apply to a magistrate "for an order requiring a specified person to provide any information or assistance that is reasonable and necessary" to allow the member to

[2] Telecommunications (Interception and Access) Act 1979 (Cth) (TIA Act), https://www.legislation.gov.au/Details/C2016C00102, *archived at* https://perma.cc/CD3H-SGW7.

[3] Surveillance Devices Act 2004 (Cth), https://www.legislation.gov.au/Details/C2016C00103, *archived at* https://perma.cc/AA2T-8AM3.

[4] Telecommunications Act 1997 (Cth), https://www.legislation.gov.au/Details/C2016C00107, *archived at* https://perma.cc/4RA5-7YFQ.

[5] Crimes Act 1914 (Cth), https://www.legislation.gov.au/Details/C2016C00121, *archived at* https://perma.cc/Q7XY-ZKJ6.

[6] *See infra*, Part IV.

[7] Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 (Cth), https://www.legislation.gov.au/Details/C2015A00039, *archived at* https://perma.cc/TP4K-HQGP. *See generally Data Retention*, ATTORNEY-GENERAL'S DEPARTMENT, https://www.ag.gov.au/NationalSecurity/DataRetention/ Pages/Default.aspx (last visited Apr. 8, 2016), *archived at* https://perma.cc/6UFK-W2NF.

[8] *See* definition of "constable" in section 3 of the Crimes Act 1914 (Cth).

- "access data held in, or accessible from, a computer or data storage device"[9] that is on the premises subject to a warrant or has been moved elsewhere for examination or processing, or that has otherwise been seized in accordance with the Act;
- "copy data held in, or accessible from, a computer, or data storage device, . . . to another data storage device"; and/or
- "convert into documentary form or another form intelligible to a constable" data held in, accessible from, or copied from a computer or device.[10]

Therefore, it appears that a person may be ordered to provide information related to (1) unlocking a computer or digital storage device that is subject to a warrant, and (2) the decryption of data on such a computer or digital storage device in order to make it accessible and intelligible to the police.

The magistrate may grant the order if he or she is satisfied that there are "reasonable grounds for suspecting that evidential material is held in, or accessible from, the computer or data storage device."[11] In addition, the magistrate must be satisfied that the person specified in the application is either "reasonably suspected of having committed the offense stated in the relevant warrant," or is the owner or lessee of the computer or device, an employee of or engaged under a contract of service by the owner or lessee, a person who uses or has used the computer or device, or a person who is or was a system administrator for the relevant system that includes the computer or device.[12] The specified person must also have relevant knowledge of the computer or device or the relevant computer network, or of the "measures applied to protect data held in, or accessible from, the computer or device."[13] Thus, if a technology company, or employee of such a company, does not fall within these categories it cannot be subject to an order requiring it to provide access to the data on a device.

If a person does not comply with an order made under section 3LA, he or she may be charged with an offense that is subject to a penalty of two years' imprisonment.[14]

B. ASIO Powers

There is no similar provision in the ASIO Act requiring a person to provide assistance to ASIO in order for it to access or read data on a computer. A computer access warrant issued by the relevant government Minister under the ASIO Act may authorize the agency to do certain things, including using the target computer, a telecommunications facility, any other electronic equipment, a data storage device, another computer, or a communication in transit for the

[9] "Data storage device" is defined in section 3 of the Crimes Act 1914 (Cth) as "a thing containing, or designed to contain, data for use by a computer."

[10] Crimes Act 1914 (Cth), s 3LA(1).

[11] *Id.* s 3LA(2)(a).

[12] *Id.* s 3LA(2)(b).

[13] *Id.* s 3LA(2)(c).

[14] *Id.* s 3LA(5).

purpose of obtaining access to the relevant data held in the target computer. If necessary, this can include "adding, copying, deleting or altering other data in the target computer" or in the other computer, or the communication in transit.[15]

III. Interception of Communications and Access to Stored Communications

A. Warrant System

1. Interception Warrants

Under the TIA Act, the Director-General of Security may request an interception warrant, issued by the Attorney-General, with respect to a telecommunications service,[16] where the interception of communications made to or from that service will assist ASIO in carrying out its function of obtaining intelligence relating to national security.[17] "Named person warrants" can also be issued that allow the interception of communications made to or from any telecommunications service that the particular person uses or those made using a device identified in the warrant.[18]

In the course of investigating serious offenses, federal law-enforcement agencies and anticorruption agencies, as well as designated state police forces and other agencies, can apply for similar warrants with respect to a telecommunications service or person.[19] These are issued by an eligible judge or nominated Administrative Appeals Tribunal (AAT) member.[20]

2. Stored Communications Warrants

The TIA Act "establishes a system of preserving certain stored communications that are held by a carrier" in order to prevent them from being destroyed before they can be accessed under certain warrants.[21] It also authorizes the issuance of stored communications warrants to criminal

[15] ASIO Act s 25A(4)(a) & (ab).

[16] "Telecommunications service" is defined in section 5 of the TIA Act as "a service for carrying communications by means of guided or unguided electromagnetic energy or both, being a service the use of which enables communications to be carried over a telecommunications system operated by a carrier but not being a service for carrying communications solely by means of radiocommunication."

[17] TIA Act s 9(1). Warrants issued to ASIO under chapter 2 of the TIA are also referred to as "Part 2-2 warrants."

[18] *Id.* s 9A.

[19] *Id.* ss 46 & 46A. "Serious offence" is defined in section 5D of the TIA Act.

[20] *Id.* s 39, 46 & 46A. Such warrants are also referred to as "Part 2-5 warrants."

[21] *Id.* s 107G. "Carrier" and "carriage service provider" (included in the definition of "carrier" in section 5 of the TIA Act) are defined in the Telecommunications Act 1997 (Cth). A "carriage service provider" is a person who supplies, or proposes to supply, a listed carriage service using "a network owned by one or more carriers" or "a network unit in relation to which a nominated carrier declaration is in force." Telecommunications Act 1997 (Cth) s 87. "Carriage service" means "a service for carrying communications by means of guided and/or unguided electromagnetic energy." *Id.* s 7. A "carrier" refers to a holder of a carrier license issued under the Act. The Act requires that the owner of a network unit used to supply carriage services to the public must hold a carrier license, unless a declaration or exemption applies. *See id.* s 41.

law enforcement agencies in the course of investigating a "serious contravention."[22] Such warrants can be issued by a judge, magistrate, or certain Administrative Appeals Tribunal members.[23] They authorize access to a stored communication that was made by the person named in the warrant, or by another person with the person named in the warrant being the intended recipient.[24]

Interception warrants issued to ASIO, outlined above, are taken to authorize access to a stored communication where "the warrant would have authorised interception of the communication if it were still passing over a telecommunications system."[25]

B. Requirement for Carriers and Service Providers to Assist Agencies

Carriers and carriage service providers[26] (including Internet service providers) are required to provide certain assistance to ASIO and law enforcement agencies under the Telecommunications Act 1997 (Cth).[27] However, there is no specific requirement for carriers and service providers to assist agencies by making intercepted or stored encrypted communications intelligible.

Part 14 of the TIA Act, titled "National Interest Matters," establishes obligations for such entities to

- "do their best to prevent telecommunications networks and facilities from being used to commit offenses"; and
- "give authorities such help as is reasonably necessary" for the purposes of "enforcing the criminal law and laws imposing pecuniary penalties," "protecting the public revenue," and "safeguarding national security."[28]

Such help includes giving assistance by way of

> (a) the provision of interception services, including services in executing an interception warrant under the Telecommunications (Interception and Access) Act 1979; or

[22] TIA Act s 116. "Criminal law enforcement agencies" for the purposes of this part are listed in section 110A of the TIA Act. "Serious contravention" is defined in section 5E of the TIA Act.

[23] *Id.* ss 110, 116 & 6DB.

[24] *Id.* s 117.

[25] *Id.* s 109(a).

[26] *See* definition of "carriers" and "carriage service providers," *supra* note 21.

[27] *See generally Law Enforcement (Telecommunications)*, AUSTRALIAN COMMUNICATIONS AND MEDIA AUTHORITY (ACMA), http://www.acma.gov.au/theACMA/law-enforcement-telecommunications (last updated Feb. 23, 2016), *archived at* https://perma.cc/TTR9-YZY4; *Licensing – I Want to be an ISP: Carriage Service Provider Rules: Law Enforcement*, ACMA, http://www.acma.gov.au/Industry/Internet/Licensing--I-want-to-be-an-ISP/Carriage-service-provider-rules/isps-and-law-enforcement-isp-licensing-i-acma (last updated Mar. 7, 2014), *archived at* https://perma.cc/GC43-7FLA.

[28] Telecommunications Act 1997 (Cth) s 311. *See also id.* s 313(1) & (3).

(b) giving effect to a stored communications warrant under that Act; or

(c) providing relevant information about:

(i) any communication that is lawfully intercepted under such an interception warrant; or

(ii) any communication that is lawfully accessed under such a stored communications warrant; or

(ca) complying with a domestic preservation notice or a foreign preservation notice that is in force under Part 3-1A of that Act; or

(d) giving effect to authorisations under Division 3 or 4 of Part 4-1 of that Act [related to accessing telecommunications data]; or

(e) disclosing information or a document in accordance with section 280 of this Act [related to disclosures of certain information in compliance with a warrant or as required or authorized by or under law].[29]

Additional obligations are contained in Chapter 5 of the TIA Act. These primarily relate to data retention requirements[30] and interception capability.[31] This includes a requirement to comply with any determinations regarding the interception capabilities that a carrier must develop, install, and maintain.[32] Carriers and nominated carriage service providers must also develop interception capability plans and submit these annually to the Communications Access Coordinator in the Attorney-General's Department for consideration.[33] Approval of such plans may be granted following consultation with interception agencies.[34]

IV. Reviews of the Relevant Laws

The following three reviews or inquiries, conducted in the past ten years, include discussions of the impact of new technologies and privacy considerations in relation to intercepting or accessing electronic communications:

- Australian Law Reform Commission (ALRC) inquiry into Australian privacy law and practice (completed 2008)[35]

[29] *Id.* s 313(7).

[30] TIA Act pt 5-1A.

[31] *Id.* pts 5-3 to 5-6.

[32] *Id.* ss 189 & 190.

[33] *Id.* ss 195(2) & 198(1); *Interception Capability Plans*, ATTORNEY-GENERAL'S DEPARTMENT, https://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Pages/InterceptionCapabilityPlans.aspx (last visited Apr. 11, 2016), *archived at* https://perma.cc/WA3B-YJNG. The Communication Access Coordinator "liaises between law enforcement agencies and the telecommunications industry." *Id.*

[34] TIA Act s 198(2).

[35] *For Your Information: Australian Privacy Law and Practice (ALRC Report 108)*, AUSTRALIAN LAW REFORM COMMISSION (ALRC), http://www.alrc.gov.au/publications/report-108 (last visited Apr. 11, 2016), *archived at* https://perma.cc/497T-FNQM.

- Parliamentary Joint Committee on Intelligence and Security (PJCIS) inquiry into potential reforms of national security legislation (completed May 2013)[36]
- Senate Legal and Constitutional Affairs References Committee inquiry regarding the comprehensive revision of the TIA Act (completed March 2015).[37]

Prior reviews relevant to the TIA Act were also carried out in 1994, 1999, 2000, 2003, and 2005.[38] Various amendments have been enacted implementing some of the recommendations that resulted from these reviews.

A. ALRC Report

Chapter 73 of the ALRC report examined the TIA Act, including its interaction with the Privacy Act 1988 (Cth), and made several recommendations for particular legislative and procedural changes.[39] It also recommended that the government "should initiate a review to consider whether the Telecommunications Act 1997 (Cth) and the Telecommunications (Interception and Access) Act 1979 (Cth) continue to be effective in light of technological developments (including technological convergence), changes in the structure of communication industries and changing community perceptions and expectations about communication technologies."[40]

B. PJCIS Inquiry

Chapter 2 of the 2013 PJCIS report on its inquiry into a package of potential reforms to national security legislation relates to telecommunications interception.[41] The committee recommended various changes to the TIA Act, including in relation to privacy protections.[42] It also recommended that the Attorney-General's Department conduct a review of the legislation and that the TIA Act should be "substantially revised," with a new interception system designed that is underpinned by clear protection for the privacy of communications, provisions that are

[36] *Inquiry into Potential Reforms of National Security Legislation*, PARLIAMENT OF AUSTRALIA, http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/index.htm (last visited Apr. 11, 2016), *archived at* https://perma.cc/XY8C-MC52.

[37] *Comprehensive Revision of Telecommunications (Interception and Access) Act 1979*, PARLIAMENT OF AUSTRALIA, http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/Comprehensive_revision_of_TIA_Act (last visited Apr. 11, 2016), *archived at* https://perma.cc/A39M-S6RV.

[38] *Telecommunications Interception Reviews*, ATTORNEY-GENERAL'S DEPARTMENT, https://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Pages/TIReviews.aspx (last visited Apr. 11, 2016), *archived at* https://perma.cc/7GGD-T6GV; *see also* ALRC, 3 FOR YOUR INFORMATION: AUSTRALIAN PRIVACY LAW AND PRACTICE 2530–32 (ALRC Report 108, 2008) (ALRC Report), http://www.alrc.gov.au/sites/default/files/pdfs/publications/108_vol3.pdf, *archived at* https://perma.cc/2W6C-LHLV.

[39] ALRC Report at 2478.

[40] *Id.* at 2395.

[41] PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY (PJCIS), REPORT OF THE INQUIRY INTO POTENTIAL REFORMS OF AUSTRALIA'S NATIONAL SECURITY LEGISLATION (May 2013) (PJCIS Report), http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/report/full.pdf, *archived at* https://perma.cc/XXX8-YJAQ.

[42] *See id.* at xxiii–xxv (recommendations 1–4, 6 & 8).

technology neutral, maintenance of investigative capabilities, clearly articulated and enforceable industry obligations, and robust oversight and accountability.[43]

As part of the inquiry, the Attorney-General's Department proposed that an offense should be introduced for failure by telecommunications providers to assist in the decryption of communications. The Department stated that

> Section 3LA of the Crimes Act 1914 (the Crimes Act) sets out provisions concerning decryption regarding information obtained under search warrants; however this does not extend to communications intercepted pursuant to a warrant under the TIA Act.
>
> In summary, section 3LA of the Crimes Act allows a police officer to apply to a magistrate for a warrant to require a person to provide in accessible form (i.e. in decrypted form) data held on a computer or data storage device, where the computer or data storage device had been seized under a warrant. A warrant may be applied to the person under investigation, an owner of the device, an employee of the owner, a relevant contractor, a person who has used the device, or a systems administrator. There is a penalty of up to two years imprisonment for failing to comply with an order.
>
> A consistent approach to that contained in the Crimes Act would ensure that information lawfully accessed for national security or law enforcement purposes under the TIA Act was intelligible.[44]

The PJCIS report noted support for the proposal from certain law enforcement agencies and also reflected the objections of different groups.[45] It considered that there was some lack of clarity and specificity in what was being proposed[46] and recommended that, should the government decide to develop an offense of failing to provide decryption assistance, it should do so in consultation with the telecommunications industry and relevant government agencies.[47]

C. TIA Act Revision Inquiry

The Senate committee's inquiry regarding the comprehensive revision of the TIA Act was carried out over a fifteen-month period, with the report being issued in March 2015.[48] The

[43] *Id.* at xxviii (recommendation 18).

[44] *Id.* at 59–60; Attorney-General's Department, Submission to PJCIS, Inquiry into Potential Reforms of National Security Legislation (submission 218), at 7, http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/subs/sub%20218.pdf, *archived at* https://perma.cc/NXE8-KC62.

[45] PJCIS Report, *supra* note 41, at 60–63.

[46] *Id.* at 63 & 64.

[47] *Id.* at 64 (recommendation 16).

[48] SENATE LEGAL AND CONSTITUTIONAL AFFAIRS REFERENCES COMMITTEE, COMPREHENSIVE REVISION OF THE TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) ACT 1979, at 1 (Mar. 2015), http://www.aph.gov.au/~/media/Committees/Senate/committee/legcon_ctte/tia_act/report/report.pdf?la=en, *archived at* https://perma.cc/KN7S-NLC9.

committee was asked by the Senate to have regard to both the ALRC report and the PJCIS report.[49]

The committee noted that "all law enforcement and national security agencies agreed that the current TIA Act was at risk of becoming ineffective without reform."[50] Of particular concern was that the TIA Act should be modernized in order to keep pace with changes in technology, including the view, expressed by the Australian Crime Commission, that the TIA Act "must be capable of overcoming technical advances which are deliberately used to prevent law enforcement from lawfully intercepting and accessing communications."[51]

The chair of the committee recommended that the TIA Act be "substantially redrafted" to enact a single attribute-based warrant system, and that a Public Interest Monitor should be established to have oversight of the warrant system.[52] Other members agreed with the recommendation for a substantial revision of the Act and the establishment of a single warrant, although some did not think a Public Interest Monitor was necessary.[53]

D. Government Response

In July 2015 the government released its response to recommendations related to the TIA Act that were included in the PJCIS report on national security legislation.[54] It indicated support for nearly all of the recommendations, including the recommendation related to the potential establishment of an offense for failure to assist in decrypting communications. The response stated that

> [t]he Australian government supports strong encryption, which underpins modern, secure communications technologies. These technologies are fundamental to a digital economy, and provide an unparalleled opportunity for exercise of the fundamental freedoms of expression, peaceful assembly and association.
>
> However, the use of encrypted communications for serious criminal purposes and purposes prejudicial to security represents an increasingly significant barrier to the ability of governments to bring serious offenders to justice.

[49] *Id.* at 3.

[50] *Id.* at 10.

[51] *Id.*

[52] *Id.* at 41.

[53] *Id.* at 82–87.

[54] AUSTRALIAN GOVERNMENT RESPONSE TO CHAPTERS 2 AND 3 OF THE PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY'S REPORT OF THE INQUIRY INTO POTENTIAL REFORMS OF AUSTRALIA'S NATIONAL SECURITY LEGISLATION (July 1, 2015) (Government Response), http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=pjcis/nsl2012/govresponse.pdf, *archived at* https://perma.cc/S9XA-CEX4; *PJCIS Committee Activities (Inquiries and Reports), 43rd Parliament (September 2010–August 2013)*, PARLIAMENT OF AUSTRALIA, http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=pjcis/reports.htm (last visited Apr. 12, 2016), *archived at* https://perma.cc/69ZZ-SMWT.

> Accordingly, the Government will explore, in consultation with agencies and the telecommunications industry, the development of appropriate legislative provisions, including safeguards, oversight and accountability measures.[55]

More broadly, the government stated that it intends to finalize its detailed response to a number of the recommendations related to the TIA Act following the delivery of a report concerning whether the agencies that may access the content of communications should be standardized, which is to be completed by April 13, 2017.[56]

[55] Government Response, *supra* note 54, at 11–12.

[56] *See id.* at 2–3, 4 & 8.

Belgium

Nicolas Boring
Foreign Law Specialist

I. Decryption at the Request of Intelligence and Security Services

The main legislative framework for intelligence-gathering in Belgium is the Law of November 30, 1998, Organizing the Intelligence and Security Services.[1] Article 18/17 of this Law provides that intelligence services may "listen to, gain knowledge of, and record communications" in order to fulfill their missions.[2] An intelligence service must obtain prior authorization from a special independent commission before secretly accessing, listening to, or recording private communications.[3] When an intelligence service has obtained the required authorization to conduct this kind of surveillance on an electronic communications network, it can serve a written demand to the network operator or the service provider, upon which the network operator or service provider is required to give technical assistance to the intelligence service.[4] Any person who refuses to give technical assistance pursuant to a properly authorized demand is punishable by a fine of €26 to €10,000 (about US$29 to US$11,270).[5] On the other hand, companies and individuals who cooperate in giving technical assistance are paid for their services on the basis of government-established rates.[6]

The principal statute governing electronic communications in Belgium requires that network operators as well as end users be capable of allowing the authorities to "listen to, gain knowledge of, and record" communications.[7] A Royal Order from 2010 includes electronic communications service providers alongside network operators as being required to have the technical ability to provide clear and readable (decoded, decompressed, and decrypted) copies of communications requested by Belgian intelligence services.[8] It appears, in other words, that

[1] Loi du 30 novembre 1998 organique des services de renseignement et de sécurité [Organic Law of November 30, 1998, Organizing the Intelligence and Security Services], http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&table_name=loi&cn=1998113032, *archived at* https://perma.cc/58QH-E735.

[2] *Id.* art. 18/17.

[3] *Id.* art. 43/1.

[4] *Id.* art. 18/17.

[5] *Id.*

[6] *Id.* art. 18/18.

[7] Loi du 13 juin 2005 relative aux communications électroniques [Law of June 13, 2005, Regarding Electronic Communications] art. 127, http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2005061332&table_name=loi, *archived at* https://perma.cc/92QM-7E5S.

[8] Arrêté royal du 12 octobre 2010 déterminant les modalités de l'obligation de collaboration légale en cas de demandes concernant les communications électroniques par les services de renseignement et de sécurité [Royal Order of October 12, 2010, Establishing the Conditions of the Obligation of Lawful Collaboration in Cases of Demands by Intelligence and Security Services Regarding Electronic Communications] art. 8, http://www.ejustice.just.fgov.be/cgi_loi/loi_a.pl, *archived at* https://perma.cc/5ZG7-VUL9.

service providers and network operators may not use or make available any form of encryption that they would be unable to decrypt themselves.

II. Decryption at the Request of Judicial and Law Enforcement Agencies

The Belgian Code of Criminal Investigations allows investigative judges (*juges d'instruction*) to "listen to, gain knowledge of, and record" private communications when warranted by certain legally-defined circumstances.[9] An investigative judge must authorize the communication interception operation by a reasoned ordinance, which must be sent to the Royal Prosecutor.[10] An investigative judge may order anyone who has a particular knowledge of the communication service or, if the communication is protected or encrypted, of the protection and encryption service, to help access the communication in a readable format.[11] Refusal to cooperate is punishable by between six months and one year of incarceration, and a fine.[12] A 2003 Royal Order governing the cooperation of electronic communications providers with judicial authorities was amended in 2011 to require that electronic communications service providers and network operators have the technical ability to provide clear and readable copies of communications requested by Belgian judicial authorities.[13]

[9] CODE D'INSTRUCTION CRIMINELLE [CODE OF CRIMINAL INVESTIGATIONS] art. 90ter, http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language= fr&la=F&table_name=loi&cn=1808111730, *archived at* https://perma.cc/N2GE-PMAE.

[10] *Id.* art. 90quater.

[11] *Id.*

[12] *Id.*

[13] Arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques [Royal Order of January 9, 2003, Establishing the Conditions of the Obligation of Lawful Collaboration in Cases of Judicial Demands Regarding Electronic Communications] art. 6, http://www.ejustice.just.fgov.be/cgi_loi/loi_a1.pl?sql=%28text%20contains%20%28%27%27%29%29&language=fr&rech=1&tri=dd%20AS%20RANK&value=&table_name=loi&F=&cn=2003010942&caller=image_a1&fromtab=loi&la=F, *archived at* https://perma.cc/VAA8-ZVBF.

Brazil

Eduardo Soares
Senior Foreign Law Specialist

SUMMARY In Brazil, a constitutional principle provides for the protection of communications. A federal law regulates the breach of such protection by a court order, while a federal agency determines whether the providers of telecommunications and multimedia services must make available to the authorities the technological resources necessary to suspend telecommunications confidentiality in accordance with the law.

The Code of Civil Procedure does not provide any exemption from the duty to cooperate with the Judiciary, the Penal Code imposes jail time on those who disobey a court order, and a federal law punishes with imprisonment anyone who obstructs the investigation of a criminal offense involving a criminal organization.

I. Access to Communications

This report discusses the Brazilian legal framework for privacy of communications. This framework includes the constitutional principle that protects the secrecy of communications in the country and the law that regulates this principle and grants access to an individual's communications, provided that such access has been authorized by a court order. The report also discusses the federal agency that regulates telecommunications in the country and that agency's regulations regarding the suspension of telecommunications confidentiality as a result of a court order.

Provisions of the Brazilian Code of Civil Procedure, the Penal Code, and a federal law that punish disobedience to court orders, is also addressed. The report also offers two examples of application of the abovementioned laws in connection with court orders directing two different companies to grant access to the accounts of individuals who were under criminal investigation.

A. Constitutional Principle

According to article 5, section XII, of the Brazilian Constitution, the secrecy of correspondence and of telegraphic, data, and telephonic communications is inviolable. The only exception is for legally defined, court-ordered interceptions of telephonic communications in criminal investigations and fact-finding phases of criminal prosecutions (*instrução processual penal*).[1]

B. Law No. 9,296 of July 24, 1996

On July 24, 1996, Law No. 9,296 was enacted to regulate the final part of section XII of article 5 of the Constitution regarding lawful interceptions of communications. The Law states that the

[1] CONSTITUIÇÃO FEDERAL [C.F.] art. 5(XII), http://www.planalto.gov.br/ccivil_03/Constituicao/ Constituicao.htm, *archived at* https://perma.cc/FH8R-Z4Y6.

interception of telephone communications of any kind, as proof in a criminal investigation or in the fact-finding phase of a criminal prosecution, requires a court order issued by the competent judge in the main legal action, under judicial secrecy.[2] It also says that this provision applies to the interception of the flow of communications on data systems (*sistemas de informática e telemática*).[3]

C. Law No. 9,472 of July 16, 1997

Law No. 9,472 of July 16, 1997, provides for the organization of telecommunications services in the country. The Law created the National Telecommunications Agency (Agência Nacional de Telecomunicações, ANATEL), a federal agency subordinate to the Ministry of Communications and charged with the duty of regulating telecommunications in the country.[4]

"Telecommunications" are defined by Law No. 9,472 as the "transmission, emission, or reception, by wire, radio, optical, or other electromagnetic process, of symbols, characters, signals, writing, images, sounds, or information of any kind."[5]

Pursuant to article 3 of Law No. 9,472, the user of telecommunications services has the right to the inviolability and secrecy of his or her communications, except in the cases and conditions established in the Constitution and the law.[6]

1. Resolution ANATEL No. 73 of November 25, 1998

Fulfilling its duties as established under Law No. 9,472, on November 25, 1998, ANATEL issued Resolution No. 73, which approved the regulation of telecommunications services (*Regulamento dos Serviços de Telecomunicações*).[7] The Resolution defines "telecommunications services" as the set of activities that enables the "transmission, emission or reception, by wire, radio, optical or other electromagnetic process, of symbols, characters, signals, writing, images, sounds or information of any kind."[8]

The provider of telecommunications services is obligated to safeguard the privacy inherent in telecommunications services and the confidentiality of data and information, using all necessary means and technology to ensure this right of users. The provider must make available the technological resources necessary to suspend telecommunications confidentiality when so ordered by

[2] Lei No. 9.296, de 24 de Julho de 1996, art. 1, http://www.planalto.gov.br/ccivil_03/leis/L9296.htm, *archived at* https://perma.cc/RB7M-WLTA.

[3] *Id.* art. 1(sole para.).

[4] Lei No. 9.472, de 16 de Julho de 1997, art. 8, http://www.planalto.gov.br/ccivil_03/leis/L9472.htm, *archived at* https://perma.cc/C5QX-AJBP.

[5] *Id.* art. 60(§1).

[6] *Id.* art. 3(V).

[7] Resolução ANATEL No. 73, de 25 de Novembro de 1998, art. 1, http://www.anatel.gov.br/legislacao/resolucoes/13-1998/34-resolucao-73, *archived at* https://perma.cc/B8B6-FZN9.

[8] Resolução ANATEL No. 73, anexo, art. 2.

a judicial authority and "maintain permanent control" of all cases, after the execution of such orders, ensuring that they are strictly fulfilled within the authorized limits.[9]

2. Resolution ANATEL No. 614 of May 28, 2013

To regulate multimedia communications services (*Serviço de Comunicação Multimídia*), on May 28, 2013, ANATEL issued Resolution No. 614.[10] The regulation defines "multimedia information" as "audio signals, video, data, voice and other sounds, images, texts and other information of any kind."[11]

The provider of multimedia communications services must ensure the secrecy inherent in telecommunications services and the confidentiality of data, including connection records and subscriber information, using all means and technology available.[12] The provider must make available to the authorities authorized to request such information data relating to the suspension of telecommunications confidentiality.[13]

D. Code of Civil Procedure

The new Brazilian Code of Civil Procedure determines that no one is exempt from the duty to cooperate with the judiciary for the discovery of truth.[14]

E. Penal Code

The Penal Code provides that disobeying a legal order is punishable by imprisonment for fifteen days to six months and a fine.[15]

F. Law No. 12,850 of August 2, 2013

Law No. 12,850 of August 2, 2013, defines the term "criminal organization" and provides for criminal investigations, the means of obtaining evidence, criminal offenses related to criminal organizations, and criminal prosecution.[16] At any stage of a criminal prosecution, authorities are allowed to access telephone records and data links, records of public and private databases, and

[9] *Id.* art. 26.

[10] Resolução ANATEL No. 614, de 28 de Maio de 2013, art. 1, http://www.anatel.gov.br/legislacao/resolucoes/2013/465-resolucao-614#art3res, *archived at* https://perma.cc/2HBD-CS26.

[11] Resolução ANATEL No. 614, anexo, art. 4(VII).

[12] *Id.* art. 52.

[13] *Id.* art. 52(sole para.).

[14] CÓDIGO DE PROCESSO CIVIL, Lei No. 13.105, de 16 de Março de 2015, art. 378, http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Lei/L13105.htm#art378, *archived at* https://perma.cc/WB5A-79XA.

[15] CÓDIGO PENAL, Decreto-Lei No. 2.848, de 7 de Dezembro de 1940, art. 330, http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm, *archived at* https://perma.cc/QL9V-UZND.

[16] Lei No. 12.850, de 2 de Agosto de 2013, art. 1, http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm, *archived at* https://perma.cc/CY4B-26RY.

electoral or commercial information, as well as to intercept telephone and data communications, without prejudice to other means already provided by law, according to the specific legislation.[17]

A person who personally or through an intermediary promotes, creates, finances, or participates in a criminal organization is punishable by imprisonment for three to eight years and a fine, and is also subject to the corresponding penalties for other criminal offenses committed.[18] The same penalties apply to those who prevent or in any way obstruct the investigation of a criminal offense involving a criminal organization.[19]

G. Law No. 12,965 of April 23, 2014

In 2014, Brazil issued Law No. 12,965, which establishes principles, guarantees, rights, and duties for the use of the Internet in the country and guidelines for state action.[20]

Article 7 guarantees to Internet users in the country the inviolability and confidentiality of the flow of their Internet communications and their stored private communications, except as otherwise dictated by court order.[21]

Article 10 determines that the content of private communications can be made available only by court order, in the cases and manner provided by law, subject to the provisions of sections II and III of article 7 of Law No. 12,965.[22]

According to article 11, the right to privacy, the protection of personal data, and the confidentiality of private communications and records must be respected in any activity involving the collection, storage, custody, and treatment of records, personal data, and communications through Internet service providers and Internet applications when at least one of these acts occur in the national territory.[23] This provision applies to the data collected in the national territory and the contents of communications, provided that at least one of the terminals is located in Brazil.[24] The provision also applies even if the activities are carried out by a legal entity based abroad, provided that the services are offered to the Brazilian public, or at least one member of the same group is established in Brazil.[25]

[17] *Id.* art. 3(IV)–(V).

[18] *Id.* art. 2.

[19] *Id.* art. 2(§1).

[20] Lei No. 12.965, de 23 de Abril de 2014, art. 1, http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm, *archived at* https://perma.cc/CNG4-6AQZ.

[21] *Id.* art. 7(II)–(III).

[22] *Id.* art. 10(§2).

[23] *Id.* art. 11.

[24] *Id.* art. 11(§1).

[25] *Id.* art. 11(§2).

The providers of Internet services and applications must provide, in accordance with the regulation, information allowing verification of compliance with Brazilian legislation on the collection, custody, storage, or processing of data, as well as information demonstrating the protection of privacy and confidentiality of communications.[26]

Pursuant to article 12, the following penalties are applied individually or cumulatively to violations of the rules established in articles 10 and 11 of Law No. 12,965, without prejudice to other civil, criminal, and administrative sanctions:

> I – a warning, with time indication for corrective action;
>
> II – a fine of up to 10% (ten percent) of the economic group revenue [*faturamento*] in Brazil in its previous financial year, excluding taxes, considering the economic condition of the offender and the principle of proportionality between the seriousness of the offense and the intensity of the sanction;
>
> III – temporary suspension of activities involving the acts provided for in article 11; or
>
> IV – a ban on activities involving the acts provided for in article 11.[27]

In the case of a foreign company, the branch, office, or establishment in the country is jointly liable for the payment of fines.[28]

II. Recent Court Cases

Two court cases illustrate the practical application of the legal framework involving the secrecy of communications and its breach by court order. The first occurred in December 2015 and concerned the suspension for forty-eight hours of the WhatsApp application in the country for failure to obey a legal order as determined by article 12 of Law No. 12,965.[29]

The second case involved the use of Law No. 12,850 to arrest the Latin American vice-president of Facebook in Brazil for the apparent obstruction of a criminal investigation because the company refused to provide information requested by a judge related to a criminal investigation involving a criminal organization and drug trafficking.[30]

[26] *Id.* art. 11(§3).

[27] *Id.* art. 12.

[28] *Id.* art. 12 (sole para.).

[29] Marcelo Crespo, *Investigação Criminal, Obstrução da Justiça e Bloqueio do WhatsApp*, CANAL CIÊNCIAS CRIMINAIS (Dec. 17, 2015), http://canalcienciascriminais.com.br/artigo/investigacao-criminal-obstrucao-da-justica-e-bloqueio-do-whatsapp, *archived at* https://perma.cc/55UD-5JJB.

[30] Marcelo Crespo, *O Que Ninguém Falou Sobre o Caso Facebook*, JUSBRASIL (Mar. 2016), http://canalcienciascriminais.jusbrasil.com.br/artigos/310735589/o-que-ninguem-falou-sobre-o-caso-do-facebook?ref=topic_feed, *archived at* https://perma.cc/Y7NB-7MRM.

Both cases are under judicial secrecy (*segredo de justiça*). Therefore, it was not possible to access the cases to precisely determine the legal basis for the actions taken against the executives of the companies and the current status of access to the users' communications.

III. Conclusion

In Brazil, the secrecy of communications is a constitutional principle that can be violated only by a court order. A specific law enacted in this regard regulates the issue and further determines that the authorized interception of communications also encompasses data systems.

The law does not make direct reference to decryption of communications after a warrant has been issued. However, the federal agency in charge of regulating telecommunications, in its regulations defining telecommunications and multimedia services, has specifically determined that the provider of such services must make available to the authorities authorized to request such information the technological resources necessary to suspend telecommunications confidentiality and the data relating to the suspension of telecommunications confidentiality.

In addition to these regulations, the Code of Civil Procedure states that no one is exempt from the duty to cooperate with the judiciary for the discovery of truth, and the Penal Code provides that disobeying a legal order is punishable by fifteen days to six months in jail and a fine.

Furthermore, whoever prevents or in any way obstructs the investigation of a criminal offense involving a criminal organization is punishable by imprisonment for three to eight years and a fine.

Apparently, the burden imposed on companies to make available the technological resources necessary to suspend telecommunications confidentiality includes the obligation to decrypt the communication. Otherwise, a court order granting access to an individual's communications would be easily avoided. In this sense, it seems that this is what occurred in the two cases mentioned above. As a result, in one instance the service was suspended, and in the other the executive was arrested as a means to compel the companies to grant access to the communications, whether encrypted or not.

Canada

Tariq Ahmad
Foreign Law Specialist

SUMMARY In Canada, the term "lawful access" is used to describe the government's surveillance powers, and primarily involves the interception of communications, the search and seizure of information, and the issuance of production and preservation orders. Part VI of Canada's Criminal Code regulates the powers of the police to engage in electronic surveillance or interception of private communications. With some exceptions, these powers require judicial authorization or a warrant before they can be exercised. Canada's existing legal framework for interception, search and seizure, and production of data also applies to encrypted data. However, there does not appear to be a specific provision that imposes requirements on telecommunications providers to decrypt data.

Since 1995, the Solicitor General's Enforcement Standards (SGES) have been in force. The SGES outline twenty-three technical surveillance standards that must be followed as a condition of obtaining a wireless spectrum license in Canada. Standard 12 establishes an obligation that any type of encryption algorithm initiated by a service provider must be provided to a requesting law enforcement agency. This excludes end-to-end encryption.

I. Introduction

In Canada, the term "lawful access" is used to describe the government's surveillance powers, and primarily involves the interception of communications, the search and seizure of information, and the issuance of production orders.[1] With some exceptions, these powers require judicial authorization or a warrant before they can be exercised.

Lawful access powers of the police are regulated by the Criminal Code,[2] while the surveillance powers of the Canadian Security Intelligence Service (CSIS) are governed by the Canadian Security Intelligence Service Act.[3] These powers are subject to the Canadian Charter of Rights and Freedoms and Canada's other privacy laws. On December 9, 2014, Bill C-13,[4] the most recent amending legislation that contains "lawful access" provisions, was passed. The law

[1] *Lawful Access FAQ*, SAMUELSON-GLUSKO CANADIAN INTERNET POLICY & PUBLIC INTEREST CLINIC (CIPPIC), http://www.cippic.ca/lawful-access-faq (last updated June 2, 2007), *archived at* https://perma.cc/MA4C-AGQU.

[2] CRIMINAL CODE, R.S.C. 1985, c. C-46, http://laws-lois.justice.gc.ca/eng/acts/C-46/, *archived at* https://perma.cc/KRF2-KJFN.

[3] Canadian Security Intelligence Service Act, R.S.C. 1985, c. C-23, http://laws-lois.justice.gc.ca/eng/acts/C-23/, *archived at* https://perma.cc/76L5-MHBU.

[4] Act to Amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act (Act) (Protecting Canadians from Online Crime Act), S.C. 2014, c. 31 (in force Mar. 9, 2015), http://laws-lois.justice.gc.ca/eng/annualstatutes/2014_31/FullText.html, *archived at* https://perma.cc/Y6ES-Q6AU.

includes “new investigative powers (preservation demands, preservation orders and production orders) for law enforcement officers for the conduct of their investigation.”[5]

II. Encryption

A. Criminal Code’s Lawful Access Powers

Part VI of Canada’s Criminal Code regulates the powers of the police to engage in electronic surveillance or interception of private communications, including real-time communications, while conducting criminal investigations. Apart from certain exceptions outlined in the Code, judicial authorization is required for the interception of private communications, but in comparison to ordinary search warrants “[t]he requirements for obtaining such an authorization are more onerous.”[6]

Police officials have the power to make demands to preserve computer data.[7] Subject to certain exceptions, searches and seizures[8] of computer data are also subject to judicial warrants. On application, courts may also issue preservation orders to preserve computer data[9] and production orders for the production of transmission[10] or tracking data.[11] In order to disclose the substance of a communication the police must apply for a general production order, which requires a higher evidentiary standard.[12] According to an RCMP statement reported in the news, “wiretap authorization, a search warrant and a general warrant can also be accompanied by an assistance order issued by a court, which compels a third party to provide assistance where that assistance may reasonably be considered as required to give effect to the authorization or warrant.”[13]

[5] Sean Griffin, Anne-Elisabeth Simard & Marianne Bellefleur, *Bill C-13: Lawful Access and the Relationship Between Organizations, Cyber-bullying and the Protection of Privacy Rights*, SNIP/ITS (Feb. 25, 2015), http://www.canadiantechlawblog.com/2015/02/25/bill-c-13-lawful-access-and-the-relationship-between-organizations, *archived at* https://perma.cc/8YH7-PEEJ.

[6] Steven Penney, *National Security Surveillance in an Age of Terror: Statutory Powers & Charter Limits*, 48 OSGOODE HALL L.J. 247, 284 (2010), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1994525, *archived at* https://perma.cc/KN8Q-X5LK (construing Criminal Code § 184.2).

[7] CRIMINAL CODE § 487.012(1).

[8] *Id.* § 487(1).

[9] *Id.* § 487.013(1).

[10] *Id.* § 487.016(1).

[11] *Id.* § 487.017(1).

[12] *Id.* § 487.014.

[13] Nicole Bogart, *Can Law Enforcement Legally Access Data on Your Smartphone in Canada?*, GLOBAL NEWS (Feb. 24, 2016), http://globalnews.ca/news/2537715/can-law-enforcement-legally-access-data-on-your-smartphone-in-canada, *archived at* https://perma.cc/4GDV-RJST. “Assistance orders” are provisioned under 487.02 of the Criminal Code, which stipulates that,

> [i]f an authorization is given under section 184.2, 184.3, 186 or 188 or a warrant is issued under this Act, the judge or justice who gives the authorization or issues the warrant may order a person to provide assistance, if the person’s assistance may reasonably be considered to be required to give effect to the authorization or warrant.

CRIMINAL CODE § 487.02.

Canada's existing legal framework for interception, search and seizure, preservation and production of data, appears to apply to encrypted data or communications.[14] However, there does not appear to be a specific provision in the Criminal Code that imposes requirements on telecommunications providers to decrypt or establishes backdoor access. According to a recent statement by the Royal Canadian Mounted Police (RCMP) quoted in an investigative report by *Motherboard*, "there is no specific power in the Criminal Code to compel a third party to decrypt or develop decryption tools, nor is there any requirement for telecommunications services to provide these services,"[15] but courts may "compel" third parties like BlackBerry to assist with investigations.[16]

In the same *Motherboard* report defense lawyer Michael Lacy is quoted as saying that the RCMP's statement "is 'an overstatement of the law,' and that even though there is no explicit power relating to encryption backdoors in the Criminal Code, there may still be legal means to order a company to assist the police with decryption."[17]

According to another news report, which quotes Christopher Parsons, a security researcher and postdoctoral fellow at the University of Toronto's Citizen Lab, "[w]e don't actually understand how the RCMP is using the laws that are developed for them."[18] One critic notes that the Canadian government has been successful "at keeping their abilities regarding encryption quiet."[19]

Canada's previous Conservative government introduced lawful access legislation, Bill C-30, which included specific sections that would have imposed decryption requirements on telecommunications service providers, but the Bill was not adopted. Section 6(3) & (4) of the Bill stipulated as follows:

> (3) If an intercepted communication is encoded, compressed, encrypted or otherwise treated by a telecommunications service provider, the service provider must use the

[14] In October 1998 the Government of Canada announced its policy on cryptography, which stipulated that the government would "apply existing interception, search and seizure and assistance procedures to cryptographic situations and circumstances." *See 6.0 Cryptography Policies*, MCCARTHY TETRAULT, http://www.mccarthy.ca/pubs/cicpaper06.htm (last visited Apr. 19, 2016), *archived at* https://perma.cc/YH7W-SRRM; *see also* Christopher Parsons & Tamir Israel, *Canada's Quiet History of Weakening Communications Encryption*, THE CITIZEN LAB (Aug. 11, 2015), https://citizenlab.org/2015/08/canadas-quiet-history-of-weakening-communications-encryption, *archived at* https://perma.cc/HMT9-B3HW.

[15] Jordan Pearson & Justin Ling, *Exclusive: How Canadian Police Intercept and Read Encrypted BlackBerry Messages*, MOTHERBOARD (Apr. 14, 2016), http://motherboard.vice.com/read/rcmp-blackberry-project-clemenza-global-encryption-key-canada, *archived at* https://perma.cc/JK2T-RDQG.

[16] *Id.*

[17] *Id.*

[18] Justin Ling & Jordan Pearson, *Exclusive: Canadian Police Obtained BlackBerry's Global Decryption Key*, VICE NEWS (Apr. 14, 2016), https://news.vice.com/article/exclusive-canada-police-obtained-blackberrys-global-decryption-key-how, *archived at* https://perma.cc/K9AT-E36K.

[19] Jordan Pearson, *Canada Desperately Needs to Have a Public Debate About Encryption,* MOTHERBOARD (Apr. 14, 2016), http://motherboard.vice.com/read/canada-desperately-needs-to-have-a-public-debate-about-encryption, *archived at* https://perma.cc/9TGC-FZR9.

> means in its control to provide the intercepted communication in the same form as it was before the communication was treated by the service provider.
>
> (4) Despite subsection (3), a telecommunications service provider is not required to make the form of an intercepted communication the same as it was before the communication was treated if
>
> > *(a)* the service provider would be required to develop or acquire decryption techniques or decryption tools; or
> >
> > *(b)* the treatment is intended only for the purposes of generating a digital signature or for certifying a communication by a prescribed certification authority, and has not been used for any other purpose.[20]

B. Solicitor General's Enforcement Standards

Since 1995, the Solicitor General's Enforcement Standards (SGES) have been in force. Those Standards outline twenty-three technical surveillance standards[21] identifying "how mobile telecommunications companies must configure their networks to facilitate telecommunications interceptions."[22] The Standards must be followed as a condition of obtaining a wireless spectrum license in Canada.[23]

Standard 12 stipulates that, "[i]f 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."[24] The annotation for this standard also provides

> [l]aw enforcement requires that any type of encryption algorithm that is initiated by the service provider must be provided to the law enforcement agency unencrypted. This would include proprietary compression algorithms that are employed in the network. This does not include end to end encryption that can be employed without the service provider's knowledge.[25]

[20] Bill C-30, An Act to Enact the Investigating and Preventing Criminal Electronic Communications Act and to Amend the Criminal Code and Other Acts (Protecting Children from Internet Predators Act), http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=5380965&File=59#10, *archived at* https://perma.cc/D3BL-WNPS.

[21] Parsons & Israel, *supra* note 14.

[22] TELECOM TRANSPARENCY PROJECT, THE GOVERNANCE OF TELECOMMUNICATIONS SURVEILLANCE: HOW OPAQUE AND UNACCOUNTABLE PRACTICES AND POLICIES THREATEN CANADIANS 10 (2015), https://www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf, *archived at* https://perma.cc/5339-EUYK.

[23] Mathew Braga, *Why Canada Isn't Having a Policy Debate Over Encryption*, THE GLOBE AND MAIL (Feb. 23, 2016), http://www.theglobeandmail.com/technology/why-canada-isnt-having-a-rigorous-debate-over-encryption/article28859991, *archived at* https://perma.cc/YA8W-CDCR.

[24] Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications, Standard 12, https://cippic.ca/uploads/Solicitor_General_Standards_Annotaed-2008.pdf, *archived at* https://perma.cc/NQB9-ZHPY.

[25] *Id.*

Only circuit-based communications are subject to these requirements[26] as opposed to packet-based communications.[27]

These standards were reportedly updated in 2008 and only made public by *The Globe & Mail*, which obtained past and current versions of the documents in 2013.[28] Some critics have pointed to a lack of transparency "surrounding the government's position and policies" with regard to encryption.[29]

C. Police–Telecommunications Provider Cooperation on Encryption

In 2012, Rogers, a Canadian telecommunications provider, and the French telecommunications equipment company Alcatel-Lucent proposed an encryption backdoor for law enforcement at a meeting of the 3rd Generation Partnership Project's (3GPP's) Lawful Interception Working Group.[30] The proposal was for "a next-generation voice encryption protocol, known as MIKEY-IBAKE."[31] The protocol was designed to protect end-to-end conversations.[32] According to Parsons and Tamir Israel of the Citizen Lab this proposal was a discussion on "how to weaken communications-related encryption protocols such as MIKEY-IBAKE."[33] The Telecom Transparency Project describes this process as follows:

> Rogers and Alcatel Lucent proposed that "[i]nstead of deploying the true random number generator to create the random secret" that is used to establish an end-to-end encrypted communication, "a pseudo-random number generator (PRG) is deployed in the client application of the user device." The Rogers/Alcatel Lucent solution would let a TSP either decrypt traffic in real time or retroactively decrypt traffic that had been encrypted using the PRG. As such, their proposal would effectively undermine the core security design decisions that were "baked" into MIKEY-IBAKE.[34]

According to an investigative report by *Motherboard*, Canadian police have been in possession of a BlackBerry master encryption key since 2010. The report states that the RCMP used the key in a criminal investigation into a mafia-related death that took place between 2010 and 2012 to intercept and decrypt over one million BlackBerry messages sent using its proprietary BBM

[26] TELECOM TRANSPARENCY PROJECT, *supra* note 22, at 10.

[27] Parsons & Israel, *supra* note 14.

[28] *Id.*

[29] *Id.*

[30] Matthew Braga, *Rogers and Alcatel-Lucent Proposed an Encryption Backdoor for Police*, MOTHERBOARD (Feb. 12, 2016), http://motherboard.vice.com/read/rogers-and-alcatel-lucent-proposed-an-encryption-backdoor-for-police, *archived* at https://perma.cc/4U75-7B5R.

[31] *Id.*

[32] *Id.*

[33] Parsons & Israel, *supra* note 14.

[34] TELECOM TRANSPARENCY PROJECT, *supra* note 22, at 10 (footnote in original omitted).

service. Based on court records in the case, it is unclear how the RCMP actually obtained the key, *Motherboard* said.[35]

III. Conclusion

In conclusion, although there is no specific provision or power in Canada's Criminal Code to compel a third-party telecommunications provider to decrypt or create decryption tools, Canada's existing lawful access provisions in the Code may provide a legal framework for ordering companies to assist the police with decryption.

[35] Pearson & Ling, *supra* note 15.

European Union

Theresa Papademetriou
Senior Foreign Law Specialist

SUMMARY At the European Union (EU) level, there is no requirement that keys to encrypted materials be disclosed to law enforcement authorities, or that companies decrypt communications in response to a government request. A 2001 nonbinding resolution merely calls upon the Member States in cooperation with telecommunications companies to take into consideration the operational needs of law enforcement authorities when data are encrypted. Electronic surveillance is regulated at the EU Member State level.

The EU agencies dealing with security, terrorism, cybercrime, and organized crime have not reached consensus on access to encryption by law enforcement authorities. The EU's cybersecurity agency, the European Union Agency for Network and Information (ENISA), is against creating backdoors in encryption products, whereas the EU Counter-Terrorism Coordinator believes the Commission should contemplate introducing legislation on this matter. In a similar vein, the EU's law enforcement agency, Europol, favors enacting legislation on disclosure as the only practical solution for handling encryption when the keys are held by individual users.

I. Introduction

The European Union (EU) and its Member States share competence in enacting legislation to combat serious crime, including terrorism and organized crime, and to reinforce cooperation between police and judicial authorities to protect people in the EU, while at the same time ensuring compliance with EU rules on personal data protection and privacy.[1] Electronic surveillance conducted by national law enforcement authorities to detect and investigate crimes and the parallel cooperation of telecommunications and Internet service providers to allow access is an issue that is regulated at the Member State level.[2] The Paris and Brussels terrorist attacks reignited the debate across Europe over whether to expand monitoring by law enforcement authorities in light of concerns about potential violations of the privacy and personal data of individuals. A number of Member States have shown a keen interest in granting their law enforcement authorities greater access to personal data.[3]

[1] Consolidated Version of the Treaty on European Union art. 3, para. 2, 2012 OFFICIAL JOURNAL OF THE EUROPEAN UNION [O.J.] (C 326) 13, updated version *available at* http://data.consilium.europa.eu/doc/document/ST-6655-2008-REV-8/en/pdf, *archived at* https://perma.cc/7Z7R-5RQ4.

[2] Consolidated Version of the Treaty on the Functioning of the European Union art. 4, para. 2(J), 2012 O.J. (C 326) 47, updated version *available at* http://data.consilium.europa.eu/doc/document/ST-6655-2008-REV-8/en/pdf, *archived at* https://perma.cc/7Z7R-5RQ4.

[3] Patrick Howell O'Neill, *Dutch Government Backs Strong Encryption, Condemns Backdoors*, THE DAILY DOT (Jan. 4, 2016), http://www.dailydot.com/politics/dutch-encryption-cabinet-backdoor, *archived at* https://perma.cc/CTR7-C7GK; Thorsten Benner & Mirko Hohmann, *How Europe Can Get Encryption Right*, POLITICO (Apr. 13, 2016), http://www.politico.eu/article/how-europe-can-get-encryption-right-data-protection-privacy-counter-terrorism-technology, *archived at* https://perma.cc/9N7W-786H; *see also* Paul Hockenos, *Europe Considers Surveillance*

II. Legal Framework

At the EU level, two measures deal with access to personal data by law enforcement authorities: a 2001 nonbinding Resolution[4] establishing guidelines concerning cooperation between law enforcement authorities and the telecommunications industry, and the Authorization Directive (2002/20/EC), which, *inter alia*, makes lawful interception by law enforcement authorities a condition for granting electronic networks and services the authority to operate.[5]

The 2001 Resolution on Law Enforcement Operational Needs with Respect to Public Telecommunication Networks and Services,[6] similarly to its predecessor Resolution adopted in 1995 on the Lawful Interception of Telecommunications,[7] contains in the Annex a detailed list of the operational needs of law enforcement authorities.[8] The Resolution calls upon the EU Member States to cooperate with communications service providers and to take into account law enforcement operational needs in the development and implementation of any measures concerning legally authorized forms of interception of telecommunications.[9] It is up to the discretion of the Member States to adopt legislation requiring telecommunications industries to decrypt materials.

The Resolution, which contains language specific to encrypted materials, calls on the Member States to provide that,

> [i]f 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 [in a readable format].[10]

Expansion After Deadly Attacks, THE INTERCEPT (Jan. 20, 2015), https://theintercept.com/2015/01/20/europe-considers-surveillance-expansion, *archived at* https://perma.cc/6VHP-WLGP.

[4] Resolutions adopted by EU institutions are non-binding and are published in the "C" series of the *Official Journal* (O.J.) of the EU rather than in the "L" series of the O.J. where all legislation is published. *Legislation*, EUR-LEX, http://eur-lex.europa.eu/collection/eu-law/legislation/recent.html (last visited Apr. 21, 2016), *archived at* https://perma.cc/P2FA-NXZW.

[5] Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the Authorization of Electronic Communications and Services (Authorization Directive), 2002 O.J. (L 108) 21, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0021:0032:EN:PDF, *archived at* https://perma.cc/V49P-2RDA.

[6] Council of the European Union, Council Resolution on Law Enforcement Operational Needs with Respect to Public Telecommunication Networks and Services, June 20, 2001, *available at* http://www.statewatch.org/news/2001/sep/9194.pdf, *archived at* https://perma.cc/66XC-ZP3R. This Council Resolution was not published in the *Official Journal*.

[7] Council Resolution of 17 January 1995 on the Lawful Interception of Telecommunications, 1996 O.J. (C 329) 1, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996G1104:EN:HTML, *archived at* https://perma.cc/QRY9-VXAU.

[8] Council Resolution, *supra* note 6.

[9] *Id.*, Annex.

[10] *Id.*, Annex, para. 3.3.

Directive 2002/20/EC contains a number of conditions that may be attached to the general authorization for providing electronic communications networks or services,[11] among them the "[e]nabling of legal interception by competent national authorities in conformity with Directive 97/66/EC and Directive 95/46/EC . . . on the protection of individuals with regard to the processing of personal data and on the free movement of such data."[12]

III. Encryption

Currently, the EU does not require that keys to encrypted material be disclosed to law enforcement authorities or require companies to decrypt encrypted communications on request of a government, nor have its critical agencies on cybersecurity, organized crime, and terrorism reached a clear and uniform position on this issue.

A. Europol

The 2015 Internet Organised Crime Threat Assessment (IOCTA) prepared by Europol, the EU's law enforcement agency, estimates that more than three-quarters of cybercrime investigations in the EU confront the use of some form of encryption to protect data and avoid interception. Both TrueCrypt and BitLocker are commonly and increasingly encountered, despite the cessation of TrueCrypt's development in May 2014. Almost half of all Member States also noted an increased use of encrypted email, typically through PGP (Pretty Good Privacy) software.[13]

The IOCTA explored various options in its debate on encryption, such as using "key escrow" systems, using weakened encryption, or introducing legislation on the mandatory disclosure of encryption keys. It concluded that legislation was the only practical solution for handling encryption, especially in instances where the keys are held by individual users.[14]

In addition, the IOCTA made the following two specific recommendations:

- Law enforcement would benefit from a central database of VPN [Virtual Private Network] and proxy services used by cybercriminals to determine if any are suitable for either information exchange with law enforcement or intervention if criminal in nature.
- Legislators and policy makers, including industry representatives and academia, must implement a workable solution to the issue of encryption which allows legitimate users to protect their privacy and property without severely compromising government and law enforcement's ability to investigate criminal or national security threats.[15]

[11] Directive 2002/20/EC, *supra* note 5, art. 6, para. 1.

[12] *Id.*, Annex(A), para. 11.

[13] Europol, *The Internet Organised Crime Threat Assessment (IOCTA) 2015*, at 50, *available at* http://statewatch.org/news/2015/oct/eu-europol-iocta-2015.pdf, *archived at* https://perma.cc/CPA4-58W3.

[14] *Id.* at 69.

[15] *Id.* at 51.

Regarding the enactment of "obligation to disclose" laws, which would oblige individuals to disclose their encryption keys or be subject to a criminal penalty, the IOCTA noted that "this tends to be effective only when data remains on the suspect/criminal's computer. If the keys are transient, especially if they are system generated, it can be practically impossible to recover these."[16]

Finally, the Director of Europol, Rob Wainwright, declared that encrypted communications are the biggest obstacle to monitoring terrorists' actions, adding that "there is a significant capability gap that has to change if we're serious about ensuring the internet isn't abused and effectively enhancing the terrorist threat."[17]

B. EU Cybersecurity Agency

On March 26, 2016, the EU's cybersecurity agency, the European Union Agency for Network and Information (ENISA), declared that it is against forcing Internet and telecommunications companies to create backdoors for authorities to unlock encrypted messages. ENISA's director, Udo Helmbrecht, pointed out that the EU has sufficient legislation on information sharing among the national intelligence agencies of the Member States, and emphasized that available information is not used sufficiently and effectively.[18]

C. EU Counter-Terrorism Coordinator

The EU Counter-Terrorism Coordinator, Gilles de Kerchoven, in a 2015 document addressed to EU Justice and Home Affairs Ministers, expressed the view that the European Commission "should be invited to explore rules obliging internet and telecommunications companies operating in the EU to provide . . . access of the relevant national authorities to communications (i.e. share encryption keys)."[19]

D. EU Internet Forum

In 2015, the Commission announced in its Communication on Security Agenda the creation of an IT forum where Europe's major IT companies would be invited to discuss a number of concerns, including "deploying the best tools to counter terrorist propaganda on the internet and in social networks" and "the concerns of law enforcement authorities on new encryption

[16] *Id.* at 69.

[17] *Europol Chief Warns on Computer Encryption*, BBC (Mar. 29, 2015), http://www.bbc.com/news/technology-32087919, *archived at* https://perma.cc/Q9FQ-JL55.

[18] Catherine Stupp, *EU Cybersecurity Agency Slams Calls for Encryption Backdoors*, EURACTIV (Mar. 30, 2016), http://www.euractiv.com/section/digital/news/eu-cybersecurity-agency-slams-calls-for-encryption-backdoors, *archived at* https://perma.cc/K9U3-NRFW.

[19] Council of the European Union, General Secretariat, EU CTC Input for the Preparation of the Informal Meeting of Justice and Home Affairs Ministers in Riga on 29 January 2015, DS1035/15 (Jan. 17, 2015), *available at* http://www.statewatch.org/news/2015/jan/eu-council-ct-ds-1035-15.pdf, *archived at* https://perma.cc/XA4T-CF2B.

technologies."[20] The EU Internet Forum was established on December 3, 2015, through the joint efforts of Dimitris Avramopoulos, the EU Commissioner for Migration, Home Affairs and Citizenship, and Věra Jourová, the Commissioner for Justice, Consumer and Gender Equality.[21]

IV. Conclusion

Currently, there is no EU legislation that requires tech companies to disclose the keys to encrypted materials to law enforcement authorities, or to decrypt communications upon the request of a government.

[20] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: The European Agenda on Security*, at 13–14, COM (2015) 185 final (Apr. 28, 2015), http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf, *archived at* https://perma.cc/9NXB-SHLK.

[21] European Commission Press Release IP/15/6243, EU Internet Forum: Bringing Together Governments, Europol and Technology Companies to Counter Terrorist Content and Hate Speech Online (Dec. 3, 2015), http://europa.eu/rapid/press-release_IP-15-6243_el.htm, *archived at* https://perma.cc/H225-L5CQ.

France

Nicolas Boring
Foreign Law Specialist

I. Decryption at the Request of Intelligence and Security Services

French law authorizes national intelligence and security services to intercept and read private communications for specifically enumerated purposes, including protecting national security, protecting the "safety of essential elements of France's economic and scientific potential," preventing acts of terrorism, repressing organized crime, or preventing the reconstitution of illegal groups (such as banned hate groups or private paramilitary groups).[1]

Such interceptions must be authorized in writing by the Prime Minister or someone specifically and directly chosen by him/her for that purpose, upon the written request of the Defense Minister, the Minister of the Interior, or the minister in charge of customs and border security.[2]

Agents duly authorized to intercept electronic communications for intelligence purposes may request from providers of cryptology services the means to decipher their codes.[3] This refers not just to encryption keys, but also to any software or other information that would allow the encrypted data to be read.[4] A cryptology service provider must submit to the request within seventy-two hours.[5] Furthermore, a cryptology service provider may be required to apply the means of decryption him/herself within that same timeframe, unless he/she can demonstrate an inability to do so.[6]

[1] CODE DE LA SECURITE INTERIEURE [INTERIOR SECURITY CODE] art. L811-3, https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000025503132&idArticle=LEGIARTI000030935040&dateTexte=&categorieLien=cid, *archived at* https://perma.cc/Z32U-CVJA & art. L852-1, https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000030935848&cidTexte=LEGITEXT000025503132&dateTexte=20160322&fastPos=1&fastReqId=19915746&oldAction=rechCodeArticle, *archived at* https://perma.cc/28FX-F4S4.

[2] *Id.* art. L821-4, https://www.legifrance.gouv.fr/affichCode.do?idSectionTA=LEGISCTA000030935046&cidTexte=LEGITEXT000025503132&dateTexte=20160321, *archived at* https://perma.cc/ V74K-J3AQ.

[3] *Id.* art. L871-1, https://www.legifrance.gouv.fr/affichCode.do?idSectionTA=LEGISCTA000030937374&cidTexte=LEGITEXT000025503132&dateTexte=20160321, *archived at* https://perma.cc/9DPZ-JSK8.

[4] *Id.* art. R871-3, https://www.legifrance.gouv.fr/affichCode.do;jsessionid=64075B6429EC9ED93CFF00D70F55E60E.tpdila14v_1?idSectionTA=LEGISCTA000031944913&cidTexte=LEGITEXT000025503132&dateTexte=20160322, *archived at* https://perma.cc/S6XJ-NS7D.

[5] *Id.* art. L871-1.

[6] *Id.*

II. Decryption at the Request of Judicial and Law Enforcement Agencies

If certain conditions are met, an investigative judge (*juge d'instruction*) may order the interception, recording, and transcription of private telecommunications for the purposes of a criminal investigation.[7] In certain circumstances, telecommunications interception, recording, and transcription may also be ordered by a *juge des libertés et de la detention* (a judge who specializes in determining whether a suspect should be placed in police custody).[8]

When intercepted information is password protected or encrypted, law enforcement authorities may ask any qualified person or corporation to perform the technical operations that would allow access to this information.[9] This requires authorization from the investigative judge, the public prosecutor (*procureur de la République*), or the court that has jurisdiction over the crime being investigated.[10] The Code of Criminal Procedure also provides that law enforcement authorities can request the help of a "Technical Support Center," which was created in 2002 under the authority of the Ministry of the Interior (the ministry in charge of law enforcement in France).[11] Details on this "Technical Support Center" are classified,[12] but it appears to specialize in data decryption.[13]

[7] CODE DE PROCÉDURE PÉNALE [CODE OF CRIMINAL PROCEDURE] art. 100, https://www.legifrance.gouv.fr/affichCode.do;jsessionid=42F5EDFF9D0C401F5371916B7A9BDE31.tpdila14v_1?idSectionTA=LEGISCTA000006182887&cidTexte=LEGITEXT000006071154&dateTexte=20160322, *archived at* https://perma.cc/YG4V-8FJT.

[8] *Id.* art. 706-95, https://www.legifrance.gouv.fr/affichCode.do;jsessionid=42F5EDFF9D0C401F5371916B7A9BDE31.tpdila14v_1?idSectionTA=LEGISCTA000006167523&cidTexte=LEGITEXT000006071154&dateTexte=20160322, *archived at* https://perma.cc/V8ZJ-QK5M.

[9] *Id.* art. 230-1, https://www.legifrance.gouv.fr/affichCode.do;jsessionid=42F5EDFF9D0C401F5371916B7A9BDE31.tpdila14v_1?idSectionTA=LEGISCTA000023712010&cidTexte=LEGITEXT000006071154&dateTexte=20160322, *archived at* https://perma.cc/6UWV-3BZJ.

[10] *Id.*

[11] Décret n°2002-1073 du 7 août 2002 d'application de l'article 30 de la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne et portant création du centre technique d'assistance [Decree No. 2002-1073 of August 7, 2002, Applying Article 30 of Law No. 2001-1062 of November 2001 Regarding Everyday Security and Creating the Technical Support Center] (as amended on May 9, 2014), http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=D3D3BF1F4D47E24B7C9D0FB4B55005AC.tpdjo06v_2?cidTexte=LEGITEXT000005633260&dateTexte=20150127, *archived at* https://perma.cc/H8C6-RNNP.

[12] *Id.*

[13] *Circulaire relative au fonctionnement du centre technique d'assistance (C.T.A.)* [*Circular Regarding the Functioning of the Technical Support Center (C.T.A.)*], MINISTÈRE DE L'INTÉRIEUR, DE LA SÉCURITÉ INTÉRIEURE ET DES LIBERTÉS LOCALES [MINISTRY OF THE INTERIOR, OF INTERIOR SECURITY, AND OF LOCAL FREEDOMS] (Mar. 27, 2003), http://www.interieur.gouv.fr/content/download/8005/75906/file/INTC0300032C.pdf, *archived at* https://perma.cc/E4Z8-65NX.

Germany

Jenny Gesley
Foreign Law Specialist

I. Interception of Communications Data

Article 10 of the German Basic law provides that the privacy of correspondence, mail, and telecommunications is inviolable. Restrictions may only be imposed pursuant to law. If the restriction serves to protect the free, democratic basic order or the existence or security of the German Federation or of a German state, the law may provide that the affected person will not be informed of the measure.[1]

Several German intelligence and law enforcement agencies have been authorized to access, intercept, and request stored communications data. This authority and its limits are delineated in article 10 of the Basic Law as explained above and in specific acts. For the Federal Intelligence Agencies, the specific authorizations are contained in the Act on the Federal Office for the Protection of the Constitution;[2] the Act on the Federal Intelligence Service;[3] the Act on the Military Counterintelligence Service;[4] and the Act to Restrict the Privacy of Correspondence, Mail, and Telecommunications (Article 10 Act).[5]

Furthermore, restrictions on the privacy of mail and telecommunications undertaken by Federal Intelligence Agencies are monitored by the Article 10 Commission of the German Parliament.[6]

The authorizations for the federal law enforcement agencies are contained in the Act on the Federal Criminal Police Office,[7] the Act on the Federal Police,[8] the Act on the Customs

[1] GRUNDGESETZ FÜR DIE BUNDESREPUBLIK DEUTSCHLAND [GRUNDGESETZ] [GG] [BASIC LAW], May 23, 1949, BUNDESGESETZBLATT [BGBL.] [FEDERAL LAW GAZETTE] I at 1, unofficial English translation *at* http://www.gesetze-im-internet.de/englisch_gg/basic_law_for_the_federal_republic_of_germany.pdf, *archived at* http://perma.cc/MER4-79JH.

[2] Bundesverfassungsschutzgesetz [BVerfSchG], Dec. 20, 1990, BGBL. I at 2954, 2970, as amended, §§ 8a, 8d, http://www.gesetze-im-internet.de/bundesrecht/bverfschg/gesamt.pdf, *archived at* http://perma.cc/C858-Y6VY.

[3] Bundesnachrichtendienstgesetz (BNDG), Dec. 20, 1990, BGBL. I at 2954, 2979, as amended, §§ 2a, 2b, http://www.gesetze-im-internet.de/bundesrecht/bndg/gesamt.pdf, *archived at* http://perma.cc/7DTM-H656.

[4] Gesetz über den militärischen Abschirmdienst [MADG], Dec. 20, 1990, BGBL. I at 2954, 2977, as amended, §§ 4a, 4b, http://www.gesetze-im-internet.de/bundesrecht/madg/gesamt.pdf, *archived at* http://perma.cc /99CA-LB6W.

[5] Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses [Artikel 10-Gesetz] [G 10], June 26, 2001, BGBL. I at 1254, 2298, as amended, § 1, para. 1, http://www.gesetze-im-internet.de/bundesrecht/g10_2001/gesamt.pdf, *archived at* http:// perma.cc/6YVZ-UCCU.

[6] Article 10 Act § 1, para. 2, § 15.

[7] Bundeskriminalamtgesetz [BKAG], July 7, 1997, BGBL. I at 1650, as amended, § 7, paras. 3, 4; § 20b, paras. 3, 4; § 20l; § 20m; § 20m; § 22, http://www.gesetze-im-internet.de/bundesrecht/bkag_1997/gesamt.pdf, *archived at* http://perma.cc/XJ9R-4HUX.

Investigation Bureau and the Customs Investigation Offices,[9] and the Code of Criminal Procedure.[10]

II. Transmission of Communications

The German Federal Constitutional Court has held that the transmission of subscriber data by telecommunications providers to a requesting agency is only permissible if there is a legal norm authorizing the agency to request the data and an additional legal norm obligating the telecommunications provider to transfer the data ("double door model").[11] Telecommunications providers are defined as anyone who exclusively or occasionally provides telecommunications services or who contributes to the provision of such services.[12]

Anyone who operates a telecommunications network that provides publicly available telecommunications services to more than 10,000 participants is obligated to install a surveillance system that complies with the technical requirements set out in the Telecommunications Surveillance Directive and the technical guideline adopted by the German Federal Network Agency.[13] Telecommunications providers must ensure that they are at all times capable of being informed by telephone of incoming requests and their urgency, and that they are able to accept and process such requests during regular business hours.[14]

[8] Bundespolizeigesetz [BpolG], Oct. 19, 1994, BGBl. I at 2978, 2979, as amended, http://www.gesetze-im-internet.de/bundesrecht/bpolbg/gesamt.pdf, *archived at* http://perma.cc/LEU5-HE59.

[9] Gesetz über das Zollkriminalamt und die Zollfahndungsämter [ZFdG], Aug. 16, 2002, BGBl. I at 3202, as amended, § 7, paras. 5-9; § 15, paras. 2–6; §§ 23a–23g, http://www.gesetze-im-internet.de/bundesrecht/zfdg/gesamt.pdf, *archived at* http://perma.cc/T7J8-T9TV.

[10] Strafprozessordnung [StPO], Apr. 7, 1987, BGBl. I at 1074, 1319, as amended, §§ 100a, 100b, 100g, 100i, 100j, http://www.gesetze-im-internet.de/bundesrecht/stpo/gesamt.pdf, *archived at* http://perma.cc/ZA7K-47GY, unofficial English translation *at* http://www.gesetze-im-internet.de/englisch_stpo/german_code_of_criminal_procedure.pdf, *archived at* http://perma.cc/A6MH-9KXA (English translation only current up to 2014).

[11] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court], 100 Entscheidungen des Bundesverfassungsgerichts [BVerfGE] [Decisions of the Federal Constitutional Court] 313, 366 *et seq.*, http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1999/07/rs19990714_1bvr222694en.html, *archived at* http://perma.cc/QBZ9-3B9A. If the agency is authorized by law to request communications data, the Telecommunications Act requires telecommunications providers to immediately comply with such a request. Telekommunikationsgesetz [TKG] [Telecommunications Act], June 22, 2004, BGBl. I at 1190, as amended, §§ 110–115, http://www.gesetze-im-internet.de/bundesrecht/tkg_2004/gesamt.pdf, *archived at* http://perma.cc/WP2Y-XH69.

[12] Telecommunications Act § 3, no. 6.

[13] Telekommunikations-Überwachungsverordnung [TKÜV] [Telecommunications Surveillance Directive], Nov. 3, 2005, BGBl. I at 3136, as amended, §§ 3, 5, para. 1, http://www.gesetze-im-internet.de/bundesrecht/tk_v_2005/gesamt.pdf, *archived at* http://perma.cc/4MFL-9LW8; Technical Guideline for the Implementation of Legal Measures for the Surveillance of Telecommunications and the Disclosure of Information, Oct. 15, 2015, http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/TechnUmsetzung110/Downloads/TRTK%C3%9CV%20englische%20Version.pdf?__blob=publicationFile&v=7, *archived at* http://perma.cc/F382-S4TE.

[14] Telecommunications Surveillance Directive § 12.

Once a request from an authorized agency is received, a surveillance copy of the communications must be compiled and transmitted without undue delay.[15] It must include informational content and event data.[16] The communications are transmitted in the form in which they were received by the telecommunications provider.[17] If the telecommunications providers do not comply with a lawful transmission request, the Federal Network Agency may impose fines of up to €500,000 (around US$561,100) to force compliance, or partially or completely shut down the operations of the providers.[18]

III. Encryption of Communications

The aforementioned laws, which allow the access, interception, and transmission of communications, make no distinction between encrypted and unencrypted communications. If the communications have been encrypted by the user, federal intelligence agencies and law enforcement agencies are allowed to use whatever technologies they have at their disposal to unlock lawfully intercepted and transmitted encrypted communications. If they discover an encryption or network key during the course of the interception or surveillance of communications or during the course of a lawful search, they may use it to unlock the encrypted communications.[19]

However, there is no legal basis that would compel the user to turn over an encryption or network key, in particular with regard to the *nemo tenetur* principle. The *nemo tenetur* principle, derived from the general right of personality found in the German Basic Law and from section 136, para. 1, sentence 1 of the German Code of Criminal Procedure, states that a suspect may not be compelled to cooperate in an investigation that would incriminate him/herself.

If the communications were encrypted by the telecommunications providers (network encryption), the encryption must be removed at the point of transmission to the requesting agency.[20] Furthermore, if the telecommunications providers support encryption of peer-to-peer communications over the Internet by means of key management provided by them without involving their network elements or those of their partners in the transmission of the content, the providers must make the initial key available to the requesting agency. The telecommunications providers do not need to transmit the exchanged key if they can remove the encryption themselves by means of additional network elements.[21]

[15] *Id.* § 6, para. 1.

[16] *Id.* § 5, para. 1.

[17] *Id.* § 8, para. 2, no. 3.

[18] Telecommunications Act § 115.

[19] Code of Criminal Procedure § 95.

[20] Telecommunications Surveillance Directive § 8, para. 3.

[21] Technical Guideline, Part A, Annex D.1, para. 7.5.1; Part A, Annex H.3.2, para. 5.5; Part A, Annex H.3.3, para. 4.4; Part A, Annex H.3.4, para. 6.2.

IV. European Developments

In an April 2015 communication titled "European Agenda on Security," the EU Commission proposed, among other ideas, to create an EU Forum with IT companies to help counter terrorist propaganda and address the concerns of law enforcement agencies about new encryption technologies.[22] The EU Forum was officially launched in December 2015.[23]

Furthermore, in July 2015, Europol launched the European Union Internet Referral Unit (EU IRU). The goal of the EU IRU is "to combat terrorist propaganda and related violent extremist activities on the internet."[24] Europol Director Rob Wainwright has expressed concerns that encrypted communications pose problems for law enforcement when dealing with terrorism threats.[25] The German government stated that it supports the efforts and goals of the EU IRU, but that it was not aware of specific plans that were discussed with technology firms regarding encryption mechanisms.[26]

[22] *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, the European Agenda on Security*, at 16, COM (2015) 185 final (Apr. 28, 2015), http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf, *archived at* http://perma.cc/Z8AR-ALEE.

[23] European Commission Press Release IP/15/6243, EU Internet Forum: Bringing Together Governments, Europol and Technology Companies to Counter Terrorist Content and Hate Speech Online (Dec. 3, 2015), http://europa.eu/rapid/press-release_IP-15-6243_en.htm, *archived at* http://perma.cc/PYG3-3DMD.

[24] Europol Press Release, Europol's Internet Referral Unit to Combat Terrorist and Violent Extremist Propaganda (July 1, 2015), https://www.europol.europa. eu/content/europol%E2%80%99s-internet-referral-unit-combat-terrorist-and-violent-extremist-propaganda, *archived at* http://perma.cc/6VA4-5RK2.

[25] Warwick Ashford, *EU Launches Internet Referral Unit to Combat Online Extremism*, COMPUTERWEEKLY.COM (July 1, 2015), http://www. computerweekly.com/news/4500249133/EU-launches-Internet-Referral-Unit-to-combat-online-extremism, *archived at* http://perma.cc/DYN5-UVG2.

[26] DEUTSCHER BUNDESTAG: DRUCKSACHEN UND PROTOKOLLE [BT-DRS.] 18/5144, p. 6, questions 16, 17, http://dip21.bundestag.de/dip21/btd/18/051/1805144.pdf, *archived at* http://perma.cc/YVE2-8DBW.

Israel

Ruth Levush
Senior Foreign Law Specialist

SUMMARY Israel's Secret Monitoring Law, 5739-1979, generally protects privacy rights in Israel by prohibiting the monitoring of conversations, but also carves out certain exceptions to the prohibition in order to protect national and public security. Access to communications data, including traffic data and information regarding the location and identity of a subscriber, may also be authorized for saving or protecting human life, investigating or preventing offenses, identifying and indicting offenders, and lawfully confiscating property. In addition, warrantless orders for access to communications data may be issued under emergency situations to prevent the perpetration of a serious offense, identify the perpetrator, or save human life. Warrantless orders can also be issued for national security purposes under limited circumstances and for a limited duration.

The Order Governing the Control of Commodities and Services (Engagement in Encryption Items) 5735-1974, as amended, prohibits any person from engaging in encryption in the absence of a license issued by the Ministry of Defense and in violation of the conditions enumerated in the license. The Order identifies three types of licenses and exempts certain encryption activities from the licensing requirements.

I. Secret Monitoring

Israel's Secret Monitoring Law, 5739-1979, provides that "listening to the conversation of another" by means of an instrument in order to prevent and detect crimes generally requires a warrant issued by the president of a district court or his designee.[1] However, listening to conversations conducted in the public domain to protect state security and to prevent and detect crimes is exempt from this requirement.[2] Monitoring international conversations for military censorship and monitoring conversations that utilize communications systems used by the Israel Defense Forces (IDF), the Israeli Police, employees of the Ministry of Communication, and licensed service providers are similarly exempt. Wireless communications for the frequency ranges that are used by amateur radio operators and for broadcasting to the public also do not require permission under the law.[3]

The Law also authorizes the Prime Minister or the Minister of Defense, upon a written request by the IDF Intelligence Division or the General Security Service (GSS), to authorize secret monitoring after considering the extent of harm to privacy and determining that the monitoring is

[1] Secret Monitoring Law, 5739-1979, §§ 1, 6, SEFER HAHUKIM [BOOK OF LAWS] [SH] (official gazette) No. 938 p. 118, *as amended*, up-to-date text available in the Nevo Legal Database, *at* http://www.nevo.co.il (in Hebrew; by subscription), *archived at* https://perma.cc/EPD4-BV6R.

[2] *Id.* § 8(1).

[3] *Id.* § 8(2)–(5).

necessary for state security.[4] Granting or extending authorization for secret monitoring for state security reasons is subject to a three-month limit, which can be periodically extended.[5] In emergency situations and subject to conditions enumerated in the Law, the head of the Israel Security Agency (ISA) or the IDF Intelligence Division are also authorized to issue permits for monitoring conversations.[6]

Under the Communications (Communications and Broadcasts) Law, 5742-1982, the Prime Minister may issue instructions to a licensed communications service provider (licensee) to provide or facilitate government surveillance in response to a request by the Minister of Defense, the Minister of Domestic Security, the GSS, or the Institute for Intelligence and Special Operations (the Mossad), on the basis of state or public security considerations, and after consultation with the Minister of Communications.[7]

II. Interception of Communications Data

Access to communications data, including information regarding traffic data and the location and identity of a subscriber, may also be authorized by a warrant issued by a circuit court upon the request of an officer designated for this purpose by the General Police Commissioner or by a representative of another investigative authority defined by law.[8] The court will issue a warrant if it determines that access is required for saving or protecting human life, investigating or preventing offenses, identifying and indicting offenders, or lawfully confiscating property.[9]

Warrantless orders for access to communications data may also be issued by an authorized law enforcement officer for a limited duration when the officer is convinced that there is an imminent need to receive communications data without delay to prevent the perpetration of a serious offense, identify the perpetrator, or save human life.[10]

The GSS Law, 5762-2002, authorizes the Prime Minister to issue rules categorizing data (excluding the content of conversations) that must be made accessible to the ISA by communications licensees for national security purposes.[11] Orders for data transmission issued by the head of the ISA in accordance with these rules must specify the type and purpose of the data and the particulars of the database in which it is stored. Such orders are effective for a limited period of up to six months and may be renewed.[12]

[4] *Id.* § 4.

[5] *Id.*

[6] *Id.* § 5.

[7] Communications (Telecommunications and Broadcasting) Law, 5782-1982, § 13, SH No. 1060 p. 216, *as amended*, *available at* http://www.nevo.co.il, *archived at* https://perma.cc/D5CC-UB5B.

[8] Criminal Procedure (Enforcement Authorities–Communications Data) Law, 5768-2007, § 3, SH No. 2122 p. 72, *available at* http://www.nevo.co.il, *archived* at https://perma.cc/Q4MZ-FPYB.

[9] *Id.* § 3(a).

[10] *Id.* § 4.

[11] General Security Service Law, 5762-2002, § 11(b), SH No. 1832 p. 179, *as amended.*

[12] *Id.* § 11(c).

III. Regulation of Encryption

Encryption is regulated by the Order Governing the Control of Commodities and Services (Engagement in Encryption Items) 5735-1974, as amended (the Encryption Order).[13] On the basis of a 1998 amendment to the Encryption Order, the control and licensing of encryption items were transferred "from a military to a civilian licensing authority—i.e., from the IDF to the Ministry of Defense."[14]

The Encryption Order prohibits any person from engaging in encryption in the absence of a license issued by the General Manager of the Ministry of Defense and in violation of the conditions enumerated in the license.[15]

The General Manager of the Ministry of Defense is authorized to enter any place where an encryption related activity is being conducted and request a licensee to provide information at any time before and after the issuance of an encryption license.[16]

The Order provides for three categories of licenses for engaging in encryption:

> A "Restricted License" – a license that imposes restrictions on engagement in encryption items. These restrictions may also apply to permissible forms of engagement in encryption items, or to the nature of permissible sales (e.g. restriction on selling to certain countries and sectors). As a rule, a restricted license is valid for one year.
>
> A "Special License" – is a license for specific engagement; generally involving sale to clients who do not fall under the restrictions imposed on an applicant for a Restricted License. As a rule, a special license is valid for one year.
>
> A "General License" – a license for a particular encryption item which allows the license-holder free use of that item (other than modifications or integration that essentially create a new item for which a separate license is required). The sale of such items of encryption is decontrolled and not subject to reporting procedures. Such general licenses are issued with no time limit to their validity.[17]

[13] Order Governing the Control of Commodities and Services (Engagement in Encryption Items) (Encryption Order), 5735-1974, KOVETZ HATAKANOT 5735 No. 3232 p. 45, *available at* http://www.nevo.co.il, *archived at* https://perma.cc/9KKF-PVJY.

[14] *Encryption Controls in Israel*, MINISTRY OF DEFENSE, http://www.mod.gov.il/English/Encryption_Controls/Pages/default.aspx (last visited Apr. 18, 2016), *archived at* https://perma.cc/X4HB-BEW2.

[15] Encryption Order § 2.

[16] *Id.* §§ 4 & 6.

[17] MINISTRY OF DEFENSE, *supra* note 14.

The Order also provides for a category of "Free Means," which exempts certain encryption activities from licensing requirements. "Free Means" is defined as

> a means of encryption for which a general license has been granted or which the Director-General has declared to be decontrolled. Once an encryption item is defined as a free means, it is free of the licensing restrictions. A periodically revised list of encryption items which have been declared "decontrolled" is published in the Official Gazette of the Government of Israel as well as on [the Ministry of Defense] website.[18]

[18] *Id.*

Japan

Sayuri Umeda
Foreign Law Specialist

Law enforcement officials in Japan may request the courts to order the decryption of encrypted information during criminal investigations. Courts during trials may also order the decryption of encrypted information.

The Criminal Procedure Code states that where an article to be seized is a recording medium pertaining to electronic records, the person executing the search or seizure order may ask the subject of the order to operate the computer or provide "some other form of cooperation,"[1] which includes decryption of encrypted electronic records.[2] However, the subject is not penalized for refusing to provide such cooperation.[3]

A court may order the custodian of the electronic records or a person with authority to use the electronic records to record the necessary records onto the recording medium or print them out, and order the recording medium seized.[4] Commentators explain that the term "to record" includes "de-encrypt[ing] encrypted electronic records and record[ing]" the necessary electronic records onto the recording medium.[5] However, refusing to make such a recording is not penalized.[6]

Law enforcement officials may request telecommunications carriers to cooperate in implementing the interception of communications pursuant to a court order.[7] Telecommunications carriers that encrypt communications may be asked by law enforcement officials to decrypt the communications.[8] Carriers are obligated to cooperate with law enforcement officials but are not penalized for refusing to do so. Carriers are not required to develop systems or software to decrypt communications because doing so is beyond the scope of the Code's requirement for carriers to cooperate in implementing the interception of

[1] CODE OF CRIMINAL PROCEDURE, Act No. 131 of July 10, 1948, amended by Act No. 74 of 2011, arts. 111-2 & 222, English translation available on the Japanese Law Translation website, *at* http://www.japaneselawtranslation.go.jp/law/detail/?printID=&ft=2&re=02&dn=1&yo=criminal&ia=03&x=0&y=0&ky=&page=2&vm=02, *archived at* https://perma.cc/8PQ9-CFS2.

[2] 条解　刑事訴訟法(第 4 版) 追補 [ARTICLE-BY-ARTICLE COMMENTARY ON CRIMINAL PROCEDURE CODE (4TH ED.) SUPPLEMENT] 19 (Koya Matsuo et al. eds., 2009), http://www.koubundou.co.jp/files/35467_1.pdf, *archived at* https://perma.cc/GZJ5-5Z9P.

[3] *Id.*

[4] CODE OF CRIMINAL PROCEDURE art. 99-2 & art. 218, para. 1.

[5] SUPPLEMENT, *supra* note 2, at 12.

[6] *Id.*

[7] Act on Interception of Communications for Criminal Investigation, Act No. 137 of 1999, art. 11.

[8] KENZABURO YAZAWA & SHUNJI KATO, Q&A SOSHIKITEKI HANZAI TAISAKU SANPO 135 (2001), *bibliographic information at* https://lccn.loc.gov/2005442553.

communications.[9] Law enforcement officials are required to record all encrypted communications in an appropriate medium and attempt to decrypt it later.[10] Currently, the interception of communications is allowed for the investigation of four organized crimes: drug trafficking, gun running, mass smuggling of people, and murders by crime syndicates.[11] A proposal for an amendment to the law that would expand its application is pending before the Diet.[12]

When law enforcement officials obtain encrypted information through the interception of communications or seizures, they may request private firms to decrypt it.[13] However, such firms are not penalized for declining the request.[14]

[9] *Id.*

[10] *Id.* art. 13, para. 2.

[11] *Id.* art. 3.

[12] Bill to Amend Criminal Procedure Code and Others, Cabinet Bill No. 42 of 189th Diet Session (2015).

[13] CODE OF CRIMINAL PROCEDURE art. 197, para. 2.

[14] *Budget Committee 10th Meeting Minutes*, *House of Councillors*, 190th Diet 39 (Mar. 7, 2016) (statement of Mitsuhide Iwaki, Minister of Justice) http://kokkai.ndl.go.jp/SENTAKU/sangiin/190/0014/19003070014010.pdf, *archived at* https://perma.cc/F3TB-YYFJ.

South Africa

Hanibal Goitom
Foreign Law Specialist

SUMMARY South Africa permits law enforcement and security agencies to intercept various forms of communication. The applicable law requires telecommunications service providers to ensure that their systems can be intercepted and to store all communication-related information for between three and five years. While the agencies must first obtain an interception direction from the relevant court in order to intercept direct or indirect communications, no direction is required in cases of emergency. An agency petitioning for an interception direction may also seek a decryption direction the issuance of which would entitle it, depending on the terms of the direction, to demand that a decryption key holder disclose the decryption key or provide decryption assistance.

I. Introduction

Surveillance of domestic communications is primarily governed under the Regulation of Interception of Communications and Provision of Communication-Related Information Act 2002 and its subsidiary legislation.[1] With the exception of a few provisions, the Act took effect in September 2005.[2] All of the provisions of the Act had been in effect as of June 2009.[3]

A 2014 report showed which of the country's law enforcement and security agencies obtained court authorizations to monitor communications and how often such authorizations were granted. According to the report, from 2008 through 2011, there was a 170% increase in the number of court authorizations (referred to as "interception directions" throughout this report—see Part III,

[1] Regulation of Interception of Communications and Provision of Communication-Related Information Act No. 70 of 2002, 34 BUTTERWORTHS STATUTES OF THE REPUBLIC OF SOUTH AFRICA (updated through 2015), available on the Southern African Legal Information Institute (SAFLII) website, *at* http://www.saflii.org/za/legis/consol_act/roiocapocia2002925, *archived at* https://perma.cc/9TRT-PFEG; Department of Communications, sched. A, Directive for Fixed Line Operators in Terms of Section 30(7)(a) Read with Section 30(2) of the Regulation of Interception of Communication-Related Information Act, 2002 (Act No. 70 of 2002), Government Notice (GN) No. 1325/2005 (Nov. 28, 2005), http://www.gov.za/sites/www.gov.za/files/28271_0.pdf, *archived at* https://perma.cc/RXS3-ZBCX; Department of Justice and Constitutional Development, Notice in Terms of Section 31 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act No. 70 of 2002): Mobile Cellular Operations, GN No. R93 (Feb. 6, 2009), http://www.gov.za/sites/www.gov.za/files/gg31844_nn93_pg10-15.pdf, *archived at* https://perma.cc/D4D5-TD5H; Department of Justice and Constitutional Development, Notice in Terms of Section 44(1)(a) of the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act 70 of 2002), GN No. R1263 (Dec. 29, 2005), http://www.justice.gov.za/legislation/regulations/r2005/gg28371_r1263_interception-notice.pdf, *archived at* https://perma.cc/XD4V-GBLZ; Department of Justice and Constitutional Development, Notice in Terms of Section 31 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act 70 of 2002): Fixed Line Operations, GN No. R. 92 (Feb. 6, 2009), http://www.gov.za/sites/www.gov.za/files/31844_92.pdf, *archived at* https://perma.cc/888G-F92Y.

[2] Regulation of Interception of Communications and Provision of Communication-Related Information Act § 63.

[3] *Id.*

below) for interception of communications with 206 authorizations in 2008/09 and 418 authorizations in 2010/11.[4] The report indicated a substantial decline in authorizations in the following two years in which 261 authorizations were issued in 2011/12 and 144 in 2012/13.[5] Most of the authorizations were issued to the South African Police Service (SAPS) and the State Security Agency (SSA). For example, SAPS was issued 107 authorizations in 2008/09 and 436 authorization in 2010/11, while the SSA was issued 84 and 127 authorizations during the same time periods.[6] It is important to note that one authorization may represent large numbers of interceptions—for instance, the report indicated that the facility that intercepts communications was able to make over three million interceptions using only 882 authorizations over a three-year period.[7]

The above numbers do not account for interceptions conducted without prior court authorization. Over a nineteen-month period in 2010/11, 3,217 interceptions without court authorization are said to have been carried out by law enforcement and security agencies in South Africa.[8]

II. Interception Capability and Storage

The Communications and Provision of Communication-Related Information Act guarantees the ability of the relevant law enforcement and security agencies in the country to intercept communications by requiring that all telecommunications service providers "provide a telecommunication service which has the capability to be intercepted" and store communications-related information.[9] The provision of telecommunications services that do not have the capability to be intercepted is prohibited.[10] The required period of storage of communication-related information ranges from three to five years.[11] In addition, electronic

[4] RIGHT TO KNOW, STATE OF THE NATION REPORT: TRENDS, PATTERNS AND PROBLEMS IN SECRECY 6 (2014), http://www.r2k.org.za/wp-content/uploads/R2K-secrecy-report-2014.pdf, *archived at* https://perma.cc/CPK5-Z4Z8.

[5] *Id.*

[6] *Id.*

[7] *Id.* at 7.

[8] Jane Duncan, *Securocrats Serious About Cyberwarfare*, MAIL & GUARDIAN (Feb. 20, 2015), http://mg.co.za/article/2015-02-19-securocrats-serious-about-cyberwarfare, *archived at* https://perma.cc/3UUS-UH6F.

[9] Regulation of Interception of Communications and Provision of Communication-Related Information Act § 30. "Communication–related information" is

> any information relating to an indirect communication which is available in the records of a telecommunication service provider, and includes switching, dialling or signalling information that identifies the origin, destination, termination, duration, and equipment used in respect, of each indirect communication generated or received by a customer or user of any equipment, facility or service provided by such a telecommunication service provider and, where applicable, the location of the user within the telecommunication system. *Id.* § 1.

[10] *Id.* Preamble; Nazreen Bawa, *The Regulation of Interception of Communications and Provisional Communication Related Information Act*, *in* TELECOMMUNICATIONS LAW IN SOUTH AFRICA 296, 300 & 307 (Lisa Thornton et al. eds., 2006), available on the University of Witwatersrand University website, *at* https://www.wits.ac.za/media/migration/files/TeleLawfull.pdf, *archived at* https://perma.cc/YE6L-GLH6.

[11] Regulation of Interception of Communications and Provision of Communication-Related Information Act § 30.

communications service providers[12] that provide mobile cellular electronic communications services must, at their own cost, "record and store" various information regarding their customers.[13]

III. Interception of Communications

The governing law allows law enforcement and security agencies to intercept[14] communications in certain circumstances with or without an interception direction.[15] The law provides that a law enforcement officer "who executes an interception direction or assists with the execution therefore, may intercept any communication . . . to which that interception direction relates," including direct[16] and indirect[17] communication.[18] An interception direction is a court-issued

[12] An "electronic communications service provider" is

> any –
> (a) person who provides an electronic communication service under and in accordance with a electronic communication service licence issued to such person under Chapter 3 of the Electronic Communications Act, and includes any person who provides –
> (i) a local access communication service, public pay-telephone service, value-added network service or private electronic communication network as defined in the Electronic Communications Act; or
> (ii) any other electronic communication service licensed or deemed to be licensed or exempted from being licensed as such in terms of the Electronic Communications Act; and
> (b) Internet service provider. *Id.* § 1.

[13] *Id.* § 40.

[14] The term "intercept" is defined as

> the aural or other acquisition of the contents of any communication through the use of any means, including an interception device, so as to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient of that communication, and includes the –
> (a) monitoring of any such communication by means of a monitoring device;
> (b) viewing, examination or inspection of the contents of any indirect communication; and
> (c) diversion of any indirect communication from its intended destination to any other destination,
> and "interception" has a corresponding meaning. *Id.* § 1

[15] *Id.* ch. 2.

[16] This is an

> (a) oral communication, other than an indirect communication, between two or more persons which occurs in the immediate presence of all the persons participating in that communication; or
> (b) utterance by a person who is participating in an indirect communication, if the utterance is audible to another person who, at the time that the indirect communication occurs, is in the immediate presence of the person participating in the indirect communication. *Id.* § 1.

[17] This is

> the transfer of information, including a message or any part of a message, whether –
> (a) in the form of –
> (i) speech, music or other sounds;
> (ii) data;
> (iii) text;
> (iv) visual images, whether animated or not;
> (v) signals; or
> (vi) radio frequency spectrum; or

authorization to intercept any communication "in the course of its occurrence or transmission."[19] In addition, a law enforcement officer may make an application before the relevant court for

- a real-time communications-related direction;
- an archived communications-related direction; or
- the simultaneous issuing of an interception direction, a real-time communications direction, and an archived communications-related direction, or of an interception direction supplemented by a real-time communications-related direction.[20]

There are instances in which law enforcement officers do not need an interception direction in order to intercept communications. These include instances where the interception is done to prevent impending serious bodily harm and for the purpose of determining location in the case of an emergency.[21]

IV. Decryption of Encrypted Information

A law enforcement officer seeking an interception direction from a court may also make an application for a "decryption direction."[22] With the issuance of a decryption direction, the decryption key holder is required, as per the specifications in the decryption direction, to disclose the decryption key or provide decryption assistance.[23] A decryption key is "any key, mathematical formula, code, password, algorithm or any other data which is used to . . . allow access to encrypted information . . . or . . . facilitate the putting of encrypted information into an intelligible form."[24] A decryption key holder is "any person who is in possession of a decryption key for the purpose of subsequent decryption of encrypted information relating to indirect communications."[25] A decryption direction may only be issued if the judge before whom the application is made is satisfied that

- the indirect information in question is partly or completely encrypted;
- the decryption key holder is in possession of the encrypted information and the decryption key;

(b) in any other form or in any combination of forms, that is transmitted in whole or in part by means of a postal service or a telecommunication system. *Id.*

[18] *Id.* § 3.

[19] *Id.* § 1.

[20] *Id.* §§ 16, 17, 18 & 19.

[21] *Id.* §§ 7 & 8.

[22] *Id.* § 21.

[23] *Id.* §§ 1 & 29.

[24] *Id.* § 1. "Intelligible form" is defined as "the form in which the electronic data was before an encryption of similar process was applied to it." *Id.* § 1.

[25] *Id.*

- failure to issue a decryption direction would defeat the purpose for which the interception direction was issued; and
- it is not "reasonably practicable" for the applicant to acquire the encrypted information in question in "an intelligible form" without a decryption direction.[26]

V. Admissibility in Court

Any information regarding the commission of an offense obtained through interception or the provision of any real-time or archived communications-related information under South African or foreign law (with the authorization of the national director of public prosecutions) may be admissible in criminal or civil proceedings.[27]

[26] *Id.* § 21.

[27] *Id.* § 47.

Sweden

Elin Hofverberg
Foreign Law Research Consultant

SUMMARY Swedish law allows for the issuance of search warrants when a crime with a prison sentence is being investigated. Swedish law does not require encryption companies to decrypt cellphones. Legislation enabling forced decryption has previously been proposed but never adopted. All searches and seizures require a prior proportionality test, weighing the reasons for the measure against the privacy and integrity of the subject of the search. A recent Supreme Court case indicates that searches on devices may be limited because of this test. Legislative proposals are pending that would allow the Swedish police to infect suspects' computers with Trojan horse malware.

I. Background

Swedish police and prosecutors have previously requested authority to use new tools, such as the deployment of Trojan horse malware, to enable decryption of suspects' cellphones, according to news reports.[1]

A 2015 audit by the Swedish National Audit Office revealed that forensic experts at the Swedish (national) Police occasionally hack into cellphones.[2] Police access to cellphones has reportedly only rarely been hampered by encryption or similar preventive efforts.[3] The Swedish Security Police (SÄPO) reports that forensic analyses are part of all its investigations.[4] There are legal restrictions, however, not least in regard to international cloud services, which under Swedish law cannot be searched by Swedish police if the servers are outside of Sweden, as it would be considered a search in a foreign country.[5]

[1] *Säpo kräver trojaner*, VECKANSAFFÄRER (Apr. 25, 2014), http://www.va.se/nyheter/2014/04/25/sapo-kraver-trojaner, *archived at* https://perma.cc/2MM7-JBW4; *Prosecutors Want Access to Decryption Tools*, RADIO SWEDEN (Aug. 22, 2012), http://sverigesradio.se/sida/artikel.aspx?programid=2054&artikel=5246277, *archived at* https://perma.cc/N33Z-ZTD2.

[2] RIKSREVISIONEN IT-RELATERAD BROTTLISGHET – POLIS OCH ÅKLAGARE KAN BLI EFFEKTIVARE 18, RIR 2015:21, http://www.riksrevisionen.se/PageFiles/23153/RiR_2015_21_IT-relaterade-brott_Anpassad.pdf, *archived at* https://perma.cc/P5AV-MVR4.

[3] *Id.* at 47.

[4] *IT är med i alla våra brottsutredningar*, SÄKERHETSPOLISEN, http://www.sakerhetspolisen.se/ovrigt/menyer/medarbetarportratt/it-ar-med-i-alla-vara-brottsutredningar-.html (last visited Apr. 12, 2016), *archived at* https://perma.cc/VB83-ZGJL.

[5] Departementsserie [Ds.] 2005:6 Brottsutredning i it-miljö [Crime Investigation in the IT Environment], at 131, http://www.regeringen.se/contentassets/3f7139539cd3460b9ee6c3d343923213/brott-och-brottsutredning-i-it-miljo.-europaradets-konvention-om-it-relaterad-brottslighet-med-tillaggsprotokoll, *archived at* https://perma.cc/7NDN-44K7.

Following the Paris terrorist attacks in November 2015 the Swedish government declared that it would initiate, research, and propose new legislation to enable access to encrypted information.[6] The proposal is forthcoming—no initial committee report has yet been published.[7]

II. Current Law

A. Decryption Pursuant to Warrants

Swedish law provides limited possibilities for decryption pursuant to a warrant. The Swedish Constitution provides protection against unlawful searches of persons and property.[8] Search warrants can only be made under law.[9] The issuance of search warrants is regulated in Rättegångsbalken (the Civil and Criminal Procedure Act).[10] A search warrant can be issued if the crime investigated is sanctioned with a prison sentence.[11] However, in each case the person issuing the search warrant must conduct a proportionality test (*proportionalitetsprövning*), weighing the invasion of the suspect's privacy versus the benefits of issuing the warrant.[12] A police officer may conduct a search without first securing a search warrant if there is an immediate danger in not conducting the search.[13] Subject to a proportionality evaluation, a search warrant may also be issued for a place not directly connected with the crime or suspect if there are extraordinary reasons to suspect that useful information will be found.[14]

The Swedish Supreme Court has found that searches of computers and cellphones are an especially sensitive area of the law, as computers and cellphones "may . . . include evaluation of a significant number of files and large amounts of data that is not sought [by the Police]."[15] This means that the proportionality test is especially important in these cases.[16] Depending on the

[6] *Fler insatser för att motverka terrorism*, REGERINGEN (Nov. 19, 2015), http://www.regeringen.se/artiklar/2015/11/fler-insatser-for-att-motverka-terrorism, *archived at* https://perma.cc/6HN4-JR6E.

[7] For an overview of the process for adopting legislation, see *Commissions of Inquiry*, SVERIGESRIKSDAG, https://www.riksdagen.se/en/How-the-Riksdag-works/What-does-the-Riksdag-do/Legislation/Commissions-of-inquiry (click headings under "Commissions of inquiry" in the list of topics on the left) (last visited Apr. 11, 2016), *archived at* https://perma.cc/664Z-29FF.

[8] 2 ch. 6 § REGERINGSFORMEN [RF] (Svensk författningssamling [SFS] 1974:152), https://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Kungorelse-1974152-om-beslu_sfs-1974-152/#K2, *archived at* https://perma.cc/KBQ2-D8BY.

[9] *Id.* 2 ch. 6 & 20 §§.

[10] RÄTTEGÅNGSBALKEN [RB] [CODE OF CIVIL AND CRIMINAL PROCEDURE] (SFS 1942:740), https://www.notisum.se/rnp/sls/lag/19420740.htm, *archived at* https://perma.cc/ULE7-Y8JQ.

[11] *Id.* 28 ch. 1 §.

[12] *Id.* 28 ch. 3a §.

[13] *Id.* 28 ch. 5 §.

[14] *Id.* 28 ch. 1 § 2 st.

[15] Högsta Domstolen [HD] [Supreme Court], 2015-08-18, Ö 3074-15, at 6, http://www.hogstadomstolen.se/Domstolar/hogstadomstolen/Avgoranden/2015/2015-08-18%20O%203074-15%20Beslut.pdf, *archived at* https://perma.cc/A5AA-8JBT (all translations by author).

[16] *Id.* 17, 28–29 ¶¶.

outcome of a proportionality test, seizure of a cellphone may thus be possible under Swedish law, but decryption might be illegal.

B. Seizure of Encrypted Information

Property that can reasonably be presumed to have importance in an investigation can be seized,[17] except for excluded property such as secret information pertaining to information that a person could not divulge in court.[18] Parliamentary committees have interpreted this exclusion to also include electronic property.[19] The Supreme Court in 2015 affirmed that conclusion.[20] If a document (or electronic media) is protected by a prohibition against seizure (*beslagsförbud)*, this is absolute and cannot be overridden by the proportionality test.[21] The reason behind this absolute prohibition is that the police and prosecutor must not be able to circumvent the rules limiting what can be asked of a witness—for example, limitations based on the attorney-client privilege or doctor-patient confidentiality under Swedish secrecy law.[22]

The Supreme Court has previously refused requests for the production of certain data because the data was held by persons who were subject to legally mandated, professional secrecy.[23] Where secret information is present on a device such as a cellphone, that fact alone does not bar a search for information on the device, but does weigh negatively against the search in a proportionality test.[24]

C. Information Owner's Obligation to Decrypt

Sweden is a signatory to the Council of Europe Directive on Cybercrime.[25] In a 2013 government report the Cyber Convention Commission, while evaluating the need for new legislation to enable implementation of the Cybercrime Directive, found that there currently is a possibility under Swedish law to "order a person with knowledge of a computer systems' function or of measures that are used to protect the [desired] information, to provide information

[17] 27 ch. 1 § RB.

[18] *Id.* 27 ch. 2 §.

[19] *See, e.g.*, Statens Offentliga Utredningar [SOU] 2011:45 Förundersökning – objektivitet, beslag, dokumentation m.m. [government report], http://data.riksdagen.se/fil/40CFC0F1-4704-4C11-9CA1-D03634483049, *archived at* https://perma.cc/NHV9-68VT.

[20] HD Ö 3074-15, 14 ¶.

[21] *Id.* 20 ¶.

[22] *Id.* 23 ¶.

[23] *Id.* 24 ¶; *see* Nytt Juridiskt Arkiv [NJA] 1981 s. 791 & NJA 1992 s. 307.

[24] HD Ö 3074-15, 29 ¶.

[25] Convention on Cybercrime, Nov. 23, 2001, 185 E.T.S., http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf, *archived at* https://perma.cc/AZE4-YJ5M; *Chart of Signatures and Ratifications of Treaty 185*, *Convention on Cybercrime*, *Status as of 18/04/2016*, *Full List*, COUNCIL OF EUROPE, TREATY OFFICE, http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=GfgVFijr.l, *archived at* https://perma.cc/R335-RSB7.

that is necessary to enable the execution of the warrant."[26] The Cyber Convention Commission thus concluded that there was no need to change Swedish legislation to adopt the Council of Europe Directive on Cybercrime.[27] It is unclear whether the Commission's interpretation would apply to the creators of encryption software or only to the person who stored the information.

The Swedish Data Protection Authority criticized the Commission's interpretation that a person subject to a warrant can be required to provide keys to his or her computer.[28] The statement could be interpreted by the courts as a requirement to self-incriminate—for example, when an individual is required to present his or her password—and as such could be a violation of human rights as interpreted by the European Court of Human Rights (ECHR).[29]

Another police measure that could potentially be invoked to force access to encryption keys is "testimony before the courts during police investigations" (*vittnesförhör inför rätta under en förundersökning*).[30] Persons who are thought to have information of importance to an investigation may, under the threat of a fine (*vite*), be asked to report to the investigator (generally the police) to divulge their information before the court.[31] This could be interpreted to include requests that third parties aware of a password divulge that information.[32]

D. Obligation of Encryption Companies to Decrypt Data

Swedish law does not require encryption companies to decrypt data. However, members of Parliament have previously made such proposals. For instance, Motion 2013/14:JU277 proposed that encryption companies be required to decrypt files in child-pornography cases, but that proposal was rejected by the Justice Committee, which cited other efforts by the government to address child pornography.[33]

[26] SOU 2013:39 Europarådets konvention om it-relaterad brottslighet [government report series], at 146, http://www.regeringen.se/contentassets/b7ef66bff0b94040b781df446546c745/europaradets-konvention-om-it-relaterad-brottslighet-sou-201339, *archived at* https://perma.cc/HN8M-K877.

[27] *Id.* at 150.

[28] *See* DATAINSPEKTIONEN, REMISSSVAR AV BETÄNKANDET EUROPARÅDETS KONVENTION OM IT-RELATEDARD BROTTSLIGHET [CONSULTATION RESPONSE TO THE GOVERNMENT REPORT ON THE EUROPEAN COUNCIL'S CONVENTION ON CYBERCRIME] (SOU 2013:39) 2–3(Sept. 19, 2013), http://www.datainspektionen.se/Documents/remissvar/2013-09-25-konvention-it-brottslighet.pdf, *archived at* https://perma.cc/4V8A-UJKG.

[29] SOU 2013:39, *supra* note 26, at 283; *see also* Johan Holmgren, Kryptering, dekryptering och de mänskliga rättigheterna 20–22 (unpublished thesis, Law Faculty, Lund University), *available at* https://lup.lub.lu.se/student-papers/search/publication/3046392 (last visited Apr. 19, 2016), *archived at* https://perma.cc/ZK9S-MHNN.

[30] SOU 2013:39, *supra* note 26, at 146.

[31] 23 ch. 13 § RB; *see also id.* 23 ch. 6, 6a, 6b §§.

[32] SOU 2013:39, *supra* note 26, at 334.

[33] Justitieutskottet betänkande 2013/14:JuU14 Polisfrågor [Justice Committee Report 2013/14:JuU14, Police Issues], https://www.riksdagen.se/sv/Dokument-Lagar/Utskottens-dokument/Betankanden/Polisfragor_H101JuU14/?html=true, *archived at* https://perma.cc/39D3-WEBY.

E. No Decryption Requirement for Internet Service Providers

Internet Server Providers (ISPs) are required to collect and store metadata on all of its customers for six months.[34] However, ISPs cannot be required to decrypt any information sent over their networks. The extent of the data collected as well as the willingness to produce such data varies among Swedish ISPs.[35]

F. Secret Surveillance

Secret surveillance is regulated in chapter 27 of the Civil and Criminal Procedure Act.[36] The police are allowed to secretly surveil electronic communications for crimes that carry a sentence of at least two years' imprisonment.[37] However, the police may only use secret surveillance if it is of exceptional importance to the investigation and the target is suspected, on reasonable grounds, of having committed the crime.[38] The police are not allowed to surveil electronic communications over communications networks that are of lesser importance from a public communications perspective.[39]

III. Court's Call for Legislative Action

In a 2015 decision denying access to digital images in a robbery case, the Swedish Supreme Court issued a rare statement[40] explaining that it was restricted by the fact that Swedish "legislation regarding the use of coercive measures in the so-called virtual space is outdated."[41] The Court continued, "[i]t is urgent that the legislative branch [Swedish Parliament] correct this [as the Court cannot do this, not least] as good legal custom presumes a significant level of technical or other non-legal expertise."[42]

The case hinged on the fact that the images were protected by a constitutional right of freedom to communicate information (*meddelarfrihet*) and that seizing the images could have exposed the

[34] 6a, 16d §§ LAG OM ELEKTRONISK KOMMUNIKATION [LEK] [ACT ON ELECTRONIC COMMUNICATION] (SFS 2003:389), http://www.notisum.se/rnp/sls/lag/20030389.HTM, *archived at* https://perma.cc/3YFS-C9YN.

[35] For example, the ISP Banhof has taken a more restrictive stance on when to provide data to the government. *Advokaten: Det måste finnas gränser för vad polisen ska kunna få tillgång till*, BAHNHOF (Apr. 8, 2016), https://www.bahnhof.se/press/press-releases/2016/04/08/advokaten-det-maste-finnas-granser-for-vad-polisen-ska-kunna-fa-tillgang-till, *archived at* https://perma.cc/PY9X-EWQQ.

[36] 27 ch. RB.

[37] *Id.* 27 ch. 18 § 2 st.

[38] *Id.* 27 ch. 20 § 1 st.

[39] *Id.* 27 ch. 20 § 3 st.

[40] Press Release, HD, Högsta domstolen avslår åklagarens begäran om husrannsakan hos Aftonbladet (Aug. 18, 2015), http://www.hogstadomstolen.se/Mer-om-Hogsta-domstolen/Nyheter-fran-Hogsta-domstolen/Hogsta-domstolen-avslar-aklagarens-begaran-om-husrannsakan-hos-Aftonbladet, *archived at* https://perma.cc/W4KA-CL4S.

[41] HD Ö 3074-15, 43 ¶.

[42] *Id.*

photographer, which was not outweighed by the police's need for the picture. Swedish journalists are not allowed to reveal confidential sources, as specified in the Swedish Constitution,[43] and a proportionality test is always required by law.[44]

IV. Conclusion

In practice it is unlikely that a Swedish court would force an ISP, encryption company, or other entity to decrypt data pursuant to current law, as the measure would not be considered proportional. The matter will likely be addressed by the legislature.

[43] *See* 1 ch. 1 § 3 st TRYCKFRIHETSFÖRORDNINGEN [TF] [FREEDOM OF THE PRESS ACT] (Constitution).

[44] 27 ch. 1 § 3 st RB.

Taiwan

Laney Zhang
Senior Foreign Law Specialist

SUMMARY Under Taiwanese law, an interception warrant generally needs to be sought by a prosecutor upon request by the judicial police authorities and issued by a court before interception can commence. The intelligence agency, however, does not appear to need a warrant from the court when intercepting the communications of foreign governments or cross-border terrorist organizations for national security purposes.

Although the law does not specifically address government access to encrypted communications, it generally requires telecommunications companies to equip their hardware and software "with functions that can cooperate with interception" and to provide "interfacing devices" in assisting government surveillance of communications.

I. Surveillance of Communications

In Taiwan, government surveillance of communications and the legal requirements of telecommunications companies in assisting such surveillance are regulated by the 1999 Communications Protection and Surveillance Act, as amended in January 2014 (Surveillance Act).[1]

"Communications" under the Surveillance Act include telecommunications, emails, letters, speeches not made though telecommunications, and face-to-face conversations.[2] The term "telecommunications" refers to "utilizing wired or wireless telecommunications equipment to send, store, transmit, or receive information."[3]

A. Interception Warrant Issued by Court

In general, an interception warrant is sought by the prosecutor upon request by the judicial police authorities and issued by a court. Such an interception must be for the purpose of investigating the specific crimes set forth by the Surveillance Act, which include all crimes punishable by a minimum of a three-year, fixed-term imprisonment. There must be sufficient evidence that the accused or the suspect is involved in such a crime and that national security or the economic or

[1] 通訊保障及監察法 [Communication Protection and Surveillance Act] (Surveillance Act) (promulgated July 14, 1999, amended Jan. 29, 2014), art. 5, LAWS AND REGULATIONS DATABASE OF THE REPUBLIC OF CHINA, http://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=K0060044, *archived at* https://perma.cc/LRH5-4PXZ, English translation *available at* http://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=K0060044, *archived at* https://perma.cc/3C86-73PW.

[2] Surveillance Act art. 3; 通訊保障及監察法施行細則 [Implementation Measures of the Communication Protection and Surveillance Act] (Implementation Measures) (Mar. 15, 2000, amended June 26, 2014), art. 2, http://law.moj.gov.tw/LawClass/LawAll_print.aspx?PCode=K0060053, *archived at* https://perma.cc/JJ6M-45V9.

[3] Surveillance Act art. 3.

social order are severely endangered. In addition, there must be a reasonable belief that the content of the communications subject to surveillance is relevant to the case being investigated, and that it is difficult or impossible to collect or investigate the evidence by other means.[4]

Under urgent situations in investigating certain offenses, however, the prosecutor may "verbally inform" the enforcement authority to start intercepting communications and apply for the interception warrant from the court within twenty-four hours afterward. The court must issue the warrant within forty-eight hours, or otherwise the interception must be ended.[5]

B. Interception Warrant Issued by Head of Intelligence Agency

In intercepting the communications of foreign governments and cross-border terrorist organizations for national security purposes, the intelligence agency does not appear to need an interception warrant from the court. Under such circumstances, the head of the national intelligence agency, the National Security Bureau, is able to issue the interception warrant.[6]

II. Obligations of Telecommunications Companies

The Surveillance Act does not specifically address encrypted communications. The Act generally requires telecommunications companies to provide facilities and personnel as needed to assist government surveillance of communications.[7] Such obligations to assist specifically include equipping their hardware and software "with functions that can cooperate with interception" and providing "spaces, electricity, and relevant interfacing devices," pursuant to the implementation measures of the Surveillance Act.[8]

Moreover, telecommunications operators are required by the Surveillance Act to assist law enforcement agencies in setting up and maintaining systems used for surveillance purposes. The obligation is limited to what is "technologically and economically reasonable" at the time of setting up the system and "should not exceed expected possibilities."[9]

A failure to fulfill the obligations of assisting surveillance is punishable by a fine of 500,000–2,500,000 New Taiwan Dollars (about US$15,500–$77,000), an additional accumulative daily fine, and revocation of licenses.[10]

[4] *Id.* art. 5.

[5] *Id.* art. 6.

[6] *Id.* arts. 7 & 8; Implementation Measures art. 9.

[7] Surveillance Act art. 14.

[8] Implementation Measures art. 26.

[9] Surveillance Act art. 14.

[10] *Id.* art. 31.

III. Conclusion

Although the Taiwanese Surveillance Act does not specifically address government access to encrypted communications, the legal obligations of telecommunications companies in assisting government surveillance may include enabling the decryption of encrypted communications.

United Kingdom

Clare Feikert-Ahalt
Senior Foreign Law Specialist

I. Decryption at the Request of the Intelligence Services and Law Enforcement

The United Kingdom (UK) has had legislation in place since the early 2000s that enables specified high-ranking law enforcement and intelligence officials to serve a written notice on individuals and bodies that requires them to disclose lawfully held encrypted information in an intelligible form.[1] This notice provides a means for what is described as "enforced decryption."[2]

To obtain a notice, the desired disclosure of information must be proportionate to what the requester is seeking to achieve and necessary in the interests of national security, for the purposes of preventing or detecting crime, or in the interests of the economic well-being of the UK. In addition, acquiring the information in an intelligible form without a notice must not be reasonably practicable.[3]

The notice must be in writing, describe the protected information to which it relates, specify the position of the person giving the notice, specify the position of the person who granted permission for the notice, and establish a time limit for compliance with the notice. The notice must also describe the disclosure that is required and the way that the disclosure should be made.[4] The penalty for failing to comply with a disclosure notice is up to two years' imprisonment for regular cases or five years' imprisonment in national security cases, upon conviction.[5] This term of imprisonment has been criticized as being insufficient on the grounds that, if an individual's device contains encrypted information that could be used as evidence to convict him or her of a serious criminal offense, refusing to provide the encryption key in response to a notice carries a lesser sentence than the individual might otherwise receive.[6]

Redacted information in a report by the Intelligence and Security Committee of Parliament indicates that Government Communications Headquarters (GCHQ) has a program of work dedicated to unlocking encrypted communications, which requires no ministerial authorization.[7]

[1] Regulation of Investigatory Powers Act 2000, c. 23, § 49 & sched. 2, http://www.legislation.gov.uk/ukpga/2000/23, *archived at* https://perma.cc/B53E-4RJ7.

[2] DAVID ANDERSON Q.C., A QUESTION OF TRUST: REPORT OF THE INVESTIGATORY POWERS REVIEW ¶ 8.30 (June 2015), https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf, *archived at* https://perma.cc/N4UN-UE7F.

[3] Regulation of Investigatory Powers Act 2000, c. 23, § 49.

[4] *Id.*

[5] *Id.* § 53.

[6] ANDERSON, *supra* note 2, ¶ 8.31.

[7] INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT, PRIVACY AND SECURITY: A MODERN AND TRANSPARENT LEGAL FRAMEWORK, 2014–15, H.C. 1075, ¶¶ 179–180, http://isc.independent.gov.uk/files/20150312_ISC_P+S+Rpt(web).pdf, *archived at* https://perma.cc/6NDK-FCKH.

The program is provided for under the general power given to the GCHQ under section 3(1)(a) of the Intelligence Services Act, which states that the GCHQ may "monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and … obtain and provide information derived from or related to such emissions or equipment and from encrypted material."[8]

The Intelligence Services and Police may interfere with equipment (also known as "computer network exploitation") to obtain communications, equipment data, and other information from equipment. The use of computer network exploitation varies from using someone's login information to remotely and covertly installing software on a device.[9] The security and intelligence agencies may apply to the Secretary of State to obtain a warrant to use equipment interference if it is necessary in the interests of national security or the economic well-being of the UK, or to prevent and detect serious crime.[10]

II. Pending Investigatory Powers Bill

A draft Investigatory Powers Bill was published in the autumn of 2015 and consolidates and expands provisions relating to law enforcement's access to encrypted information.[11]

A. Equipment Interference

The Bill would introduce specific procedures for law enforcement and intelligence services to undertake equipment interference to access individuals' devices and computers to obtain data, such as communications via texts and email, and geolocation. Equipment interference could also be used to obtain otherwise encrypted data.[12] Clauses 88–90 of the Bill would provide law enforcement with the ability to apply for warrants for two equipment interference purposes:

- Targeted equipment interference. This would authorize law enforcement to interfere with equipment to obtain communications, private information, or equipment data, as well as to disclose, monitor, and examine this material.
- Targeted examination warrants. This would authorize the individual named in the warrant to examine material obtained under a bulk equipment interference warrant. Bulk equipment interference warrants are provided for in clauses 119–137 of the Bill and would apply only to individuals outside the UK.

[8] Intelligence Services Act 1994, c. 13, § 3(1)(a), http://www.legislation.gov.uk/ukpga/1994/13, *archived at* https://perma.cc/FK2X-9ARJ.

[9] *Id.* §§ 5 & 7; Police Act 1997, c. 50, § 93, http://www.legislation.gov.uk/ukpga/1997/50, *archived at* https://perma.cc/ 2QW2-LZTX.

[10] Intelligence Services Act 1994, § 3(2).

[11] Draft Investigatory Powers Bill 2015, 2015–16 Cm. 9152, *available at* https://www.gov.uk/government/publications/draft-investigatory-powers-bill, *archived at* https://perma.cc/9P94-FTYA.

[12] HOUSE OF COMMONS LIBRARY, INVESTIGATORY POWERS BILL, Mar. 11, 2016, Briefing Paper No. 7518, http://researchbriefings.files.parliament.uk/documents/CBP-7518/CBP-7518.pdf, *archived at* https://perma.cc/LP5A-964S.

Clauses 84–91 would authorize a senior law enforcement officer, with approval from a Judicial Commissioner, or the Secretary of State upon application from the intelligence services, to issue a warrant for equipment interference. Clause 84 provides that, for the intelligence services to obtain a warrant for equipment interference from the Secretary of State, the applicant would need to show that it is necessary

- on the grounds of national security,
- to prevent or detect serious crime, or
- that it is in the interests of the economic well-being of the UK, and
- that the warrant is proportionate.

Clause 89 of the Bill would authorize senior law enforcement officers to apply for a warrant to authorize equipment interference if necessary

- for the purposes of preventing and detecting serious crime; or
- to prevent death, injury, or damage to a person's physical or mental health; and
- that is a proportionate response.

The Bill would allow warrants to be granted to intercept equipment in cases where the targeted equipment interference is to obtain information subject to a legal privilege. There must be exceptional and compelling circumstances to justify the interception of such materials, however, and additional handling arrangements must be in place.[13] An individual who has a warrant would be able to serve a copy of it on anyone who may be able to assist him/her, including individuals outside the UK.[14] Clause 111 would "[place] a duty on telecommunications providers to assist with the implementation of equipment interference warrants."[15]

Because of the sensitive nature of such warrants, the Bill would create a duty not to make unauthorized disclosures about the existence or details of both the warrant and any materials obtained under it, and clause 116 sets out a specific offense of the unauthorized disclosure of such information.

B. Notices Requiring Communication Service Providers to Facilitate Assistance

Clause 214 of the Bill would authorize the Secretary of State to introduce measures to facilitate compliance with the Bill in areas that include decryption of communications. Clause 217 would enable the Secretary of State to impose obligations on communication service providers through regulations, in the form of technical capability notices to facilitate assistance to warrants issued under specified parts of the Investigatory Powers Bill. Clause 213 provides that communication service providers would receive a contribution towards any costs they incurred to comply with

[13] Draft Investigatory Powers Bill 2015, cl. 100.

[14] *Id.* cls. 109–110.

[15] HOUSE OF COMMONS LIBRARY, *supra* note 12, at 43.

the measure. Clause 189 provides that such obligations would include the removal of electronic protection applied by an operator, or any third party acting on their behalf, to any data or communications. When making these notices, the Secretary of State would be required to take into account the technical feasibility and cost of compliance.

C. Opposition to the Bill

These provisions have met considerable resistance both within the government and in private industry, who are concerned not only with the ability to access the communications that it appears the Bill requires, but also at the negative impact it could have on the UK's technology industry. Recommendations from the committee reviewing the Bill notes that the government should make it explicit that, if the Bill is adopted, providers of "end-to-end encrypted communication or other un-decryptable communication services will not be expected to provide copies of those communications if it not practicable for them to do so."[16] Concerns have been raised that the language used in this clause would result in the prohibition of end-to-end encryption in the UK, and review committees are urging the government to clarify the nature of the obligations that would be required under the Bill. The government has responded that a Code of Practice will contain further details as to the necessity and proportionality of imposing these requirements on communication service providers.[17]

The Bill is currently in draft form, which means it will be reviewed and subject to consultations before being formally introduced in the House of Commons. As the Bill contains some controversial provisions, it is uncertain when it will be formally introduced, or if introduced whether it will be enacted.

[16] *Id.* at 71.

[17] *Id.* at 42.

Daniel Charles Richman

From: Daniel Charles Richman
Sent: Friday, January 06, 2017 12:04 PM
To: [redacted] (DO) (OGA) b6 -1 b7C -1
Subject: Re: Going Dark Comparative Approaches
Attachments: 01.03.17 Letter to House Encryption Working Group – Final.pdf

Thanks. Just looking at it. Also
1. I was in touch with Kenn Kern, at DANY who says "The state and local law enforcement community is convening in DC on Feb 7 on encryption. There is a real sense of momentum." He also send me a recent letter to House Judiciary Committee in opposition to their recent Report. See attached.
2. I checked with Jim Rybicki on your detail status. He said that they "can definitely reup" you. You and I should make sure this doesn't fall thru the cracks
d

On Fri, Jan 6, 2017 at 11:59 AM, [redacted] (DO) (OGA) [redacted] wrote: b6 -1,4 b7C -1,4 b7E -3

> We received the international GD legal piece from CRM. I forwarded to you on your FBI email account.
>
> -----Original Message-----
> From: Daniel Charles Richman [mailto:[redacted]
> Sent: Tuesday, January 03, 2017 4:50 PM
> To: [redacted] (DO) (OGA) [redacted]
> Subject: Re: Going Dark Comparative Approaches
>
> Thx. It's a start. And it's been out since may :(Lovely seeing you
>
> Daniel Richman
> Paul J. Kellner Professor of Law
> Columbia Law School
> Office: [redacted] b6 -1,4 b7C -1,4 b7E -3
> Cell: [redacted]
>
> > On Jan 3, 2017, at 4:28 PM, [redacted] (DO) (OGA) [redacted] wrote:
> >
> >
> >
> > -----Original Message-----
> > From: [redacted] (DO) (OGA) b6 -1,5 b7C -1,5
> > Sent: Tuesday, January 03, 2017 4:28 PM
> > To: [redacted] (ODAG) (JMD) [redacted]
> > Subject: Going Dark Comparative Approaches
> >
> > You may have already seen this comparative GD report, but featured on USAbook today.

>
> [redacted]
>
>
>
> --
> BEGIN-ANTISPAM-VOTING-LINKS
> ---------------------------- ----------------------
>
> Teach Email if this mail (ID 01SrVvCfP) is spam:
> Spam: https://antispam.law.columbia.edu/canit/b.php?i=01SrVvCfP&m=6947e7738b93&t=20170103&c=s
> Not spam: https://antispam.law.columbia.edu/canit/b.php?i=01SrVvCfP&m=6947e7738b93&t=20170103&c=n
> Forget vote:
> https://antispam.law.columbia.edu/canit/b.php?i=01SrVvCfP&m=6947e7738b
> 93&t=20170103&c=f
> ---------------------------- ----------------------
> END-ANTISPAM-VOTING-LINKS
>
> <GD Comparative Approaches.pdf>

b6 -1
b7C -1

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office [redacted]
cellphone [redacted]
You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

Association of Prosecuting Attorneys East Baton Rouge

January 3, 2017

House Judiciary Committee & House Energy and Commerce Committee Encryption Working Group

Re: *Encryption Working Group Year-End Report*

Dear Chairman Upton, Chairman Goodlatte, and Members of the Encryption Working Group:

The undersigned have reviewed the Encryption Working Group Year-End Report authored by Members of the House Encryption Working Group (EWG). While we appreciate the Working Group's willingness to study this critical issue that is affecting victims of crime across the United States, we write to express our strong disagreement with the Report's findings and assertions.

The stated mission of the EWG was to conduct a "thorough and objective review" of encryption as it relates to privacy and public safety. The findings of the year-end report were ostensibly derived from six months of meetings with stakeholders from both the private and public sectors. In our view, the Report inadequately addresses the profound concerns of the law enforcement and crime victim communities who grapple every day with the impact of the widespread adoption of default device encryption on criminal investigations and prosecutions.

At a basic level, the Report fails to offer concrete solutions to address the rapidly expanding backlog of warrant-proof devices piling up in police departments and prosecutors' offices across in the United States. Each of these devices, lawfully seized by the order of a neutral judge, shields evidence of criminal suspects' identity, guilt, or innocence.

Beyond the impact of device encryption on "everyday" criminal investigations, as noted by Europol in its *2016 Internet Organised Crime Threat Assessment*, the growing use of encryption services for illegal purposes is central to today's terror threat landscape, thereby thwarting U.S. security interests at home and abroad.

To our surprise, the Report fails to incorporate – much less acknowledge – the data, analysis, and concrete solutions offered by the law enforcement and crime victim communities over the past two years including, but not limited to: 1) the Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety (quantifying the impact of warrant-proof encryption on criminal investigations, explaining the limitations of metadata and other sources of data in criminal proceedings, and setting forth a range of legislative solutions and updating its November 2015 Report on Smartphone Encryption and Public Safety), 2) the Major Cities Chiefs Association and Major County Sheriffs' Association Report on "Going Dark" (providing specific examples from around the country where warrant-proof encryption has either stalled or adversely impacted investigations), and 3) the International Association of Chiefs of Police Summit Report: Data, Privacy and Public

Safety (outlining the technical and statutory barriers to access of electronic evidence). In addition to the information available in these published analyses, law enforcement representatives have briefed this Group's staff as well as other members of Congress on the challenges law enforcement faces, including non-technical barriers to accessing electronic information.

To EWG's credit, the Report does pinpoint the inherent problems associated with its own suggested alternatives to encrypted data, including the limited utility of metadata in prosecutions, the lack of resources to develop and rely on lawful hacking at the state and local levels, and large technology companies' well-documented history of ignoring valid search warrants for electronic data.

While in the past criminals may have kept evidence of their crimes in file cabinets, closets, and safes, today that evidence is more often found on smartphones. Photos and videos of child sexual assault; text messages between sex traffickers and their customers; even a video of a murder victim being shot to death – these are just a few of the pieces of evidence found on smartphones and used by the agencies we represent to prosecute people committing horrific crimes.

It is the rare case in which information from a digital device is *not* critical. Encryption increasingly undermines the ability of law enforcement to thoroughly investigate, exonerate, and prosecute criminals. The Report offers no substantive solutions to the thousands of law enforcement agencies working to protect the public and secure justice for victims and the accused.

Sincerely,

Alabama Office of Prosecution Services
Association of Prosecuting Attorneys
Association of State Criminal Investigative Agencies
East Baton Rouge District Attorney's Office
International Association of Chiefs of Police
Major Cities Chiefs Police Association
Major County Sheriffs' Association
National District Attorneys Association
National Sheriffs' Association
New York County District Attorney's Office

Daniel Charles Richman

From: Daniel Charles Richman
Sent: Friday, January 06, 2017 12:19 PM
To: [redacted](DO) (OGA) b6 -1 b7C -1
Subject: Re: Going Dark Comparative Approaches

I don't know whether there there is Bu coverage at the 2/7 meeting. I'll check right now. And I'm happy to chat whenever it's convenient. I'm working at home today (trying to actually write) and am pretty open (save for a 2pm call with a former student who wants to clerk on the S Ct).
d

On Fri, Jan 6, 2017 at 12:12 PM, [redacted](DO) (OGA)[redacted] wrote: b6 -1 b7C -1 b7E -3

> Thanks—I’ll share the letter with the wider DOJ group to make sure they know. Do you happen to know if there is already Bu coverage for the Feb. 7th meeting? If not, I’m happy to make sure its staffed appropriately.
>
> 2. That’s nice of you. When you have a moment sometime let’s chat about it?
>
> **From:** Daniel Charles Richman [mailto:[redacted] b6 -1,4 b7C -1,4 b7E -3
> **Sent:** Friday, January 06, 2017 12:04 PM
>
> **To:** [redacted](DO) (OGA)[redacted]
> **Subject:** Re: Going Dark Comparative Approaches
>
> Thanks. Just looking at it. Also
>
> 1. I was in touch with Kenn Kern, at DANY who says "The state and local law enforcement community is convening in DC on Feb 7 on encryption. There is a real sense of momentum." He also send me a recent letter to House Judiciary Committee in opposition to their recent Report. See attached.
>
> 2. I checked with Jim Rybicki on your detail status. He said that they "can definitely reup" you. You and I should make sure this doesn't fall thru the cracks
>
> d

On Fri, Jan 6, 2017 at 11:59 AM, [redacted] (DO) (OGA) [redacted] wrote:

b6 -1
b7C -1
b7E -3

We received the international GD legal piece from CRM. I forwarded to you on your FBI email account.

-----Original Message-----
From: Daniel Charles Richman [mailto [redacted]
Sent: Tuesday, January 03, 2017 4:50 PM
To: [redacted] DO) (OGA) [redacted]
Subject: Re: Going Dark Comparative Approaches

b6 -1,4
b7C -1,4
b7E -3

Thx. It's a start. And it's been out since may :(Lovely seeing you

Daniel Richman
Paul J. Kellner Professor of Law
Columbia Law School
Office: [redacted]
Cell: [redacted]

> On Jan 3, 2017, at 4:28 PM, [redacted] (DO) (OGA) [redacted] wrote:
>
>
>
> -----Original Message-----
> From: [redacted] (DO) (OGA)
> Sent: Tuesday, January 03, 2017 4:28 PM
> To: [redacted] (ODAG) (JMD) [redacted]
> Subject: Going Dark Comparative Approaches
>
> You may have already seen this comparative GD report, but featured on USAbook today.
>
> [redacted]
>
>
>
> --
> BEGIN-ANTISPAM-VOTING-LINKS
> --
>
> Teach Email if this mail (ID 01SrVvCfP) is spam:
> Spam: https://antispam.law.columbia.edu/canit/b.php?i=01SrVvCfP&m=6947e7738b93&t=20170103&c=s
> Not spam: https://antispam.law.columbia.edu/canit/b.php?i=01SrVvCfP&m=6947e7738b93&t=20170103&c=n
> Forget vote:
> https://antispam.law.columbia.edu/canit/b.php?i=01SrVvCfP&m=6947e7738b

b6 -1
b7C -1
b7E -3

b6 -1,5
b7C -1,5
b7E -3

> 93&t=20170103&c=f
> ---------------------------- -----------------------
> END-ANTISPAM-VOTING-LINKS
>
> <GD Comparative Approaches.pdf>

--

Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office [redacted]
cellphone [redacted]
You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

Spam
Not spam
Forget previous vote

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office [redacted]
cellphone [redacted]
You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

[redacted] (DO) (OGA)

b6 -1
b7C -1

From: [redacted] (DO) (OGA)
Sent: Saturday, January 07, 2017 10:30 AM
To: Daniel Charles Richman
Subject: Fwd: Reaching out to Dan Richmond

Fyi

....

-------- Original message --------
From: [redacted] (CyD) (FBI)" [redacted]
Date: 01/07/2017 10:04 AM (GMT-05:00)
To: [redacted] (DO) (OGA)" [redacted]
Subject: RE: Reaching out to Dan Richmond

b6 -1
b7C -1
b7E -3

Good idea. I'll send it along ahead of time.

--

-------- Original message --------
From: [redacted] (DO) (OGA)" [redacted]
Date: 01/06/2017 5:30 PM (GMT-05:00)
To: [redacted] CyD) (FBI)" [redacted]
Subject: RE: Reaching out to Dan Richmond

b6 -1
b7C -1
b7E -3

[redacted] perhaps it makes sense to send Dan some read-ahead written material (eg the snow globe slide) to give him an idea of the strategy?

From: Daniel Charles Richman [mailto: [redacted]
Sent: Friday, January 06, 2017 3:56 PM
To: [redacted] (CyD) (FBI) [redacted] (DO) (OGA)
[redacted]
Subject: Re: Reaching out to Dan Richmond

b6 -1,2,4
b7C -1,2,4
b7E -3

Sounds good. Probably my cell is best. [redacted] I'm not sure whether [redacted] wants to be involved, but i'm cc'ing him just in case. In the interim, if there's anything I can read that would make me more helpful (and that can be sent on the low side), please let me know
thx
dan r

On Fri, Jan 6, 2017 at 3:51 PM, [redacted] (CyD) (FBI) [redacted] wrote: b6 -1 b7C -1 b7E -3

> Dan,
>
> Let's plan for Monday at 2:00 p.m. If you provide a number where it's best to reach you, I'll plan to give you a call then.
>
> Best,
> [redacted]
>
> **From:** Daniel Charles Richman [mailto:[redacted] b6 -1,4 b7C -1,4 b7E -3
> **Sent:** Friday, January 06, 2017 11:59 AM
> **To:** [redacted] (CyD) (FBI) [redacted] (DO) (OGA)
> [redacted]
> **Subject:** Re: Reaching out to Dan Richmond
>
> Hi [redacted] I'd love to chat next week and thanks for making time. (And thanks [redacted] for making the connection). I'm particularly flexible next week because classes don't start until the week after. Any times Monday, between 12 & 5; wed 11-6; thurs 2-6; friday 11-3. (I always feel guilty talking about my schedule with people who have real, respectable jobs)
> thx
> dan richman
>
> On Fri, Jan 6, 2017 at 11:32 AM, [redacted] (CyD) (FBI) [redacted] wrote: b6 -1 b7C -1 b7E -3
>
> > Thanks, [redacted]
> >
> > Dan, it's nice to make the connection. As part of the Cyber Director Priority Initiative team stood up by Director Comey, I was happy to hear from [redacted] that you are interested in consulting on the FBI's cyber talent and recruitment challenges. If you have time next week to discuss, I would be happy to make myself available for a call. If so, please let me know a few times that work best for you.
> >
> > Kind regards,
> > [redacted]
> > --
> > [redacted]
> > Cyber Division Executive Staff
> > TDY: CCRSB Presidential Transition and Cyber DPI
> > Federal Bureau of Investigation
> > D: [redacted] M [redacted]
> >
> > -----Original Message-----
> > From: [redacted] (DO) (OGA) b6 -1,4 b7C -1,4 b7E -3,8
> > Sent: Friday, January 06, 2017 11:26 AM
> > To: [redacted] (CyD) (FBI) [redacted]
> > Cc: [redacted] Richman, Daniel C. (DO) (OGA)
> > [redacted] Daniel Charles Richman [redacted]
> > Subject: RE: Reaching out to Dan Richmond

[redacted]

b6 -1
b7C -1

Good idea-- I've cced Dan Richman to schedule a phone call.

[redacted]
-----Original Message-----
From:[redacted](CyD) (FBI)
Sent: Friday, January 06, 2017 11:06 AM
To:[redacted](DO) (OGA)[redacted]
Cc:[redacted]
Subject: Reaching out to Dan Richmond

b6 -1
b7C -1
b7E -3,8

[redacted]

Thanks for suggesting that we reach out to Dan Richmond regarding cyber talent. I know we haven't gotten our projects fully up and running, but I thought it might be worth a Skype session or phone call with Professor Richmond to make the connection. If you have his contact information, or if you would be willing to make introductions, I or a member of our team would be happy to speak with him.

[redacted]
--
[redacted]
Cyber Division Executive Staff
Federal Bureau of Investigation
Office[redacted]
Mobile[redacted]

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office[redacted]
cellphone[redacted]
You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

Spam
Not spam
Forget previous vote

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office[redacted]
[redacted]

b6 -4
b7C -4

cellphone [redacted]
You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

Daniel Charles Richman

From: Daniel Charles Richman
Sent: Saturday, January 07, 2017 10:32 AM
To: [redacted] (DO) (OGA)
Subject: Re: Reaching out to Dan Richmond

b6 -1,4
b7C -1,4

Thx for heads up

Daniel Richman
Paul J. Kellner Professor of Law
Columbia Law School
Office: [redacted]
Cell: [redacted]

On Jan 7, 2017, at 10:30 AM, [redacted] (DO) (OGA) [redacted] wrote:

b6 -1
b7C -1
b7E -3

> Fyi
>
> -------- Original message --------
> From: [redacted] (CyD) (FBI)" [redacted]
> Date: 01/07/2017 10:04 AM (GMT-05:00)
> To: [redacted] (DO) (OGA)" [redacted]
> Subject: RE: Reaching out to Dan Richmond

b6 -1
b7C -1
b7E -3

> Good idea. I'll send it along ahead of time.
>
> -------- Original message --------
> From: [redacted] (DO) (OGA)" [redacted]
> Date: 01/06/2017 5:30 PM (GMT-05:00)
> To: [redacted] (CyD) (FBI)' [redacted]
> Subject: RE: Reaching out to Dan Richmond

b6 -1
b7C -1
b7E -3

[redacted] perhaps it makes sense to send Dan some read-ahead written material (eg the snow globe slide) to give him an idea of the strategy?

From: Daniel Charles Richman [mailto: [redacted]
Sent: Friday, January 06, 2017 3:56 PM

b6 -4
b7C -4

To: [redacted] (CyD) (FBI) [redacted] (DO) (OGA)
[redacted]
Subject: Re: Reaching out to Dan Richmond

b6 -1,2
b7C -1,2
b7E -3

Sounds good. Probably my cell is best. [redacted] I'm not sure whether [redacted] wants to be involved, but i'm cc'ing him just in case. In the interim, if there's anything I can read that would make me more helpful (and that can be sent on the low side), please let me know
thx
dan r

On Fri, Jan 6, 2017 at 3:51 PM, [redacted] (CyD) (FBI)
[redacted] wrote:

b6 -1
b7C -1
b7E -3

> Dan,
>
> Let's plan for Monday at 2:00 p.m. If you provide a number where it's best to reach you, I'll plan to give you a call then.
>
> Best,
> [redacted]
>
> **From:** Daniel Charles Richman [mailto: [redacted]
> **Sent:** Friday, January 06, 2017 11:59 AM
> **To:** [redacted] (CyD) (FBI) [redacted] (DO)
> (OGA) [redacted]
> **Subject:** Re: Reaching out to Dan Richmond
>
> b6 -1,4
> b7C -1,4
> b7E -3
>
> Hi [redacted] - I'd love to chat next week and thanks for making time. (And thanks [redacted] for making the connection). I'm particularly flexible next week because classes don't start until the week after. Any times Monday, between 12 & 5; wed 11-6; thurs 2-6; friday 11-3. (I always feel guilty talking about my schedule with people who have real, respectable jobs)
> thx
> dan richman
>
> On Fri, Jan 6, 2017 at 11:32 AM, [redacted] (CyD) (FBI)
> [redacted] wrote:
>
> b6 -1
> b7C -1
> b7E -3
>
>> Thanks, [redacted]
>>
>> Dan, it's nice to make the connection. As part of the Cyber Director Priority Initiative team stood up by Director Comey, I was happy to hear from [redacted] that you are interested in consulting on the FBI's cyber talent and recruitment challenges. If you have time next week to discuss, I would be happy to make myself available for a call. If so, please let me know a few times that work best for you.
>>
>> Kind regards,
>> [redacted]
>> --
>> [redacted]
>> Cyber Division Executive Staff
>> TDY: CCRSB Presidential Transition and Cyber DPI
>> Federal Bureau of Investigation

D:[redacted] M:[redacted]

b6 -1
b7C -1
b7E -3

----- Original Message-----
From[redacted](DO) (OGA)
Sent: Friday, January 06, 2017 11:26 AM
To:[redacted](CyD) (FBI[redacted]
Cc:[redacted] Richman, Daniel C. (DO) (OGA)
[redacted] Daniel Charles Richman [redacted]
Subject: RE: Reaching out to Dan Richmond

b6 -1,4
b7C -1,4
b7E -3,8

[redacted]

Good idea-- I've cced Dan Richman to schedule a phone call.

[redacted]

----- Original Message-----
From:[redacted](CyD) (FBI)
Sent: Friday, January 06, 2017 11:06 AM
To:[redacted](DO) (OGA[redacted]
Cc:[redacted]
Subject: Reaching out to Dan Richmond

b6 -1
b7C -1
b7E -3,8

[redacted]

Thanks for suggesting that we reach out to Dan Richmond regarding cyber talent. I know we haven't gotten our projects fully up and running, but I thought it might be worth a Skype session or phone call with Professor Richmond to make the connection. If you have his contact information, or if you would be willing to make introductions, I or a member of our team would be happy to speak with him.

[redacted]

--
[redacted]
Cyber Division Executive Staff
Federal Bureau of Investigation
Office:[redacted]
Mobile:[redacted]

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office[redacted]
cellphone[redacted]

b6 -4
b7C -4

> You can download my papers at http://ssrn.com/author=937729
>
> Spam
> Not spam
> Forget previous vote

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office [redacted]
cellphon [redacted]
You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

Spam
Not spam
Forget previous vote

[redacted](DO) (OGA) b6 -1 b7C -1

From: [redacted]DO) (OGA)
Sent: Monday, January 09, 2017 2:03 PM
To: Daniel Charles Richman
Subject: RE: Reaching out to Dan Richmond

Incidentally, passed along the request for MOU changes to OGC. Don't let me forget if you don't hear back from me on this.

From: Daniel Charles Richman [mailto[redacted] b6 -1,4
Sent: Saturday, January 07, 2017 10:32 AM b7C -1,4
To:[redacted](DO) (OGA)[redacted] b7E -3
Subject: Re: Reaching out to Dan Richmond

Thx for heads up

Daniel Richman
Paul J. Kellner Professor of Law
Columbia Law School
Office:[redacted]
Cell:[redacted]

On Jan 7, 2017, at 10:30 AM,[redacted](DO) (OGA[redacted]wrote: b6 -1 b7C -1 b7E -3

> Fyi
>
> --
>
> -------- Original message --------
> From[redacted](CyD) (FBI)"[redacted] b6 -1
> Date: 01/07/2017 10:04 AM (GMT-05:00) b7C -1
> To:[redacted](DO) (OGA)"[redacted] b7E -3
> Subject: RE: Reaching out to Dan Richmond
>
> Good idea. I'll send it along ahead of time.
>
> --
>
> -------- Original message --------
> From:[redacted]DO) (OGA)"[redacted] b6 -1
> Date: 01/06/2017 5:30 PM (GMT-05:00) b7C -1 b7E -3

To: [redacted](CyD) (FBI)'[redacted]
Subject: RE: Reaching out to Dan Richmond

b6 -1
b7C -1
b7E -3

[redacted]perhaps it makes sense to send Dan some read-ahead written material (eg the snow globe slide) to give him an idea of the strategy?

From: Daniel Charles Richman [mailto[redacted]
Sent: Friday, January 06, 2017 3:56 PM
To: [redacted](CyD) (FBI)[redacted](DO) (OGA)
[redacted]
Subject: Re: Reaching out to Dan Richmond

b6 -1,2,4
b7C -1,2,4
b7E -3

Sounds good. Probably my cell is best. [redacted] I'm not sure whether [redacted] wants to be involved, but i'm cc'ing him just in case. In the interim, if there's anything I can read that would make me more helpful (and that can be sent on the low side), please let me know
thx
dan r

On Fri, Jan 6, 2017 at 3:51 PM, [redacted] (CyD) (FBI)
[redacted] wrote:

b6 -1
b7C -1
b7E -3

> Dan,
>
> Let's plan for Monday at 2:00 p.m. If you provide a number where it's best to reach you, I'll plan to give you a call then.
>
> Best,
> [redacted]
>
> **From:** Daniel Charles Richman [mailto[redacted]
> **Sent:** Friday, January 06, 2017 11:59 AM
> **To:** [redacted](CyD) (FBI)[redacted](DO)
> (OGA) [redacted]
> **Subject:** Re: Reaching out to Dan Richmond
>
> b6 -1,4
> b7C -1,4
> b7E -3
>
> Hi [redacted] I'd love to chat next week and thanks for making time. (And thanks [redacted], for making the connection). I'm particularly flexible next week because classes don't start until the week after. Any times Monday, between 12 & 5; wed 11-6; thurs 2-6; friday 11-3. (I always feel guilty talking about my schedule with people who have real, respectable jobs)
> thx
> dan richman
>
> On Fri, Jan 6, 2017 at 11:32 AM, [redacted] (CyD) (FBI)
> [redacted] wrote:
>
> b6 -1
> b7C -1
> b7E -3
>
>> Thanks, [redacted]
>>
>> Dan, it's nice to make the connection. As part of the Cyber Director Priority Initiative team stood up by Director Comey, I was happy to hear from [redacted] that you are interested in consulting on the FBI's cyber talent and recruitment challenges. If you have time next week to discuss, I would be happy to make myself available for a call. If so, please let me know a few times that work best for you.

Kind regards,
[redacted]
--
[redacted]
Cyber Division Executive Staff
TDY: CCRSB Presidential Transition and Cyber DPI
Federal Bureau of Investigation
D:[redacted] | M:[redacted]

b6 -1
b7C -1
b7E -3

----- Original Message -----
From:[redacted](DO) (OGA)
Sent: Friday, January 06, 2017 11:26 AM
To:[redacted](CyD) (FBI)[redacted]
Cc:[redacted]Richman, Daniel C. (DO) (OGA)
[redacted]Daniel Charles Richman[redacted]
Subject: RE: Reaching out to Dan Richmond

b6 -1,4
b7C -1,4
b7E -3,8

[redacted]

Good idea-- I've cced Dan Richman to schedule a phone call.

[redacted]
----- Original Message -----
From:[redacted](CyD) (FBI)
Sent: Friday, January 06, 2017 11:06 AM
To:[redacted] (DO) (OGA)[redacted]
Cc:[redacted]
Subject: Reaching out to Dan Richmond

b6 -1
b7C -1
b7E -3,8

[redacted]

Thanks for suggesting that we reach out to Dan Richmond regarding cyber talent. I know we haven't gotten our projects fully up and running, but I thought it might be worth a Skype session or phone call with Professor Richmond to make the connection. If you have his contact information, or if you would be willing to make introductions, I or a member of our team would be happy to speak with him.

[redacted]
--
[redacted]
Cyber Division Executive Staff
Federal Bureau of Investigation
Office[redacted]
Mobile[redacted]

> --
> Daniel Richman
> Paul J. Kellner Professor of Law,
> Columbia Law School
> office[redacted] b6 -4
> cellphone[redacted] b7C -4
> You can download my papers at http://ssrn.com/author=937729
>
> Spam
> Not spam
> Forget previous vote

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office[redacted] b6 -4
cellphone[redacted] b7C -4
You can download my papers at http://ssrn.com/author=937729

Spam
Not spam
Forget previous vote

Daniel Charles Richman

From: Daniel Charles Richman
Sent: Monday, January 09, 2017 6:44 PM
To: [redacted](DO) (OGA)
Subject: Re: [redacted]

b6 -1,2
b7C -1,2

oh good. I was thinking of sending it to you directly. As you'll recall, law rev editing schedules are complicated and this one is kinda in flux, because of a number of [redacted] I suspect that, now that [redacted] piece has arrived, the CLR editors will be working on it for several weeks (perhaps longer). Then it will go back to [redacted]

Given that, notwithstanding his rough treatment of the D, [redacted] is a truly nice guy and generally gets high marks for academic integrity, I think we have, and should use, several avenues: If he's gotten anything wrong, or is quoting any D speech really out of context, tell me and I will suggest to him that he fix it. I will also tell the law rev eds. If you have substantive criticisms, I'll bet [redacted] will also consider them, and if rejects them, I will think about using them in the piece I'm writing with [redacted]

b6 -2
b7C -2

On Mon, Jan 9, 2017 at 6:36 PM, [redacted] (DO) (OGA) [redacted] wrote:

> D passed along the [redacted] article. Just curious what the timeline would be to get any suggestions/edits to you ?
>
> [redacted]

b6 -1,2
b7C -1,2
b7E -3

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office [redacted]
cellphone [redacted]
You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

[redacted](DO) (OGA) b6 -1,2 b7C -1,2

From: [redacted](DO) (OGA)
Sent: Monday, January 09, 2017 7:40 AM
To: [redacted] (DO) (FBI)
Subject: FW: negative take on your policing speeches
Attachments: [redacted]on Crime -- Columbia Law Review.docx

Fyi, as discussed.

From: James B. Comey
Sent: Saturday, January 07, 2017 3:57 PM
To:[redacted](DO) (OGA)[redacted] b6 -1
Cc: Rybicki, James E. (DO) (FBI)[redacted] b7C -1
Subject: Fwd: negative take on your policing speeches b7E -3

Take a look at this and let me know yiur thoughts next week. Thanks.

-------- Original message --------
From:[redacted] b6 -1
Date: 1/7/17 3:47 PM (GMT-05:00) b7C -1
To: "James B. Comey" <jcb.dir@ic.fbi.gov>
Subject: Fwd: negative take on your policing speeches

---------- Forwarded message ---------
From: Daniel Charles Richman [redacted] b6 -1,2,4
Date: Sat, Jan 7, 2017 at 3:39 PM b7C -1,2,4
Subject: negative take on your policing speeches
To: Jbc [redacted]

I realize that you've got plenty of other stuff on your mind. But you ought to know about (if only to pass on to others) about the attached first draft that[redacted]just submitted to the CLRev as part of the "minisymposium" on the murder spike that I mentioned to you. [redacted]is OK with my sending it to you). [redacted]and is one of the most respected law & econ people writing about crime. So this is likely to get decent play within academia. And as you can see it has some quite hostile aspects, coming down hard on your de-policing musings, even as giving you credit for noting the homicide spike.

GIven the tight nature of law review deadlines (this will come out in June but you know law rev lead times) and the likelihood that you and your crew have plenty on your plates, I'm not suggesting that you consider a response (tho if you really wanted to do that, I could try to facilitate it). But if[redacted]has made factual errors in b6 -2 b7C -2 characterizing your position, we should try to point them out. And at the very least, your crew might consider some of his analysis going forward.

Daniel Charles Richman

From: Daniel Charles Richman
Sent: Monday, January 09, 2017 6:46 PM
To: [redacted] (DO) (OGA) b6 -1,2
Subject: Re: [redacted] b7C -1,2

forgot the last option - In addition to all the others, I'm sure the CLR would find room for a short pithy statement from the D (i.e. you) :)

On Mon, Jan 9, 2017 at 6:43 PM, Daniel Charles Richman [redacted] wrote: b6 -2,4

> oh good. I was thinking of sending it to you directly. As you'll recall, law rev editing schedules are complicated and this one is kinda in flux, because of a number of [redacted] I suspect that, now that [redacted] piece has arrived, the CLR editors will be working on it for several weeks (perhaps longer). Then it will go back to [redacted] b7C -2,4
>
> Given that, notwithstanding his rough treatment of the D, [redacted] is a truly nice guy and generally gets high marks for academic integrity, I think we have, and should use, several avenues: if he's gotten anything wrong, or is quoting any D speech really out of context, tell me and I will suggest to him that he fix it. I will also tell the law rev eds. If you have substantive criticisms, I'll bet [redacted] will also consider them, and if rejects them, I will think about using them in the piece I'm writing with [redacted] [redacted] b6 -2 b7C -2
>
> On Mon, Jan 9, 2017 at 6:36 PM, [redacted] (DO) (OGA) [redacted] wrote: b6 -1,2 b7C -1,2 b7E -3
>
> > D passed along the [redacted] article. Just curious what the timeline would be to get any suggestions/edits to you ?
> >
> > [redacted]
>
> --
> Daniel Richman
> Paul J. Kellner Professor of Law,
> Columbia Law School
> office [redacted] b6 -4
> cellphone [redacted] b7C -4
> You can download my papers at http://ssrn.com/author=937729

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office [redacted] b6 -4
cellphone [redacted] b7C -4

You can download my papers at: http://ssrn.com/author=937729

[redacted] (DO) (OGA)

b6 -1,2
b7C -1,2

From: [redacted] (DO) (OGA)
Sent: Monday, January 09, 2017 6:47 PM
To: Daniel Charles Richman
Subject: RE: [redacted]

I'm glad you sent it to the D first (takes the burden off me to "pitch" it as a project).

I'm taking a look through, although it's obviously relatively lengthy.

And let's hope it doesn't come to that!

From: Daniel Charles Richman [mailto [redacted]
Sent: Monday, January 09, 2017 6:46 PM
To: [redacted] (DO) (OGA) [redacted]
Subject: Re: [redacted]

b6 -1,2
b7C -1,2
b7E -3

forgot the last option - In addition to all the others, I'm sure the CLR would find room for a short pithy statement from the D (i.e. you) :)

On Mon, Jan 9, 2017 at 6:43 PM, Daniel Charles Richman [redacted] wrote:

b6 -2,4
b7C -2,4

> oh good. I was thinking of sending it to you directly. As you'll recall, law rev editing schedules are complicated and this one is kinda in flux, because of a number of [redacted] I suspect that, now that [redacted] piece has arrived, the CLR editors will be working on it for several weeks (perhaps longer). Then it will go back to [redacted]
>
> Given that, notwithstanding his rough treatment of the D [redacted] is a truly nice guy and generally gets high marks for academic integrity, I think we have, and should use, several avenues: If he's gotten anything wrong, or is quoting any D speech really out of context, tell me and I will suggest to him that he fix it. I will also tell the law rev eds. If you have substantive criticisms, I'll be [redacted] will also consider them, and if rejects them, I will think about using them in the piece I'm writing with [redacted]
>
> b6 -2
> b7C -2
>
> On Mon, Jan 9, 2017 at 6:36 PM, [redacted] (DO) (OGA) [redacted] wrote:
>
> b6 -1,2
> b7C -1,2
> b7E -3
>
>> D passed along the [redacted] article. Just curious what the timeline would be to get any suggestions/edits to you ?
>>
>> [redacted]
>
> --
> Daniel Richman
> Paul J. Kellner Professor of Law,

> Columbia Law School
> office [redacted]
> cellphone [redacted]
> You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office [redacted]
cellphone [redacted]
You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

Daniel Charles Richman

From:	Daniel Charles Richman
Sent:	Wednesday, January 11, 2017 6:53 PM
To:	[redacted]
Cc:	[redacted] (DO) (OGA)
Subject:	GD post

b6 -1,5
b7C -1,5

Hi [redacted] (and cc'ing [redacted] -- I've just been told that the D has decided that GD requires an internal Bu candidate at a senior level who'll be able to stick with the effort for some time. That means that his brilliant idea to dragoon you won't work. None of this takes away from the fact that you're a Great American to even consider taking on this mission. So thanks so much for your willingness.
Let's talk soon
dan r

[redacted] (DO) (OGA)

b6 -1,2
b7C -1,2

From: [redacted] (DO) (OGA)
Sent: Thursday, January 12, 2017 8:09 AM
To: Daniel Charles Richman
Subject: RE: [redacted]

Still reviewing this, but wanted to make sure you (and your editors) were aware of a Pew Survey that came out this week on this issue:

http://www.usatoday.com/story/news/2017/01/11/ferguson-effect-study-72-us-cops-reluctant-make-stops/96446504/

http://www.pewsocialtrends.org/2017/01/11/behind-the-badge/

From: [redacted] (DO) (OGA)
Sent: Monday, January 09, 2017 6:47 PM
To: 'Daniel Charles Richman' [redacted]
Subject: RE: [redacted]

b6 -1,2,4
b7C -1,2,4

I'm glad you sent it to the D first (takes the burden off me to "pitch" it as a project).

I'm taking a look through, although it's obviously relatively lengthy.

And let's hope it doesn't come to that!

From: Daniel Charles Richman [mailto [redacted]
Sent: Monday, January 09, 2017 6:46 PM
To: [redacted] (DO) (OGA) [redacted]
Subject: Re: [redacted]

b6 -1,2,4
b7C -1,2,4
b7E -3

forgot the last option - In addition to all the others, I'm sure the CLR would find room for a short pithy statement from the D (i.e. you) :)

On Mon, Jan 9, 2017 at 6:43 PM, Daniel Charles Richman [redacted] wrote:

b6 -2,4
b7C -2,4

> oh good. I was thinking of sending it to you directly. As you'll recall, law rev editing schedules are complicated and this one is kinda in flux, because of a number of [redacted] I suspect that, now that [redacted] piece has arrived, the CLR editors will be working on it for several weeks (perhaps longer). Then it will go back to [redacted]
>
> Given that, notwithstanding his rough treatment of the D, [redacted] is a truly nice guy and generally gets high marks for academic integrity, I think we have, and should use, several avenues: If he's gotten anything wrong, or is quoting any D speech really out of context, tell me and I will suggest to him that he fix it. I will also tell the law rev eds. If you have substantive criticisms, I'll bet [redacted] will also consider them, and if rejects them, I will think about using them in the piece I'm writing with [redacted].

b6 -2
b7C -2

> On Mon, Jan 9, 2017 at 6:36 PM, [redacted] (DO) (OGA) [redacted] wrote:
>
> > D passed along the [redacted] article. Just curious what the timeline would be to get any suggestions/edits to you ?
> >
> > [redacted]
>
> --
> Daniel Richman
> Paul J. Kellner Professor of Law,
> Columbia Law School
> office [redacted]
> cellphone [redacted]
> You can download my papers at http://ssrn.com/author=937729

b6 -1,2
b7C -1,2
b7E -3

b6 -4
b7C -4

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office [redacted]
cellphone [redacted]
You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

[redacted](DO) (OGA) b6 -1,5 b7C -1,5

From: [redacted](DO) (OGA)
Sent: Wednesday, January 11, 2017 9:22 PM
To: Daniel Charles Richman; [redacted]
Subject: RE: GD post

Sorry this didn't work out [redacted] the Bu would have been very lucky to have you. Thanks for being open to it, though, and hope we can talk soon as well.

...

-------- Original message --------
From: Daniel Charles Richman [redacted] b6 -1,5 b7C -1,5 b7E -3
Date: 01/11/2017 6:52 PM (GMT-05:00)
To: [redacted]
Cc: "[redacted](DO) (OGA)" [redacted]
Subject: GD post

Hi [redacted] (and cc'ing [redacted] - I've just been told that the D has decided that GD requires an internal Bu candidate at a senior level who'll be able to stick with the effort for some time. That means that his brilliant idea to dragoon you won't work. None of this takes away from the fact that you're a Great American to even consider taking on this mission. So thanks so much for your willingness.
Let's talk soon
dan r

Daniel Charles Richman

From: Daniel Charles Richman
Sent: Thursday, January 12, 2017 8:18 AM
To: [redacted] (DO) (OGA)
Subject: Re: [redacted]

b6 -1,2,4
b7C -1,2,4

I am indeed reading and will use in my piece. Meanwhile editors have suggested many cuts in [redacted] nastiness

Daniel Richman
Paul J. Kellner Professor of Law
Columbia Law School
Office: [redacted]
Cell: [redacted]

On Jan 12, 2017, at 8:08 AM, [redacted] (DO) (OGA) [redacted] wrote:

b6 -1
b7C -1
b7E -3

> Still reviewing this, but wanted to make sure you (and your editors) were aware of a Pew Survey that came out this week on this issue:
>
> http://www.usatoday.com/story/news/2017/01/11/ferguson-effect-study-72-us-cops-reluctant-make-stops/96446504/
>
> http://www.pewsocialtrends.org/2017/01/11/behind-the-badge/
>
> **From:** [redacted] (DO) (OGA)
> **Sent:** Monday, January 09, 2017 6:47 PM
> **To:** 'Daniel Charles Richman' [redacted]
> **Subject:** RE: [redacted]
>
> I'm glad you sent it to the D first (takes the burden off me to "pitch" it as a project).
>
> I'm taking a look through, although it's obviously relatively lengthy.
>
> And let's hope it doesn't come to that!
>
> **From:** Daniel Charles Richman [mailto: [redacted]
> **Sent:** Monday, January 09, 2017 6:46 PM
> **To:** [redacted] (DO) (OGA) [redacted]
> **Subject:** Re: [redacted]
>
> forgot the last option - In addition to all the others, I'm sure the CLR would find room for a short pithy statement from the D (i.e. you) :)
>
> On Mon, Jan 9, 2017 at 6:43 PM, Daniel Charles Richman [redacted] wrote:

b6 -1,2,4
b7C -1,2,4

b6 -1,2,4
b7C -1,2,4
b7E -3

> oh good. I was thinking of sending it to you directly. As you'll recall, law rev editing schedules are complicated and this one is kinda in flux, because of a number of [redacted] I suspect that, now that [redacted] piece has arrived, the CLR editors will be working on it for several weeks (perhaps longer). Then it will go back to [redacted]
>
> Given that, notwithstanding his rough treatment of the D, [redacted] is a truly nice guy and generally gets high marks for academic integrity, I think we have, and should use, several avenues: If he's gotten anything wrong, or is quoting any D speech really out of context, tell me and I will suggest to him that he fix it. I will also tell the law rev eds. If you have substantive criticisms, I'll bet [redacted] will also consider them, and if rejects them, I will think about using them in the piece I'm writing with [redacted]
>
> On Mon, Jan 9, 2017 at 6:36 PM, [redacted] (DO) (OGA) [redacted] wrote:
>
>> D passed along the [redacted] article. Just curious what the timeline would be to get any suggestions/edits to you ?
>>
>> [redacted]
>
> --
> Daniel Richman
> Paul J. Kellner Professor of Law,
> Columbia Law School
> office [redacted]
> cellphone [redacted]
> You can download my papers at http://ssrn.com/author=937729

b6 -2
b7C -2

b6 -2
b7C -2

b6 -1,2
b7C -1,2
b7E -3

b6 -4
b7C -4

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office [redacted]
cellphone [redacted]
You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

Spam
Not spam
Forget previous vote

[redacted] (DO) (OGA)

b6 -1,2
b7C -1,2

From: [redacted] (DO) (OGA)
Sent: Thursday, January 12, 2017 10:00 AM
To: Daniel Charles Richman
Subject: RE: [redacted]

Great let's touch base on this later today if you have a moment?

From: Daniel Charles Richman [mailto[redacted]
Sent: Thursday, January 12, 2017 8:18 AM
To: [redacted] (DO) (OGA) [redacted]
Subject: Re [redacted]

b6 -1,2,4
b7C -1,2,4
b7E -3

I am indeed reading and will use in my piece. Meanwhile editors have suggested many cuts in [redacted] nastiness

Daniel Richman
Paul J. Kellner Professor of Law
Columbia Law School
Office: [redacted]
Cell [redacted]

On Jan 12, 2017, at 8:08 AM, [redacted] (DO) (OGA) [redacted] wrote:

b6 -1
b7C -1
b7E -3

> Still reviewing this, but wanted to make sure you (and your editors) were aware of a Pew Survey that came out this week on this issue:
>
> http://www.usatoday.com/story/news/2017/01/11/ferguson-effect-study-72-us-cops-reluctant-make-stops/96446504/
>
> http://www.pewsocialtrends.org/2017/01/11/behind-the-badge/
>
> **From:** [redacted] (DO) (OGA)
> **Sent:** Monday, January 09, 2017 6:47 PM
> **To:** 'Daniel Charles Richman' [redacted]
> **Subject:** RE: [redacted]
>
> I'm glad you sent it to the D first (takes the burden off me to "pitch" it as a project).
>
> I'm taking a look through, although it's obviously relatively lengthy.
>
> And let's hope it doesn't come to that!
>
> **From:** Daniel Charles Richman [mailto [redacted]
> **Sent:** Monday, January 09, 2017 6:46 PM
> **To:** [redacted] (DO) (OGA) [redacted]

b6 -1,2,4
b7C -1,2,4

b6 -1,4
b7C -1,4
b7E -3

To: [redacted] DO) (OGA) [redacted] b6 -1,2
Subject: Re [redacted] b7C -1,2
b7E -3

forgot the last option - In addition to all the others, I'm sure the CLR would find room for a short pithy statement from the D (i.e. you) :)

On Mon, Jan 9, 2017 at 6:43 PM, Daniel Charles Richman [redacted] wrote: b6 -2,4 b7C -2,4

> oh good. I was thinking of sending it to you directly. As you'll recall, law rev editing schedules are complicated and this one is kinda in flux, because of a number of [redacted] I suspect that, now that [redacted] piece has arrived, the CLR editors will be working on it for several weeks (perhaps longer). Then it will go back to [redacted]
>
> Given that, notwithstanding his rough treatment of the D, [redacted] is a truly nice guy and generally gets high marks for academic integrity, I think we have, and should use, several avenues: If he's gotten anything wrong, or is quoting any D speech really out of context, tell me and I will suggest to him that he fix it. I will also tell the law rev eds. If you have substantive criticisms, I'll bet [redacted] will also consider them, and if rejects them, I will think about using them in the piece I'm writing with [redacted] b6 -2 b7C -2
>
> On Mon, Jan 9, 2017 at 6:36 PM, [redacted] (DO) (OGA) [redacted] wrote: b6 -1,2 b7C -1,2 b7E -3
>
>> D passed along the [redacted] article. Just curious what the timeline would be to get any suggestions/edits to you ?
>>
>> [redacted]
>
> --
> Daniel Richman
> Paul J. Kellner Professor of Law,
> Columbia Law School
> office [redacted] b6 -4
> cellphone [redacted] b7C -4
> You can download my papers at http://ssrn.com/author=937729

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office [redacted] b6 -4
cellphone [redacted] b7C -4
You can download my papers at http://ssrn.com/author=937729

Spam
Not spam
Forget previous vote

Daniel Charles Richman

From: Daniel Charles Richman
Sent: Thursday, January 12, 2017 11:21 AM
To: [redacted] (DO) (OGA)
Subject: Re: [redacted]

b6 -1,2,4
b7C -1,2,4

I'll call around 2:30 if that's ok

Daniel Richman
Paul J. Kellner Professor of Law
Columbia Law School
Office: [redacted]
Cell: [redacted]

On Jan 12, 2017, at 10:00 AM [redacted] (DO) (OGA) [redacted] wrote:

b6 -1
b7C -1
b7E -3

> Great let's touch base on this later today if you have a moment?
>
> **From:** Daniel Charles Richman [mailto: [redacted]
> **Sent:** Thursday, January 12, 2017 8:18 AM
> **To:** [redacted] (DO) (OGA) [redacted]
> **Subject:** Re: [redacted]
>
> b6 -1,2,4
> b7C -1,2,4
> b7E -3
>
> I am indeed reading and will use in my piece. Meanwhile editors have suggested many cuts in [redacted] nastiness
>
> Daniel Richman
> Paul J. Kellner Professor of Law
> Columbia Law School
> Office: [redacted]
> Cell: [redacted]
>
> On Jan 12, 2017, at 8:08 AM, [redacted] (DO) (OGA) [redacted] wrote:
>
> b6 -1
> b7C -1
> b7E -3
>
>> Still reviewing this, but wanted to make sure you (and your editors) were aware of a Pew Survey that came out this week on this issue:
>>
>> http://www.usatoday.com/story/news/2017/01/11/ferguson-effect-study-72-us-cops-reluctant-make-stops/96446504/
>>
>> http://www.pewsocialtrends.org/2017/01/11/behind-the-badge/
>>
>> **From:** [redacted] (DO) (OGA)
>> **Sent:** Monday, January 09, 2017 6:47 PM
>> **To:** 'Daniel Charles Richman' [redacted]
>>
>> b6 -1,4
>> b7C -1,4

Subject: RE: [redacted] b6 -2 b7C -2

I'm glad you sent it to the D first (takes the burden off me to "pitch" it as a project).

I'm taking a look through, although it's obviously relatively lengthy.

And let's hope it doesn't come to that!

From: Daniel Charles Richman [mailto:[redacted] b6 -1,4 b7C -1,4 b7E -3
Sent: Monday, January 09, 2017 6:46 PM
To: [redacted] (DO) (OGA) [redacted]
Subject: Re: Donhue

forgot the last option - In addition to all the others, I'm sure the CLR would find room for a short pithy statement from the D (i.e. you) :)

On Mon, Jan 9, 2017 at 6:43 PM, Daniel Charles Richman
[redacted] wrote: b6 -2,4 b7C -2,4

> oh good. I was thinking of sending it to you directly. As you'll recall, law rev editing schedules are complicated and this one is kinda in flux, because of a number of [redacted] I suspect that, now that [redacted] piece has arrived, the CLR editors will be working on it for several weeks (perhaps longer). Then it will go back to [redacted]
>
> Given that, notwithstanding his rough treatment of the D, [redacted] is a truly nice guy and generally gets high marks for academic integrity, I think we have, and should use, several avenues: If he's gotten anything wrong, or is quoting any D speech really out of context, tell me and I will suggest to him that he fix it. I will also tell the law rev eds. If you have substantive criticisms, I'll bet [redacted] will also consider them, and if rejects them, I will think about using them in the piece I'm writing with [redacted] b6 -2 b7C -2
>
> On Mon, Jan 9, 2017 at 6:36 PM, [redacted] (DO) (OGA)
> [redacted] wrote: b6 -1,2 b7C -1,2 b7E -3
>
> > D passed along the [redacted] article. Just curious what the timeline would be to get any suggestions/edits to you ?
> >
> > [redacted]
>
> --
> Daniel Richman
> Paul J. Kellner Professor of Law,
> Columbia Law School
> office [redacted]
> cellphone [redacted] b6 -4 b7C -4
> You can download my papers at http://ssrn.com/author=937729

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office [redacted]
cellphone [redacted]
You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

Spam
Not spam
Forget previous vote

[redacted] (DO) (OGA)

b6 -1,2
b7C -1,2

From: [redacted] (DO) (OGA)
Sent: Thursday, January 12, 2017 12:17 PM
To: Daniel Charles Richman
Subject: RE: [redacted]

Cornyn is currently asking Pompeo about the Ferguson effect.

From: Daniel Charles Richman [mailto [redacted]
Sent: Thursday, January 12, 2017 11:21 AM
To: [redacted] (DO) (OGA) [redacted]
Subject: Re: [redacted]

b6 -1,2,4
b7C -1,2,4
b7E -3

I'll call around 2:30 if that's ok

Daniel Richman
Paul J. Kellner Professor of Law
Columbia Law School
Office: [redacted]
Cell: [redacted]

On Jan 12, 2017, at 10:00 AM, [redacted] (DO) (OGA) [redacted] wrote:

> Great let's touch base on this later today if you have a moment?
>
> ---
>
> **From:** Daniel Charles Richman [mailto [redacted]
> **Sent:** Thursday, January 12, 2017 8:18 AM
> **To:** [redacted] DO) (OGA) [redacted]
> **Subject:** Re: [redacted]
>
> b6 -1,2,4
> b7C -1,2,4
> b7E -3
>
> I am indeed reading and will use in my piece. Meanwhile editors have suggested many cuts in [redacted] nastiness
>
> Daniel Richman
> Paul J. Kellner Professor of Law
> Columbia Law School
> Office: [redacted]
> Cell: [redacted]
>
> On Jan 12, 2017, at 8:08 AM, [redacted] (DO) (OGA) [redacted] wrote:
>
> b6 -1
> b7C -1
> b7E -3
>
>> Still reviewing this, but wanted to make sure you (and your editors) were aware of a Pew Survey that came out this week on this issue:
>>
>> http://www.usatoday.com/story/news/2017/01/11/ferguson-effect-study-72-us-cops-reluctant-make-stops/96446504/

http://www.pewsocialtrends.org/2017/01/11/behind-the-badge/

From: [redacted] (DO) (OGA)
Sent: Monday, January 09, 2017 6:47 PM
To: 'Daniel Charles Richman' [redacted]
Subject: RE [redacted]

b6 -1,2,4
b7C -1,2,4

I'm glad you sent it to the D first (takes the burden off me to "pitch" it as a project).

I'm taking a look through, although it's obviously relatively lengthy.

And let's hope it doesn't come to that!

From: Daniel Charles Richman [mailto [redacted]
Sent: Monday, January 09, 2017 6:46 PM
To: [redacted] (DO) (OGA) [redacted]
Subject: Re: [redacted]

b6 -1,2,4
b7C -1,2,4
b7E -3

forgot the last option - In addition to all the others, I'm sure the CLR would find room for a short pithy statement from the D (i.e. you) :)

On Mon, Jan 9, 2017 at 6:43 PM, Daniel Charles Richman [redacted] wrote:

b6 -2,4
b7C -2,4

> oh good. I was thinking of sending it to you directly. As you'll recall, law rev editing schedules are complicated and this one is kinda in flux, because of a number of [redacted] I suspect that, now that [redacted] piece has arrived, the CLR editors will be working on it for several weeks (perhaps longer). Then it will go back to [redacted]
>
> Given that, notwithstanding his rough treatment of the D, [redacted] is a truly nice guy and generally gets high marks for academic integrity, I think we have, and should use, several avenues: If he's gotten anything wrong, or is quoting any D speech really out of context, tell me and I will suggest to him that he fix it. I will also tell the law rev eds. If you have substantive criticisms, I'll bet [redacted] will also consider them, and if rejects them, I will think about using them in the piece I'm writing with [redacted]
>
> b6 -2
> b7C -2
>
> On Mon, Jan 9, 2017 at 6:36 PM, [redacted] (DO) (OGA) [redacted] wrote:
>
> b6 -1,2
> b7C -1,2
> b7E -3
>
>> D passed along the [redacted] article. Just curious what the timeline would be to get any suggestions/edits to you ?
>>
>> [redacted]

> Daniel Richman
> Paul J. Kellner Professor of Law,
> Columbia Law School
> office [redacted]
> cellphone [redacted]
> You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office [redacted]
cellphone [redacted]
You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

Spam
Not spam
Forget previous vote

Daniel Charles Richman

From: Daniel Charles Richman
Sent: Thursday, January 12, 2017 12:23 PM
To: [redacted](DO) (OGA)
Subject: Re: [redacted]

b6 -1,2,4
b7C -1,2,4

Too much Homeland watching makes people forget that CIA stays abroad

Daniel Richman
Paul J. Kellner Professor of Law
Columbia Law School
Office:[redacted]
Cell[redacted]

On Jan 12, 2017, at 12:17 PM, [redacted](DO) (OGA)[redacted]wrote:

b6 -1
b7C -1
b7E -3

> Cornyn is currently asking Pompeo about the Ferguson effect.
>
> ---
>
> **From:** Daniel Charles Richman [mailto[redacted]
> **Sent:** Thursday, January 12, 2017 11:21 AM
> **To:** [redacted](DO) (OGA)[redacted]
> **Subject:** Re: [redacted]
>
> b6 -1,2,4
> b7C -1,2,4
> b7E -3
>
> I'll call around 2:30 if that's ok
>
> Daniel Richman
> Paul J. Kellner Professor of Law
> Columbia Law School
> Office:[redacted]
> Cell:[redacted]
>
> On Jan 12, 2017, at 10:00 AM, [redacted](DO) (OGA[redacted]
> wrote:
>
> b6 -1
> b7C -1
> b7E -3
>
>> Great let's touch base on this later today if you have a moment?
>>
>> ---
>>
>> **From:** Daniel Charles Richman [mailto[redacted]
>> **Sent:** Thursday, January 12, 2017 8:18 AM
>> **To:**[redacted](DO) (OGA)[redacted]
>> **Subject:** Re[redacted]
>>
>> b6 -1,2,4
>> b7C -1,2,4
>> b7E -3
>>
>> I am indeed reading and will use in my piece. Meanwhile editors have suggested many cuts in[redacted]nastiness
>>
>> Daniel Richman
>> Paul J. Kellner Professor of Law

Columbia Law School
Office:[redacted]
Cell[redacted]

b6 -1,4
b7C -1,4
b7E -3

On Jan 12, 2017, at 8:08 AM, [redacted](DO) (OGA)
[redacted] wrote:

> Still reviewing this, but wanted to make sure you (and your editors) were aware of a Pew Survey that came out this week on this issue:
>
> http://www.usatoday.com/story/news/2017/01/11/ferguson-effect-study-72-us-cops-reluctant-make-stops/96446504/
>
> http://www.pewsocialtrends.org/2017/01/11/behind-the-badge/
>
> ---
>
> **From:**[redacted](DO) (OGA)
> **Sent:** Monday, January 09, 2017 6:47 PM
> **To:** 'Daniel Charles Richman' [redacted]
> **Subject:** RE:[redacted]

b6 -1,2,4
b7C -1,2,4

> I'm glad you sent it to the D first (takes the burden off me to "pitch" it as a project).
>
> I'm taking a look through, although it's obviously relatively lengthy.
>
> And let's hope it doesn't come to that!
>
> **From:** Daniel Charles Richman [mailto[redacted]
> **Sent:** Monday, January 09, 2017 6:46 PM
> **To:**[redacted]DO) (OGA)[redacted]
> **Subject:** Re:[redacted]

b6 -1,2,4
b7C -1,2,4
b7E -3

> forgot the last option - In addition to all the others, I'm sure the CLR would find room for a short pithy statement from the D (i.e. you) :)
>
> On Mon, Jan 9, 2017 at 6:43 PM, Daniel Charles Richman
> [redacted] wrote:

b6 -2,4
b7C -2,4

>> oh good. I was thinking of sending it to you directly. As you'll recall, law rev editing schedules are complicated and this one is kinda in flux, because of a number of[redacted] I suspect that, now that[redacted]piece has arrived, the CLR editors will be working on it for several weeks (perhaps longer). Then it will go back to [redacted]
>>
>> Given that, notwithstanding his rough treatment of the D,[redacted]is a truly nice guy and generally gets high marks for academic integrity, I think we have, and should use, several avenues: If he's gotten anything wrong, or is quoting any D speech really out of context, tell me and I will suggest to him that he fix it. I will also tell the law rev

b6 -2
b7C -2

> eds. If you have substantive criticisms, I'll bet [redacted] will also consider them, and if rejects them, I will think about using them in the piece I'm writing with [redacted]
>
> b6 -2
> b7C -2
>
> On Mon, Jan 9, 2017 at 6:36 PM [redacted] (DO) (OGA) [redacted] wrote:
>
> b6 -1,2
> b7C -1,2
>
> > D passed along the [redacted] article. Just curious what the timeline would be to get any suggestions/edits to you ?
> >
> > [redacted]
>
> --
> Daniel Richman
> Paul J. Kellner Professor of Law,
> Columbia Law School
> office [redacted]
> cellphone [redacted]
> You can download my papers at http://ssrn.com/author=937729
>
> b6 -4
> b7C -4

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office [redacted]
cellphone [redacted]
You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

Spam
Not spam
Forget previous vote

[redacted] (DO) (OGA)

b6 -1,2
b7C -1,2
b7E -3

From: [redacted] (DO) (OGA)
Sent: Thursday, January 12, 2017 12:32 PM
To: Daniel Charles Richman
Subject: RE:[redacted]

That should work.

[redacted]
Special Counsel to the Director
Federal Bureau of Investigation
[redacted]

From: Daniel Charles Richman [mailto[redacted]
Sent: Thursday, January 12, 2017 11:21 AM
To:[redacted] (DO) (OGA) [redacted]
Subject: Re:[redacted]

b6 -1,2,4
b7C -1,2,4
b7E -3

I'll call around 2:30 if that's ok

Daniel Richman
Paul J. Kellner Professor of Law
Columbia Law School
Office:[redacted]
Cell[redacted]

On Jan 12, 2017, at 10:00 AM,[redacted] (DO) (OGA) [redacted] wrote:

b6 -1
b7C -1
b7E -3

> Great let's touch base on this later today if you have a moment?
>
> ---
>
> **From:** Daniel Charles Richman [mailto[redacted]
> **Sent:** Thursday, January 12, 2017 8:18 AM
> **To:**[redacted] (DO) (OGA)[redacted]
> **Subject:** Re:[redacted]
>
> b6 -1,2,4
> b7C -1,2,4
> b7E -3
>
> I am indeed reading and will use in my piece. Meanwhile editors have suggested many cuts in [redacted] nastiness
>
> Daniel Richman
> Paul J. Kellner Professor of Law
> Columbia Law School
> Office:[redacted]
> Cell:[redacted]
>
> On Jan 12, 2017, at 8:08 AM,[redacted] (DO) (OGA) [redacted]

wrote:

Still reviewing this, but wanted to make sure you (and your editors) were aware of a Pew Survey that came out this week on this issue:

http://www.usatoday.com/story/news/2017/01/11/ferguson-effect-study-72-us-cops-reluctant-make-stops/96446504/

http://www.pewsocialtrends.org/2017/01/11/behind-the-badge/

From: [redacted]DO) (OGA) b6 -1,2,4 b7C -1,2,4
Sent: Monday, January 09, 2017 6:47 PM
To: 'Daniel Charles Richman'[redacted]
Subject: RE:[redacted]

I'm glad you sent it to the D first (takes the burden off me to "pitch" it as a project).

I'm taking a look through, although it's obviously relatively lengthy.

And let's hope it doesn't come to that!

From: Daniel Charles Richman [mailto[redacted] b6 -1,2,4 b7C -1,2,4 b7E -3
Sent: Monday, January 09, 2017 6:46 PM
To[redacted](DO) (OGA)[redacted]
Subject: Re[redacted]

forgot the last option - In addition to all the others, I'm sure the CLR would find room for a short pithy statement from the D (i.e. you) :)

On Mon, Jan 9, 2017 at 6:43 PM, Daniel Charles Richman
[redacted] wrote: b6 -2,4 b7C -2,4

> oh good. I was thinking of sending it to you directly. As you'll recall, law rev editing schedules are complicated and this one is kinda in flux, because of a number of[redacted] I suspect that, now that[redacted]piece has arrived, the CLR editors will be working on it for several weeks (perhaps longer). Then it will go back to[redacted]
>
> Given that, notwithstanding his rough treatment of the D[redacted]is a truly nice guy and generally gets high marks for academic integrity, I think we have, and should use, several avenues: If he's gotten anything wrong, or is quoting any D speech really out of context, tell me and I will suggest to him that he fix it. I will also tell the law rev eds. If you have substantive criticisms, I'll bet[redacted]will also consider them, and if rejects them, I will think about using them in the piece I'm writing with
> [redacted] b6 -2 b7C -2
>
> On Mon, Jan 9, 2017 at 6:36 PM[redacted](DO) (OGA)
> [redacted] wrote: b6 -1,2 b7C -1,2 b7E -3
>
>> D passed along the[redacted] article. Just curious what the timeline would be to get any suggestions/edits to you ?

> [redacted]
>
> --
> Daniel Richman
> Paul J. Kellner Professor of Law,
> Columbia Law School
> office [redacted]
> cellphone [redacted]
> You can download my papers at http://ssrn.com/author=937729

b6 -1,4
b7C -1,4

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office [redacted]
cellphone [redacted]
You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

Spam
Not spam
Forget previous vote

[redacted]

b6 -1,5
b7C -1,5

From: [redacted]
Sent: Thursday, January 12, 2017 2:19 PM
To: [redacted] (DO) (OGA); Daniel Charles Richman
Subject: RE: GD post

Dan/[redacted]-

Thank you for your kind words. I look forward to keeping in touch with you both, and hopefully working together in the future.

All the best,

[redacted]

From: [redacted] (DO) (OGA) [mailto[redacted]
Sent: Wednesday, January 11, 2017 9:22 PM
To: Daniel Charles Richman [redacted]
Subject: RE: GD post

b6 -1,4,5
b7C -1,4,5
b7E -3

Sorry this didn't work out [redacted] the Bu would have been very lucky to have you. Thanks for being open to it, though, and hope we can talk soon as well.

--

-------- Original message --------
From: Daniel Charles Richman [redacted]
Date: 01/11/2017 6:52 PM (GMT-05:00)
To: [redacted]
Cc: [redacted] (DO) (OGA)"[redacted]
Subject: GD post

b6 -1,4,5
b7C -1,4,5
b7E -3

H[redacted]and cc'ing [redacted] -- I've just been told that the D has decided that GD requires an internal Bu candidate at a senior level who'll be able to stick with the effort for some time. That means that his brilliant idea to dragoon you won't work. None of this takes away from the fact that you're a Great American to even consider taking on this mission. So thanks so much for your willingness.
Let's talk soon
dan r

Daniel Charles Richman

From: Daniel Charles Richman
Sent: Thursday, January 12, 2017 5:02 PM
To: [redacted] (DO) (OGA)
Subject: a slightly more elaborate version of what i said on the phone

b6 -1
b7C -1

here's a possible sequence of point to make

[redacted]

b5 -1

[redacted] (DO) (OGA)

b6 -1
b7C -1

From: [redacted] (DO) (OGA)
Sent: Friday, January 13, 2017 4:59 PM
To: Daniel Charles Richman
Subject: RE: a slightly more elaborate version of what i said on the phone

Thanks, I'll try to edit and weave into a narrative early next week.

From: Daniel Charles Richman [mailto:[redacted]
Sent: Thursday, January 12, 2017 5:02 PM
To: [redacted] DO) (OGA [redacted]
Subject: a slightly more elaborate version of what i said on the phone

b6 -1,4
b7C -1,4
b7E -3

here's a possible sequence of point to make

[redacted]

b5 -1

Daniel Charles Richman

From: Daniel Charles Richman
Sent: Sunday, January 29, 2017 3:23 PM
To: [redacted](DO) (OGA)
Subject: 324 access

b6 -1
b7C -1
b7E -7

Hi[redacted] Sorry to bother you with this, but the person, maybe FNU[redacted] i would contact is not accessible to me without 324mail access. And today i find myself without. Until today, when i went to the 324mail site. the screen would simply ask for my username and passcode[redacted] And that worked just find. My "password" had expired long ago but it didn't matter because access did not require it. Today however, I was presented with a pop-up box demanding my username (easy) and password (impossible). So i'm locked out. Could you please pass this on the the DO tech folks to help me?
thx
d

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office[redacted]
cellphone[redacted]
You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

Daniel Charles Richman

From: Daniel Charles Richman
Sent: Monday, January 30, 2017 3:34 PM
To: [redacted] (DO) (OGA)
Subject: Re: homicide stats

b6 -1
b7C -1

let me check with the law rev people on the deadline

On Mon, Jan 30, 2017 at 2:01 PM, [redacted] (DO) (OGA) [redacted] wrote:

b6 -1
b7C -1
b7E -3

> No commitment, but I teed up for the D that you and I would draft a CLR one-pager for his review (I just haven't had a chance to turn the email you sent me into prose). Obviously data would be part of that as well. Are there deadlines I should be aware of?
>
> Let me check on crime data stats.
>
> **From:** Daniel Charles Richman [mailto: [redacted]
> **Sent:** Monday, January 30, 2017 12:19 PM
> **To:** [redacted] (DO) (OGA) [redacted]
> **Subject:** homicide stats
>
> b6 -1,2,4
> b7C -1,2,4
> b7E -3
>
> Hi again -- Any word whether you and D are writing for the CLR?
>
> And regardless, do you have official or semi-official national stats on murders and shootings, and also for the nation's 50 or 30 largest cities for 2014-2016? D sent me the Police Foundation report that just came out, but [redacted] and I want the best possible data.
>
> thx
>
> d
>
> Spam
> Not spam
> Forget previous vote

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office [redacted]
cellphone [redacted]
You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

[redacted](DO) (OGA)

b6 -1
b7C -1

From: [redacted]DO) (OGA)
Sent: Monday, January 30, 2017 3:35 PM
To: Daniel Charles Richman
Subject: RE: homicide stats

Separately, has OGC been in touch on revising your MOU?

From: Daniel Charles Richman [mailto:[redacted]
Sent: Monday, January 30, 2017 3:34 PM
To:[redacted](DO) (OGA)[redacted]
Subject: Re: homicide stats

b6 -1,4
b7C -1,4
b7E -3

let me check with the law rev people on the deadline

On Mon, Jan 30, 2017 at 2:01 PM,[redacted](DO) (OGA[redacted] wrote:

> No commitment, but I teed up for the D that you and I would draft a CLR one-pager for his review (I just haven't had a chance to turn the email you sent me into prose). Obviously data would be part of that as well. Are there deadlines I should be aware of?
>
> Let me check on crime data stats.
>
> **From:** Daniel Charles Richman [mailto:[redacted]
> **Sent:** Monday, January 30, 2017 12:19 PM
> **To:**[redacted]DO) (OGA)[redacted]
> **Subject:** homicide stats
>
> b6 -1,2,4
> b7C -1,2,4
> b7E -3
>
> Hi again -- Any word whether you and D are writing for the CLR?
>
> And regardless, do you have official or semi-official national stats on murders and shootings, and also for the nation's 50 or 30 largest cities for 2014-2016? D sent me the Police Foundation report that just came out, but[redacted]and I want the best possible data.
> thx
> d
>
> ---
>
> Spam
> Not spam
> Forget previous vote

--
Daniel Richman
Paul J. Kellner Professor of Law,

Columbia Law School
office [redacted]
cellphone [redacted]
You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

Daniel Charles Richman

From:	Daniel Charles Richman
Sent:	Monday, January 30, 2017 12:19 PM
To:	[redacted] (DO) (OGA)
Subject:	homicide stats

b6 -1,2
b7C -1,2

Hi again -- Any word whether you and D are writing for the CLR?

And regardless, do you have official or semi-official national stats on murders and shootings, and also for the nation's 50 or 30 largest cities for 2014-2016? D sent me the Police Foundation report that just came out, but [redacted] and I want the best possible data.
thx
d

Daniel Charles Richman

From: Daniel Charles Richman
Sent: Monday, January 30, 2017 3:36 PM
To: [redacted] (DO) (OGA)
Subject: Re: homicide stats

b6 -1
b7C -1
b7E -3

nothing from OGC

On Mon, Jan 30, 2017 at 3:34 PM [redacted] DO) (OGA) [redacted] wrote:

> Separately, has OGC been in touch on revising your MOU?
>
> **From:** Daniel Charles Richman [mailto: [redacted]
> **Sent:** Monday, January 30, 2017 3:34 PM
> **To:** [redacted] (DO) (OGA) [redacted]
> **Subject:** Re: homicide stats
>
> b6 -1,4
> b7C -1,4
> b7E -3
>
> let me check with the law rev people on the deadline
>
> On Mon, Jan 30, 2017 at 2:01 PM, [redacted] DO) (OGA) [redacted] wrote:
>
> b6 -1
> b7C -1
> b7E -3
>
> > No commitment, but I teed up for the D that you and I would draft a CLR one-pager for his review (I just haven't had a chance to turn the email you sent me into prose). Obviously data would be part of that as well. Are there deadlines I should be aware of?
> >
> > Let me check on crime data stats.
> >
> > **From:** Daniel Charles Richman [mailto [redacted]
> > **Sent:** Monday, January 30, 2017 12:19 PM
> > **To:** [redacted] (DO) (OGA) [redacted]
> > **Subject:** homicide stats
> >
> > b6 -1,4
> > b7C -1,4
> > b7E -3
> >
> > Hi again -- Any word whether you and D are writing for the CLR?

>> And regardless, do you have official or semi-official national stats on murders and shootings, and also for the nation's 50 or 30 largest cities for 2014-2016? D sent me the Police Foundation report that just came out, but [redacted] and I want the best possible data. b6 -2 b7C -2
>>
>> thx
>>
>> d
>>
>> ---
>>
>> Spam
>> Not spam
>> Forget previous vote
>
> --
>
> Daniel Richman
> Paul J. Kellner Professor of Law,
> Columbia Law School
> office [redacted] b6 -4
> cellphone [redacted] b7C -4
> You can download my papers at http://ssrn.com/author=937729
>
> ---
>
> Spam
> Not spam
> Forget previous vote

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office [redacted] b6 -4
cellphone [redacted] b7C -4
You can download my papers at http://ssrn.com/author=937729

Daniel Charles Richman

From: Daniel Charles Richman
Sent: Monday, January 30, 2017 5:55 PM
To: [redacted](DO) (OGA)
Subject: Re: homicide stats

b6 -1
b7C -1

on timing for the CLR the response is

"Our EME says that the absolute latest we could have Comey submit the piece for publication in print would require us to have a complete draft submitted by Monday (February 6). If this doesn't work, we can also discuss publishing something online. Unfortunately, we have such limited flexibility here!"

I say: On Line is ok, but far from optimal

On Mon, Jan 30, 2017 at 3:34 PM, Daniel Charles Richman [redacted] wrote:

b6 -1,4
b7C -1,4
b7E -3

> let me check with the law rev people on the deadline
>
> On Mon, Jan 30, 2017 at 2:01 PM, [redacted]DO) (OGA) [redacted] wrote:
>
>> No commitment, but I teed up for the D that you and I would draft a CLR one-pager for his review (I just haven't had a chance to turn the email you sent me into prose). Obviously data would be part of that as well. Are there deadlines I should be aware of?
>>
>> Let me check on crime data stats.
>>
>> **From:** Daniel Charles Richman [mailto:[redacted]
>> **Sent:** Monday, January 30, 2017 12:19 PM
>> **To:** [redacted](DO) (OGA) [redacted]
>> **Subject:** homicide stats
>>
>> b6 -1,2,4
>> b7C -1,2,4
>> b7E -3
>>
>> Hi again -- Any word whether you and D are writing for the CLR?
>>
>> And regardless, do you have official or semi-official national stats on murders and shootings, and also for the nation's 50 or 30 largest cities for 2014-2016? D sent me the Police Foundation report that just came out, but [redacted] and I want the best possible data.
>>
>> thx
>>
>> d

> > Spam
> > Not spam
> > Forget previous vote
>
> --
> Daniel Richman
> Paul J. Kellner Professor of Law,
> Columbia Law School
> office [redacted]
> cellphone [redacted]
> You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office [redacted]
cellphone [redacted]
You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

[redacted] (DO) (OGA)

b6 -1
b7C -1

From: [redacted] (DO) (OGA)
Sent: Monday, January 30, 2017 2:02 PM
To: Daniel Charles Richman
Subject: RE: homicide stats

No commitment, but I teed up for the D that you and I would draft a CLR one-pager for his review (I just haven't had a chance to turn the email you sent me into prose). Obviously data would be part of that as well. Are there deadlines I should be aware of?

Let me check on crime data stats.

From: Daniel Charles Richman [mailto[redacted]
Sent: Monday, January 30, 2017 12:19 PM
To:[redacted] (DO) (OGA) [redacted]
Subject: homicide stats

b6 -1,2,4
b7C -1,2,4
b7E -3

Hi again -- Any word whether you and D are writing for the CLR?

And regardless, do you have official or semi-official national stats on murders and shootings, and also for the nation's 50 or 30 largest cities for 2014-2016? D sent me the Police Foundation report that just came out, but [redacted] and I want the best possible data.
thx
d

[redacted] (DO) (OGA)

b6 -1
b7C -1

From: [redacted] (DO) (OGA)
Sent: Monday, January 30, 2017 5:56 PM
To: Daniel Charles Richman
Subject: RE: homicide stats

Ok, thanks, I didn't realize there was such a tight deadline.

From: Daniel Charles Richman [mailto [redacted]
Sent: Monday, January 30, 2017 5:55 PM
To [redacted] DO) (OGA) [redacted]
Subject: Re: homicide stats

b6 -1,4
b7C -1,4
b7E -3

on timing for the CLR the response is

"Our EME says that the absolute latest we could have Comey submit the piece for publication in print would require us to have a complete draft submitted by Monday (February 6). If this doesn't work, we can also discuss publishing something online. Unfortunately, we have such limited flexibility here!"

I say: On Line is ok, but far from optimal

On Mon, Jan 30, 2017 at 3:34 PM, Daniel Charles Richman [redacted] wrote:

b6 -1,4
b7C -1,4
b7E -3

> let me check with the law rev people on the deadline
>
> On Mon, Jan 30, 2017 at 2:01 PM, [redacted] (DO) (OGA) [redacted] wrote:
>
>> No commitment, but I teed up for the D that you and I would draft a CLR one-pager for his review (I just haven't had a chance to turn the email you sent me into prose). Obviously data would be part of that as well. Are there deadlines I should be aware of?
>>
>> Let me check on crime data stats.
>>
>> **From:** Daniel Charles Richman [mailto: [redacted]
>> **Sent:** Monday, January 30, 2017 12:19 PM
>> **To:** [redacted] (DO) (OGA) [redacted]
>> **Subject:** homicide stats
>>
>> b6 -1,2,4
>> b7C -1,2,4
>> b7E -3
>>
>> Hi again -- Any word whether you and D are writing for the CLR?
>>
>> And regardless, do you have official or semi-official national stats on murders and shootings, and also for the nation's 50 or 30 largest cities for 2014-2016? D sent me the Police Foundation report that just came out, but [redacted] and I want the best possible data.
>> thx
>> d
>>
>> Spam

> > Not spam
> > Forget previous vote
>
> --
> Daniel Richman
> Paul J. Kellner Professor of Law,
> Columbia Law School
> office [redacted]
> cellphone [redacted]
> You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office [redacted]
cellphone [redacted]
You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

Daniel Charles Richman

From: Daniel Charles Richman
Sent: Monday, January 30, 2017 6:28 PM
To: [redacted] (DO) (OGA)
Subject: Re: transition sentences

b6 -1,2
b7C -1,2

[redacted] Jim Comey's awesome special counsel (cc'd here), would like to help us on this, but needs more detail on what you want. Also wants to know if you've already checked the UCR

On Mon, Jan 30, 2017 at 10:55 AM, [redacted] wrote:

b6 -2
b7C -2

> Ask FBI for 'official' national stats on murders and shootings, the reports are all over the place and we need to get the official count.
>
> and if possible, get it for the nation's 50 or 30 largest cities.
>
> [redacted]

[redacted] (DO) (OGA) b6 -1,2 b7C -1,2

From: [redacted] (DO) (OGA)
Sent: Monday, January 30, 2017 6:29 PM
To: Daniel Charles Richman; [redacted]
Subject: RE: transition sentences

As a starting point, here's the UCR page, if you haven't already seen it:

https://ucr.fbi.gov/

From: Daniel Charles Richman [mailto [redacted]
Sent: Monday, January 30, 2017 6:28 PM
To: [redacted] (DO) (OGA) [redacted]
Subject: Re: transition sentences

b6 -1,2,4 b7C -1,2,4 b7E -3

[redacted] Jim Comey's awesome special counsel (cc'd here), would like to help us on this, but needs more detail on what you want. Also wants to know if you've already checked the UCR

On Mon, Jan 30, 2017 at 10:55 AM, [redacted] wrote: b6 -2 b7C -2

> Ask FBI for 'official' national stats on murders and shootings, the reports are all over the place and we need to get the official count.
>
> and if possible, get it for the nation's 50 or 30 largest cities.
>
> [redacted]

[redacted](DO) (OGA)

b6 -1,2
b7C -1,2

From: [redacted](DO) (OGA)
Sent: Monday, January 30, 2017 6:43 PM
To: Daniel Charles Richman
Subject: RE: study

I'll take a look, thanks. (Not that she would remember, but) I had [redacted]

From: Daniel Charles Richman [mailto:[redacted]
Sent: Monday, January 30, 2017 6:33 PM
To:[redacted](DO) (OGA) [redacted]
Subject: study

b6 -1,2,4
b7C -1,2,4
b7E -3

The Baltimore study i menttioned is at http://socweb.soc.jhu.edu/faculty/morgan/papers/MorganPally2016.pdf
http://socweb.soc.jhu.edu/faculty/morgan/papers/MorganPally2016FallUpdate.pdf

Attached is[redacted]new draft and[redacted]draft
also the beginning of my draft with[redacted]- it's mostly him and I'm just starting (see yellow)

[redacted](DO) (OGA)

b6 -1
b7C -1

From: [redacted](DO) (OGA)
Sent: Monday, January 30, 2017 6:38 PM
To: Daniel Charles Richman
Subject: RE: homicide stats

What's the projected print date?

From: Daniel Charles Richman [mailto[redacted]
Sent: Monday, January 30, 2017 5:55 PM
To:[redacted](DO) (OGA)[redacted]
Subject: Re: homicide stats

b6 -1,4
b7C -1,4
b7E -3

on timing for the CLR the response is
"Our EME says that the absolute latest we could have Comey submit the piece for publication in print would require us to have a complete draft submitted by Monday (February 6). If this doesn't work, we can also discuss publishing something online. Unfortunately, we have such limited flexibility here!"

I say: On Line is ok, but far from optimal

On Mon, Jan 30, 2017 at 3:34 PM, Daniel Charles Richman[redacted]wrote:

b6 -1,4
b7C -1,4
b7E -3

> let me check with the law rev people on the deadline
>
> On Mon, Jan 30, 2017 at 2:01 PM,[redacted](DO) (OGA)[redacted]wrote:
>
>> No commitment, but I teed up for the D that you and I would draft a CLR one-pager for his review (I just haven't had a chance to turn the email you sent me into prose). Obviously data would be part of that as well. Are there deadlines I should be aware of?
>>
>> Let me check on crime data stats.
>>
>> **From:** Daniel Charles Richman [mailto[redacted]
>> **Sent:** Monday, January 30, 2017 12:19 PM
>> **To:**[redacted](DO) (OGA)[redacted]
>> **Subject:** homicide stats
>>
>> b6 -1,2,4
>> b7C -1,2,4
>> b7E -3
>>
>> Hi again -- Any word whether you and D are writing for the CLR?
>>
>> And regardless, do you have official or semi-official national stats on murders and shootings, and also for the nation's 50 or 30 largest cities for 2014-2016? D sent me the Police Foundation report that just came out, but[redacted]and I want the best possible data.
>> thx
>> d
>>
>> ---
>>
>> Spam

> > Not spam
> > Forget previous vote
>
> --
> Daniel Richman
> Paul J. Kellner Professor of Law,
> Columbia Law School
> office [redacted]
> cellphone [redacted]
> You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office [redacted]
cellphone [redacted]
You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

Daniel Charles Richman

From: Daniel Charles Richman
Sent: Monday, January 30, 2017 6:43 PM
To: [redacted](DO) (OGA)
Subject: Re: homicide stats

b6 -1,4
b7C -1,4

I believe march-April

Daniel Richman
Paul J. Kellner Professor of Law
Columbia Law School
Office:[redacted]
Cell:[redacted]

On Jan 30, 2017, at 6:38 PM,[redacted](DO) (OGA) [redacted]wrote:

b6 -1,4
b7C -1,4
b7E -3

> What's the projected print date?
>
> **From:** Daniel Charles Richman [mailto[redacted]
> **Sent:** Monday, January 30, 2017 5:55 PM
> **To:** [redacted](DO) (OGA)[redacted]
> **Subject:** Re: homicide stats
>
> on timing for the CLR the response is
>
> "Our EME says that the absolute latest we could have Comey submit the piece for publication in print would require us to have a complete draft submitted by Monday (February 6). If this doesn't work, we can also discuss publishing something online. Unfortunately, we have such limited flexibility here!"
>
> I say: On Line is ok, but far from optimal
>
> On Mon, Jan 30, 2017 at 3:34 PM, Daniel Charles Richman[redacted]wrote:
>
> b6 -1,4
> b7C -1,4
> b7E -3
>
> > let me check with the law rev people on the deadline
> >
> > On Mon, Jan 30, 2017 at 2:01 PM,[redacted](DO) (OGA)
> > [redacted]wrote:
> >
> > > No commitment, but I teed up for the D that you and I would draft a CLR one-pager for his review (I just haven't had a chance to turn the email you sent me into prose). Obviously data would be part of that as well. Are there deadlines I should be aware of?
> > >
> > > Let me check on crime data stats.
> > >
> > > **From:** Daniel Charles Richman [mailto:[redacted]
> > > **Sent:** Monday, January 30, 2017 12:19 PM
> > > **To:** [redacted](DO) (OGA)[redacted]
> > > **Subject:** homicide stats

b6 -1,4
b7C -1,4
b7E -3

> > Hi again -- Any word whether you and D are writing for the CLR?
> >
> > And regardless, do you have official or semi-official national stats on murders and shootings, and also for the nation's 50 or 30 largest cities for 2014-2016? D sent me the Police Foundation report that just came out, but [redacted] and I want the best possible data.
> > thx
> > d
> >
> > b6 -2
> > b7C -2
> >
> > ---
> >
> > Spam
> > Not spam
> > Forget previous vote
>
> --
> Daniel Richman
> Paul J. Kellner Professor of Law,
> Columbia Law School
> office [redacted]
> cellphone [redacted]
> You can download my papers at http://ssrn.com/author=937729
>
> b6 -4
> b7C -4

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office [redacted]
cellphone [redacted]
You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

Spam
Not spam
Forget previous vote

Daniel Charles Richman

From: Daniel Charles Richman
Sent: Monday, January 30, 2017 6:33 PM
To: [redacted](DO) (OGA)
Subject: study
Attachments: [redacted]_CLR_on Crime -- Revised Jan 20.docx; columbia essay 2.0.docx; CLR _ MiniSymposium DR jan 30.docx

b6 -1,2
b7C -1,2

The Baltimore study i menttioned is at
http://socweb.soc.jhu.edu/faculty/morgan/papers/MorganPally2016.pdf
http://socweb.soc.jhu.edu/faculty/morgan/papers/MorganPally2016FallUpdate.pdf

Attached is [redacted]new draft and [redacted]draft
also the beginning of my draft with [redacted] it's mostly him and I'm just starting (see yellow)

Daniel Charles Richman

From: Daniel Charles Richman
Sent: Tuesday, January 31, 2017 4:26 PM
To: [redacted] (DO) (OGA)
Cc: [redacted] (DO) (FBI)
Subject: Re: Law Review Draft

b6 -1
b7C -1

very nice work. The deadline is indeed short, and this piece has just the reach tone -- openness to inquiry -- that I think the D would like

Small point. Call me hypersensitive (an occupational hazard for law profs), but the sentence

[redacted] b5 -1

[redacted]

dan r

On Tue, Jan 31, 2017 at 4:15 PM, [redacted] (DO) (OGA) [redacted] wrote:

b6 -1
b7C -1
b7E -3

> Dan, [redacted]
>
> Please find attached a 3-paragraph draft statement on crime and policing that Dan suggested that Director submit for the next edition of the Columbia Law Review (which is focused on that subject). [redacted] I'm hoping you (or someone in the Executive Writing Unit) can review, in particular, for the Boss's style, tone, etc.
>
> I believe we're on a relatively short deadline, with Dan hoping to submit a draft to the Boss in the next day or so?
>
> [redacted]
>
> --
> BEGIN-ANTISPAM-VOTING-LINKS
> ------------------------------ ------------------------

> Teach Email if this mail (ID 01SD9eii6) is spam:
>
> Spam: https://antispam.law.columbia.edu/canit/b.php?i=01SD9eii6&m=400671e5f20f&t=20170131&c=s
>
> Not spam: https://antispam.law.columbia.edu/canit/b.php?i=01SD9eii6&m=400671e5f20f&t=20170131&c=n
>
> Forget vote: https://antispam.law.columbia.edu/canit/b.php?i=01SD9eii6&m=400671e5f20f&t=20170131&c=f
> ---------------------------- -----------------------
> END-ANTISPAM-VOTING-LINKS

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office [redacted]
cellphone [redacted]
You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

[redacted] (DO) (OGA)

b6 -1
b7C -1

From: [redacted] (DO) (OGA)
Sent: Tuesday, January 31, 2017 4:15 PM
To: Daniel Charles Richman; [redacted] (DO) (FBI)
Subject: Law Review Draft
Attachments: Policing Draft.docx

Dan, [redacted]

Please find attached a 3-paragraph draft statement on crime and policing that Dan suggested that Director submit for the next edition of the Columbia Law Review (which is focused on that subject). [redacted] I'm hoping you (or someone in the Executive Writing Unit) can review, in particular, for the Boss's style, tone, etc.

I believe we're on a relatively short deadline, with Dan hoping to submit a draft to the Boss in the next day or so?

[redacted]

Daniel Charles Richman

From: Daniel Charles Richman
Sent: Tuesday, January 31, 2017 4:38 PM
To: [redacted](DO) (OGA)
Cc: [redacted](DO) (FBI)
Subject: Re: Law Review Draft

b5 -1
b6 -1
b7C -1

even though there's little time to think about this, i wonder if the D should [redacted]

On Tue, Jan 31, 2017 at 4:27 PM, [redacted] DO) (OGA) [redacted] wrote:

b6 -1
b7C -1
b7E -3

> That change makes sense to me.
>
> **From:** Daniel Charles Richman [mailto[redacted]
> **Sent:** Tuesday, January 31, 2017 4:26 PM
> **To:** [redacted](DO) (OGA) [redacted]
> **Cc:** [redacted](DO) (FBI) [redacted]
> **Subject:** Re: Law Review Draft
>
> very nice work. The deadline is indeed short, and this piece has just the reach tone -- openness to inquiry -- that I think the D would like
>
> Small point. Call me hypersensitive (an occupational hazard for law profs), but the sentence
>
> [redacted]
>
> [redacted]
>
> dan r

b6 -1,4
b7C -1,4
b7E -3

b5 -1

On Tue, Jan 31, 2017 at 4:15 PM, [redacted] (DO) (OGA) [redacted] wrote:

b6 -1
b7C -1
b7E -3

> Dan, [redacted]
>
> Please find attached a 3-paragraph draft statement on crime and policing that Dan suggested that Director submit for the next edition of the Columbia Law Review (which is focused on that subject). [redacted] I'm hoping you (or someone in the Executive Writing Unit) can review, in particular, for the Boss's style, tone, etc.
>
> I believe we're on a relatively short deadline, with Dan hoping to submit a draft to the Boss in the next day or so?
>
> [redacted]
>
> --
>
> BEGIN-ANTISPAM-VOTING-LINKS
>
> ------------------------------ ------------------------
>
> Teach Email if this mail (ID 01SD9eii6) is spam:
>
> Spam: https://antispam.law.columbia.edu/canit/b.php?i=01SD9eii6&m=400671e5f20f&t=20170131&c=s
>
> Not spam: https://antispam.law.columbia.edu/canit/b.php?i=01SD9eii6&m=400671e5f20f&t=20170131&c=n
>
> Forget vote: https://antispam.law.columbia.edu/canit/b.php?i=01SD9eii6&m=400671e5f20f&t=20170131&c=f
>
> ------------------------------ ------------------------
>
> END-ANTISPAM-VOTING-LINKS

--

Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office [redacted]
cellphone [redacted]
You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

Spam

> Not spam
> Forget previous vote

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office [redacted]
cellphone [redacted]
You can download my papers at http://ssrn.com/author=937729

b6 -4
b7C -4

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Friday, October 09, 2015 12:20 PM
To: Oconnell, Sasha C. (DO) (FBI)
Subject: RE: encryption articles re: yesterdays hearing

thanks. So why nothing from my local rag? Since the NYT often (as here) misses the initial news, it's shtick is to do the deepening and broadening on the second beat. So it's probably doing "how tech folks are reacting."

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Friday, October 09, 2015 12:12 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: FW: encryption articles re: yesterdays hearing

From: [redacted] (DO) (FBI) b6 -1 b7C -1
Sent: Friday, October 09, 2015 11:06 AM
To: Oconnell, Sasha C. (DO) (FBI)
Subject: encryption articles re: yesterdays hearing

https://www.washingtonpost.com/world/national-security/obama-administration-opts-not-to-force-firms-to-decrypt-data--for-now/2015/10/08/1d6a6012-6dca-11e5-aa5b-f78a98956699_story.html

http://thehill.com/policy/cybersecurity/256491-white-house-will-not-force-tech-firms-to-decrypt-data

http://cdn.govexec.com/interstitial.html?v=2.1.1&rf=http%3A%2F%2Fwww.govexec.com%2Fmanagement%2F2015%2F10%2Ffbi-dozens-terror-suspects-have-used-encryption-hide-law-enforcement%2F122674%2F

http://www.zdnet.com/article/us-says-no-to-encryption-law-for-now/

http://www.pcworld.com/article/2991272/encryption/us-will-not-seek-legislation-against-encryption.html

****
[redacted]
Federal Bureau of Investigation
Office of National Policy
[redacted]

b6 -1
b7C -1
b7E -3

Richman, Daniel C. (DO) (OGA)

From:	Richman, Daniel C. (DO) (OGA)
Sent:	Friday, October 09, 2015 12:31 PM
To:	Oconnell, Sasha C. (DO) (FBI)
Subject:	RE: encryption articles re: yesterdays hearing

Let's see what further coverage comes in the next few days. But my inclination is to circulate the WaPo piece and maybe another one to roundtable attendees (to ensure everyone is focused).
d

____
From: Oconnell, Sasha C. (DO) (FBI)
Sent: Friday, October 09, 2015 12:12 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: FW: encryption articles re: yesterdays hearing

From: [redacted] (DO) (FBI) b6 -1 b7C -1
Sent: Friday, October 09, 2015 11:06 AM
To: Oconnell, Sasha C. (DO) (FBI)
Subject: encryption articles re: yesterdays hearing

https://www.washingtonpost.com/world/national-security/obama-administration-opts-not-to-force-firms-to-decrypt-data--for-now/2015/10/08/1d6a6012-6dca-11e5-aa5b-f78a98956699_story.html

http://thehill.com/policy/cybersecurity/256491-white-house-will-not-force-tech-firms-to-decrypt-data

http://cdn.govexec.com/interstitial.html?v=2.1.1&rf=http%3A%2F%2Fwww.govexec.com%2Fmanagement%2F2015%2F10%2Ffbi-dozens-terror-suspects-have-used-encryption-hide-law-enforcement%2F122674%2F

http://www.zdnet.com/article/us-says-no-to-encryption-law-for-now/

http://www.pcworld.com/article/2991272/encryption/us-will-not-seek-legislation-against-encryption.html

****
[redacted] b6 -1 b7C -1 b7E -3
Federal Bureau of Investigation
Office of National Policy
[redacted]

Oconnell, Sasha C. (DO) (FBI)

Subject: Call re: Going Dark Example Collection
Location: dial [redacted] passcode: [redacted] b7E -3

Start: Tuesday, October 13, 2015 4:00 PM
End: Tuesday, October 13, 2015 5:00 PM
Show Time As: Tentative

Recurrence: (none)

Meeting Status: Not yet responded

Organizer: Oconnell, Sasha C. (DO) (FBI)
Required Attendees: [redacted] b6 -1,2,5 b7C -1,2,5
[redacted] (USANYS);
[redacted] (USANYS); [redacted]
Richman, Daniel C. (DO) (OGA); [redacted] (NY) (FBI);
Mahairas, Aristedes (CTD) (FBI); [redacted] (ODAG) (JMD);
[redacted] (DO) (FBI) [redacted] (DO) (FBI)
Optional Attendees: [redacted]

When: Tuesday, October 13, 2015 4:00 PM-5:00 PM (UTC-05:00) Eastern Time (US & Canada).
Where: dial: [redacted] passcode: [redacted] b7E -3

Note: The GMT offset above does not reflect daylight saving time adjustments.

~~*~*~*~*~*~*~*~*

We have a quorum, look forward to talking with you then!

Thank you,

Sasha

Sasha Cohen O'Connell
Chief, Office of National Policy
Office of the Deputy Director
FBIHQ– [redacted] b7E -3

Oconnell, Sasha C. (DO) (FBI)

From:	Oconnell, Sasha C. (DO) (FBI)
Sent:	Friday, October 09, 2015 12:35 PM
To:	Richman, Daniel C. (DO) (OGA)
Subject:	RE: encryption articles re: yesterdays hearing

Concur!

-----Original Message-----
From: Richman, Daniel C. (DO) (OGA)
Sent: Friday, October 09, 2015 12:31 PM
To: Oconnell, Sasha C. (DO) (FBI)
Subject: RE: encryption articles re: yesterdays hearing

Let's see what further coverage comes in the next few days. But my inclination is to circulate the WaPo piece and maybe another one to roundtable attendees (to ensure everyone is focused).
d

____
From: Oconnell, Sasha C. (DO) (FBI)
Sent: Friday, October 09, 2015 12:12 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: FW: encryption articles re: yesterdays hearing

From: [redacted] (DO) (FBI) b6 -1 b7C -1
Sent: Friday, October 09, 2015 11:06 AM
To: Oconnell, Sasha C. (DO) (FBI)
Subject: encryption articles re: yesterdays hearing

https://www.washingtonpost.com/world/national-security/obama-administration-opts-not-to-force-firms-to-decrypt-data--for-now/2015/10/08/1d6a6012-6dca-11e5-aa5b-f78a98956699_story.html

http://thehill.com/policy/cybersecurity/256491-white-house-will-not-force-tech-firms-to-decrypt-data

http://cdn.govexec.com/interstitial.html?v=2.1.1&rf=http%3A%2F%2Fwww.govexec.com%2Fmanagement%2F2015%2F10%2Ffbi-dozens-terror-suspects-have-used-encryption-hide-law-enforcement%2F122674%2F

http://www.zdnet.com/article/us-says-no-to-encryption-law-for-now/

http://www.pcworld.com/article/2991272/encryption/us-will-not-seek-legislation-against-encryption.html

****
[redacted] b6 -1 b7C -1
Federal Bureau of Investigation
Office of National Policy

[redacted]

b6 -1
b7C -1
b7E -3

Richman, Daniel C. (DO) (OGA)

From:	Richman, Daniel C. (DO) (OGA)
Sent:	Friday, October 09, 2015 1:10 PM
To:	Oconnell, Sasha C. (DO) (FBI)

It is true that [redacted] and I are concerned about the size of the group next fri and being quite grudging about adding people. But as I look at the number of govt vs. non-govt coming, my new thought is that if, in the wake of the post-hearing "clarity," a really well placed industry person wanted in, I'd lean toward inviting. But not just anyone :) b6 -2 b7C -2

Oconnell, Sasha C. (DO) (FBI)

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Friday, October 09, 2015 2:34 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE:

Hmmm. Do you have any thoughts? I think I have offered all of our productive engagement folks but I will look through my stack of cards here...

-----Original Message-----
From: Richman, Daniel C. (DO) (OGA)
Sent: Friday, October 09, 2015 1:10 PM
To: Oconnell, Sasha C. (DO) (FBI)
Subject:

It is true that [redacted] and I are concerned about the size of the group next fri and being quite grudging about adding people. But as I look at the number of govt vs. non-govt coming, my new thought is that if, in the wake of the post-hearing "clarity," a really well placed industry person wanted in, I'd lean toward inviting. But not just anyone :) b6 -2 b7C -2

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Friday, October 09, 2015 3:02 PM
To: Oconnell, Sasha C. (DO) (FBI)
Subject: RE:

I don't. But I know my prime candidate: someone who wasn't willing to productively engage before, but who now realizes that there really needs to be "a discussion"

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Friday, October 09, 2015 2:33 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE:

Hmmm. Do you have any thoughts? I think I have offered all of our productive engagement folks but I will look through my stack of cards here...

-----Original Message-----
From: Richman, Daniel C. (DO) (OGA)
Sent: Friday, October 09, 2015 1:10 PM
To: Oconnell, Sasha C. (DO) (FBI)
Subject:

It is true that [redacted] and I are concerned about the size of the group next fri and being quite grudging about adding people. But as I look at the number of govt vs. non-govt coming, my new thought is that if, in the wake of the post-hearing "clarity," a really well placed industry person wanted in, I'd lean toward inviting. But not just anyone :) b6 -2 b7C -2

Richman, Daniel C. (DO) (OGA)

From:	Richman, Daniel C. (DO) (OGA)
Sent:	Friday, October 09, 2015 3:32 PM
To:	Oconnell, Sasha C. (DO) (FBI); [redacted] (ODAG) (JMD)
Subject:	anonymization
Attachments:	CIGI Dark Web Dilemma.pdf

b6 -5
b7C -5

For down the road: To show the Bu's reasonableness: You might tout its (USGs) readiness to accept (because of the need to balance interests) anonymizing mechanisms like Tor, even in the face of studies of Tor suggesting that "the majority of sites were criminally oriented, with drug marketplaces featuring prominently. . . . [S]ites hosting child abuse imagery were the most frequently requested" https://www.cigionline.org/sites/default/files/no20_0.pdf

In the (not so impressive) paper attached here, this fact becomes an argument for proactive policing of the Dark Web. (Duh)

CIGI

CHATHAM HOUSE
The Royal Institute of
International Affairs

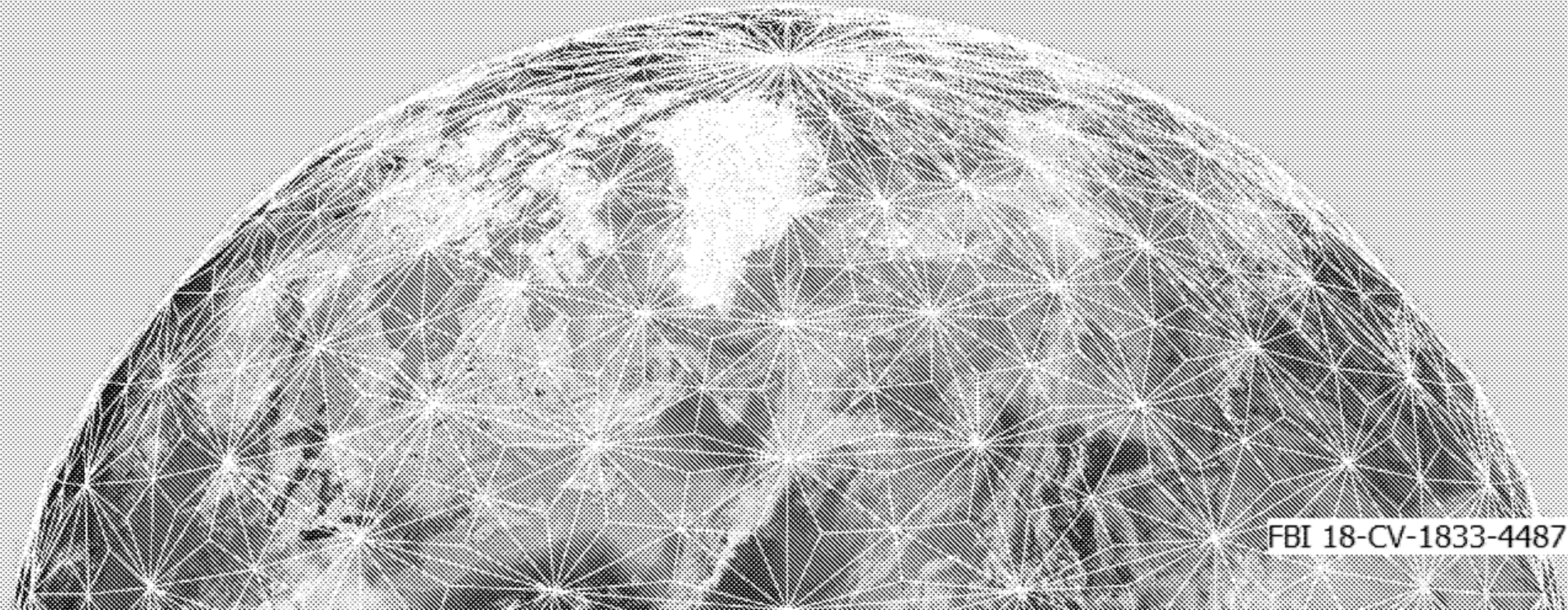
Global Commission
on Internet Governance

ourinternet.org

PAPER SERIES: NO. 21 — SEPTEMBER 2015

The Dark Web Dilemma: Tor, Anonymity and Online Policing

Eric Jardine



THE DARK WEB DILEMMA: TOR, ANONYMITY AND ONLINE POLICING

Eric Jardine

CIGI

CHATHAM HOUSE
The Royal Institute of
International Affairs

Published by the Centre for International Governance Innovation and Chatham House.

The opinions expressed in this publication are those of the author and do not necessarily reflect the views of the Centre for International Governance Innovation or its Board of Directors.

CIGI

67 Erb Street West
Waterloo, Ontario N2L 6C2
Canada
tel +1 519 885 2444 fax +1 519 885 5450
www.cigionline.org

CHATHAM HOUSE
The Royal Institute of International Affairs

10 St James's Square
London, England SW1Y 4LE
United Kingdom
tel +44 (0)20 7957 5700 fax +44 (0)20 7957 5710
www.chathamhouse.org

TABLE OF CONTENTS

ABOUT THE GLOBAL COMMISSION ON INTERNET GOVERNANCE

The Global Commission on Internet Governance was established in January 2014 to articulate and advance a strategic vision for the future of Internet governance. The two-year project conducts and supports independent research on Internet-related dimensions of global public policy, culminating in an official commission report that will articulate concrete policy recommendations for the future of Internet governance. These recommendations will address concerns about the stability, interoperability, security and resilience of the Internet ecosystem.

Launched by two independent global think tanks, the Centre for International Governance Innovation (CIGI) and Chatham House, the Global Commission on Internet Governance will help educate the wider public on the most effective ways to promote Internet access, while simultaneously championing the principles of freedom of expression and the free flow of ideas over the Internet.

The Global Commission on Internet Governance will focus on four key themes:

- enhancing governance legitimacy — including regulatory approaches and standards;
- stimulating economic innovation and growth — including critical Internet resources, infrastructure and competition policy;
- ensuring human rights online — including establishing the principle of technological neutrality for human rights, privacy and free expression; and
- avoiding systemic risk — including establishing norms regarding state conduct, cybercrime cooperation and non-proliferation, confidence-building measures and disarmament issues.

The goal of the Global Commission on Internet Governance is two-fold. First, it will encourage globally inclusive public discussions on the future of Internet governance. Second, through its comprehensive policy-oriented report, and the subsequent promotion of this final report, the Global Commission on Internet Governance will communicate its findings with senior stakeholders at key Internet governance events.

www.ourinternet.org

ABOUT THE AUTHOR

Eric Jardine joined CIGI as a research fellow in May 2014 in the Global Security & Politics Program. He contributes to CIGI's work on Internet governance, including the CIGI–Chatham House-sponsored Global Commission on Internet Governance. His current research focuses on cyber security, cyber terrorism, cybercrime and cyber protest. He holds a Ph.D. in international relations from the Norman Paterson School of International Affairs at Carleton University, Ottawa, Canada.

EXECUTIVE SUMMARY

Online anonymity-granting systems such as The Onion Router (Tor) network can be used for both good and ill. The Dark Web[1] is possible only because of online anonymity. The Dark Web poses a dilemma. Illegal markets, trolls and online child abuse rings proliferate due to the technology of Tor and other similar systems. However, the anonymity provided by such systems gives cover for people in repressive regimes that need the protection of technology in order to surf the Web, access censored content and otherwise exercise their genuine right to free expression. In other words, Tor is basically a neutral tool that can be used for either good or ill. Whether the technology is worth it depends upon the net effect. Unfortunately, the costs and benefits of a system like Tor are not evenly distributed globally. The ills tend to cluster in liberal countries, while the benefits tend to cluster most in repressive regimes. Shuttering anonymity networks is not a viable long-term solution, as it will probably prove ineffective and will be costly to those people that genuinely benefit from these systems.

Rather than being a solely technological problem, this paper argues that the issue posed by the Dark Web, enabled by anonymity-granting technologies, is a social one. Just as peace and order are maintained in our offline lives through judicious policing, the same principle should apply online. The networks of the Dark Web need to be more actively policed, especially in liberal democratic countries. Online policing, as shown by the takedown of illegal marketplaces such as Silk Road and child pedophilia rings, is actually possible, and both as effective and as expedient as offline policing. More movement in the direction of judicious online policing can minimize the socially damaging costs of anonymity-granting technologies, while still allowing the benefits of such systems. It is not the ideal solution, but it is likely the best that can be done.

INTRODUCTION

The Dark Net: its very name brings to mind images of shadowy alleys, malicious, hard-faced individuals and socially damaging activity. The Dark Net is a part of the Internet that most people probably do not know how to access, nor want to explore. A special web browser is needed just to reach it.[2] One such browser, embedded in a larger networked system, is the widely used Tor network.[3]

A lot happens via Tor. This paper runs through some of what goes on in the Dark Net, with a particular focus upon how the anonymity of the Tor browser allows for both nefarious and noble undertakings. It uses evidence from a variety of news accounts and secondary literature to detail how anonymity can be used as a tool of those that want to undertake socially damaging activity. It also uses the results of a recently conducted study on Tor usage rates that shows empirically that people in politically repressive countries are often driven to use the anonymity network out of necessity (Jardine, n.d.).

The basic story to emerge from all of this evidence is that an anonymity-granting system such as Tor, as with other technologies, is just a tool. Like fire, a hammer, or a car, the Tor network can both improve life and provide the means to take it away. What matters is not what the technology is, but how it is used and what the net effect turns out to be.

Framed from this perspective, the focus of public debate should move away from demonizing the technology, or looking for quick technological fixes, toward the idea that, like every other aspect of human society, the Dark Net needs to be policed. This recommendation is particularly relevant for liberal democratic countries, where the dark side of anonymity imposes the highest costs and the benefits of Tor are least pronounced. Ideally, policing needs to be undertaken within clearly defined, rule-based limits. That is no different than the rest of society. Sometimes, as the saying goes, the more things change, the more they stay the same.

The next section describes the Tor-hosted Dark Net. Following that, the paper discusses the negative effects generated by the anonymity of the Dark Web. The third section presents new statistical evidence to show that sometimes the anonymous network is used for good. The fourth discusses the policy implications that flow from the dual nature of the technology, in particular, how online policing of the Dark Web has proven to be just as effective as offline policing. The only way forward is to police the Dark Web, just as we police all aspects of society.

[1] The Dark Web and the Dark Net are used interchangeably throughout this paper and mean the same thing.

[2] The borders of the Dark Web are blurry. See, for example, Chertoff and Simon (2015). For the purposes of this paper, the Dark Web can be defined as a part of the Internet that is only possible because of online anonymity. This definition does not imply that online anonymity is enough to create the Dark Web, only that the Dark Web can't exist without it. In social science terms, online anonymity is a necessary, but not a sufficient, cause of the Dark Web.

[3] The Tor browser is the entry point of focus to the Dark Web for this paper, but there are other ways into the Internet's underground. The Tor browser is also one of the main gateways to anonymity in this paper. Again, others exist.

TOR AND THE DARK NET

Under normal circumstances, when you are trying to access the Web, you send a signal from your device across the Internet to the server that hosts the material that you want to view. That can be a cat meme, a pornographic video, a news organization's webpage or whatever else might tickle your fancy. The server then returns the data to your device. The relationship is direct. Your request is sent via the networks of the Internet to the place that holds the information you want to view and it is sent back.

Because of this directness, our Internet service providers (ISPs) know our names, addresses, search histories and the sites that we are visiting. It is also how the websites we view know our unique Internet Protocol (IP) address. It is because of this direct connection that companies such as Amazon know everything we view and even how long we've lingered upon a page. Law enforcement agencies are able to capitalize on this directness and can pinpoint who posted what information on an online chat forum.

Tor accesses information on the Web in much the same way, but it breaks up the direct connection. After a fashion, the Tor browser is a bit like an anonymous version of the children's game of telephone. You send your request for a particular video or bit of information to a computer somewhere in the Tor network. This computer then relays that information on to another computer somewhere else in the network. Once again, this computer simply relays your request onwards to yet another machine. This third machine in the game of telephone then requests the information you want to view and sends it back to you along a similar, disjointed path.

Breaking up the request in this way means that different people can see different parts of what you are viewing online, but it is exceptionally difficult, although not impossible, for any one person to connect all the dots to pinpoint who you actually are (Owen and Savage 2015). Your ISP, for example, which normally knows exactly what sites you are visiting, can only see that you are sending a request to the first computer in the network. On the other end of things, the website can tell a lot about the computer that is accessing their content, but this information does not relate to your computer, instead linking to the last of the three computers in the game of telephone. The computers in the relay system know about their neighbour, but no more than that. The first link knows you and the middle computer, but not the end computer or the content viewed. The middle link knows the first computer and the end computer, but not you or the destination of your request. The end computer knows the destination and the middle computer, but not who you are. Layered onto this broken routing of your request is the heavily encrypted signal that prevents data flowing across the Tor network from being accessible to prying eyes.

Tor is not just a way to view online content anonymously. You can also host content, but only in a way that is accessible to other users of the Tor browser. Put another way, you can be the one running the website to which people venture for their bits of information, whatever they might be. The process by which anonymity is obtained is similar to that laid out above. The website itself moves around from server to server in the Tor network. Changes to the website are made using the same three-relay system that is used to prevent the website or server from knowing who is hosting the page. Anonymity is secured.

Finally, it is important to clear up at the outset that, while large parts of the Dark Web are only reachable via Tor, the Tor browser itself can actually be used for other far more innocent purposes, such as simply surfing the day-to-day Web, free from the constraints of censored content and concern over state or corporate surveillance. If you try to download and use Tor (a process that is very easy), you will find that you never need to venture into the seedy underbelly of the Internet if you don't want to. Instead, you can use the Tor browser just like Google Chrome or Mozilla Firefox to check news websites, look at funny memes or anything else you would do normally when browsing the Internet.[4] Even these routine activities are rendered anonymous by Tor.

The end result of this system is a way to use the Internet anonymously, with all the immunity that provides. Clearly, as shown in the next section, that anonymity opens the door to abuses.

THE DARK SIDE OF ONLINE ANONYMITY

The Dark Net certainly is the seedy underbelly of the Internet. Its sordid nature is exemplified in a few stories about drugs, assassination, trolling and child abuse.

In the early years of this decade, a site popped up on the Dark Web called Silk Road. The reference to the ancient trading route from the Orient to Europe was not a mistake. The website was like an illegal version of Amazon, eBay, Kijiji or Craigslist. It aimed to connect sellers of items ranging from drugs to assassinations-for-hire with eager customers with money to burn.

Silk Road started in February 2011. One study observed activity on the website during a six-month period in 2012 and found that Silk Road, while selling all sorts of illegal content, was mostly a proverbial "drugstore." Categorizing all the things that were for sale on the site, the authors found that "the four most popular categories are all linked to drugs," along with 90 percent of the top 10

[4] Plug-ins are limited on Tor, so you might not have the full range of functionality you would on another web browser, but the idea that you could just use Tor for your normal Internet activity is valid.

categories and 80 percent of the top 20 (Christin 2012, 8). The transactions were anonymous due to the use of the Tor network and payments were made with a so-called crypto-currency known as bitcoin, which is a purely digital means of payment that leaves no trace.

Silk Road quickly surpassed other illegal market sites, with its revenue and traffic expanding rapidly. In an uncomfortable mix of metaphors, the site was owned by a then 29-year-old man who went by the moniker Dread Pirate Roberts — taken straight out of the 1980s movie *The Princess Bride*. By 2012, the site operators were earning upwards of $92,000[5] per month, as people were flocking to the site to buy and sell items on the illegal market. The audacity of Silk Road's illegal activities lead US Senator Charles Schumer to call for the site to be shut down in June 2011, noting that it is "more brazen that anything else by light-years" (cited in Koebler 2012).

The investigation into Silk Road started in 2011, when an informant broke word of activity on the illegal marketplace site to personnel at the Department of Homeland Security (DHS). Operation "Marco Polo," as the investigation came to be called, quickly expanded to encompass personnel from the Federal Bureau of Investigation (FBI), DHS, Drug Enforcement Administration, Internal Revenue Service and others (Zetter 2013).

As the law enforcement net was closing in on the Dread Pirate Roberts, the modern-day bandit got desperate, even offering $80,000 to an undercover agent to assassinate a former site administrator that had been captured by the police and turned state's evidence. The police staged the killing of the site administrator just to draw the noose that much tighter around Dread Pirate Roberts' neck (ibid.). Ross Ulbricht, the Dread Pirate Roberts, was arrested in October 2013 and the site was taken down. It was a clear victory.

It was also very short lived. Silk Road 2.0 popped up on the Dark Net in November 2013, just one month after the arrest of Ulbricht. Again, the website expanded rapidly, quickly having as many as 150,000 active users and processing, according to FBI records, as much as $8 million in monthly sales (Cook 2014). Within a year, this new incarnation of the illegal marketplace was taken down and Blake Benthall, the Silk Road 2.0 site administrator and former Space-X employee, was arrested.

Another win, another drop in the pond. Silk Road 3.0 was online within a few hours of Benthall's arrest (Knibbs 2014). The cycle goes on, like a globe-spanning game of whack-a-mole.

The dark recesses of the Dark Web are also populated with proverbial trolls, some of whom use Tor to maintain their anonymity, some of whom do not. We have all come across Internet trolls. They surf the Web, posting inflammatory comments, aiming for nothing more than to wreck someone's day, often just for the fun of it.

Consider this telling story of trolling and a needlessly ruined life on the 4chan /b/ board (Bartlett 2014, 13–19).[6] A young university student named Sarah ventured half-naked via a posted photograph into the chat board filled with Dark Web trolls. Her first photo spawned a number of requests for further nudity, which she willingly provided. The requests built gradually to a terrible point. One request asked her to pose naked with her name written on her body. She did it. Another request asked her to pose naked with any medications that she might be taking. She did that, too.

From there, the situation got really ugly. Her mistake was providing the trolls of the Dark Web with enough information to identify her. They found her school, accessed its directory and got her full name, address, phone number and other contact information. Facebook searches revealed her social media profile. From there, the anonymous chatters of the /b/ chatroom then began a "doxing"[7] campaign to wreck her reputation by sharing her naked photos with everyone she had even a slight connection with. Why? Because they could. The viciousness of it all needs to be recounted verbatim to be believed:

> Anonymous: "she gave her first name, her physician's full name, and even the dormitory area she lives in[.] [S]he wants to be found" (Bartlett 2014, 15).
>
> Anonymous: "here is a list of all her Facebook friends. You can message friends, and all their own friends, so that anyone with a slight connection to sarah [sic] via friend of friend knows" (ibid., 17-18).

[5] All currency in this paper is in US dollars.

[6] 4chan actually forbids users from posting using Tor or a virtual private network (VPN) to hide their true identities, so this example might seem slightly outside of the scope of the paper. It is, nevertheless, included for a couple of reasons. First, the extent to which the ban on Tor is followed or enforceable is quite unclear, and it is likely that many routinely violate it. Additionally, the nature of the 4chan board itself provides a degree of anonymity to posters, with users actually being told not to use any identifiable information in their profiles. So, even if the operators would (assuming the rule prohibiting Tor is followed) be able to backtrace posts to a particular person if law enforcement requested it, the ability of people to behave badly because of the anonymity of the board is still present.

[7] Doxing basically involves taking people's personal information and spreading it as widely as possible.

> Anonymous: "so has somebody started messaging her friends or family or can I begin with it? (ibid., 18).
>
> Anonymous: "[xxxxx] is her Fone [sic] number — confirmed" (ibid.).
>
> Anonymous: "just called her, she is crying. She sounded like a sad[,] sad sobbing whale" (ibid.)
>
> Anonymous: "Is anyone else continually calling?" (ibid.).

The attacks were personal, devastating and brutal. But the anonymous posters of the /b/ 4chan board were also remorseless.

> Anonymous: "If [she] was clever she would have g[ot] t[he] f[***] o[ut][,] she didn[']t, therefore she deserves the consequences" (ibid., 19).
>
> Anonymous: "I don't give a s*** what happens either. Bitch was camwhoring while she had a boyfriend" (ibid., 19).

The torment promised to be long-lived as well. Amid the maelstrom, Sarah had tried to minimize the damage by deleting her social media accounts, such as Facebook, to limit the trolls' access to the people she knew. But, as one troll noted, the Internet's memory is eternal:

> Anonymous: "Eventually once all this settles she will reactivate it [her Facebook account] and she will have her jimmies rustled once more. She will now never know peace from this rustling. And she's going to have one embarrassing f***ing time with her family" (ibid., 16).

It is sad to see even one life wrecked by a couple of bad choices that are then magnified by the destructive behaviour of anonymous trolls. But this case is in no way an isolated incident. One study found that upwards of two-thirds of people between the ages of 13 and 22 have been bullied online (Butterly 2013). And while certainly not all bullying goes on in the Dark Web — Facebook being a key vehicle of bullying — some of the most egregious often does. It is widespread, malicious and at times enabled by anonymity-granting tools like Tor. Its consequences are both individually and socially destructive.

With its illegal drug and weapon markets and online trolls, the Dark Web seems immoral and unscrupulous, but the scary part is that the shadows of the Dark Web can actually get even darker. Nothing makes that point more clearly than the prevalence of child abuse imagery on the Dark Net.

In 2011, Europol, coordinating with 13 national governments, launched Operation Rescue. The concerted law enforcement action uncovered 670 suspects and led to 184 arrests on child abuse imagery-related charges (Europol 2011). In July 2014, the UK's National Crime Agency arrested some 650 people on various child abuse charges, ranging from the possession of images to the actual abuse of minors (BBC 2014a). In 2015, another 50 suspects were identified in Northern Ireland and 37 charges were laid (BBC 2015). These are just a few examples of the successful instances of law enforcement uncovering pedophilia rings in the recesses of the Dark Web.

Unfortunately, as Gareth Owen and Nick Savage (2015) point out in their study for the Global Commission on Internet Governance, the problem of child abuse images on the Dark Web is probably even more widespread than the record of arrests would lead us to believe. In their innovative study, Owen and Savage actually volunteered a couple of servers to host the Tor network at their university in Portsmouth, United Kingdom. Over a period of several months, they categorized the type of websites found on the Tor-hosted Dark Web. They found that the available sites ranged from whistle-blower chatrooms to pornography sites, illegal markets and child abuse sites. This last category accounted for only a small fraction of all sites hosted on the Dark Web. Unfortunately, they also found that over 80 percent of the actual traffic along the Tor anonymity network went to this small proportion of sites (ibid.).

The lesson from all this is that anonymity allows the Dark Web to be a very nasty place indeed, and Tor makes this type of behaviour possible. Illegal markets selling drugs and guns to whomever will pay, malicious trolls and those who want to harm children, are but a few of the villainous activities going on within the lower recesses of the Internet.

The Virtuous Protection of the Shadows

But the anonymity of the technology of Tor cuts both ways — while people can use the network for villainous purposes, people can also use it for good.

Anonymity is important for the possibility of democracy. Anonymity provides space for people to think and voice opinions that are against the grain. Anonymity ensures both protection for an individual that holds a minority point of view and a window of opportunity for the majority consensus to be challenged by outside ways of thinking. As noted in a US Supreme court decision, *McIntyre v. Ohio Elections Commission*, "Anonymity is a shield from the tyranny of the majority….It thus exemplifies the purpose behind the Bill of Rights and of the First Amendment in particular: to protect unpopular individuals from retaliation…at the hand of an intolerant society" (cited in Electronic Frontiers Foundation, n.d.). Without a healthy public debate encompassing all viewpoints, democracy shrivels. In non-democratic countries, the presence of anonymity is the only way that people can voice contrary points of view against despotic regimes in the hope of securing political freedom.

For its part, the Tor Project website maintains that political activists, reformers, journalists, civil rights workers and development workers can use Tor in repressive countries to circumvent censorship and, to some extent, avoid the prying eyes of state and corporate surveillance. Use of the anonymity network has also been suggested by human rights groups. Reporters Without Borders, for example, recommends the use of Tor as a part of its journalist's "survival kit" (Murray 2014). In its somewhat older report on Internet usage in China, *Race to the Bottom*, Human Rights Watch supported the use of Tor (Human Rights Watch 2006). And the human rights advocacy group, Global Voices, suggests that Tor is useful for dissidents and activists (Global Voices, n.d.).

All of these suggestions for using the Tor network might or might not translate into people actually using it for noble purposes in regimes that mean harm to ordinary citizens. Unlike the high-profile instances of online drug busts and child pornography arrests, which are both on the moral high ground and newsworthy, there are few public stories of political activists using Tor. Repressive regimes do not broadcast when they break the encryption of the network and throw people who are simply asserting their right to free expression into dank prisons. Those who use Tor to avoid surveillance or to circumvent censorship are also not likely to publicly proclaim the specifics of their use of the network (or even that they use it at all), since the whole point of the system is to keep one's online activity anonymous.

There is another way, however, to discover whether people really do use the Tor Dark Web in repressive countries. Rather than have people self-report that they use the network, one can look at usage numbers per country. While many of the specifics are unknowable (as befits an anonymity network), the Tor Project provides data on the number of users of its network per country. Of course, each country has a different number of Internet users and different rates of Internet penetration, so you it isn't just a matter of counting the number of users and saying that the largest number of users are in either repressive or liberal regimes. Instead, to get at whether the level of political rights in a country drives usage of the Tor network, you need to use special statistical methods with a large sample size that can account for other factors that might also lead to people using the network. The process is not as complex as it sounds. At their most basic level, statistical methods can give you an impression of how often a certain level of political rights is associated with either high or low use of the Tor bridge network, given the effect of a host of other factors.

Before turning to the outcome of the statistical tests, it is a good idea to explain how statistical methods can produce some relatively intelligible answers. The basic question explored in another study (Jardine, n.d.) is whether people used Tor more as political repression increased from 2011 to 2013, which gets at the problem of whether the anonymity of the Dark Net can actually provide a cloak to protect those that want to exercise their rights to free speech and freedom of information.

On the one side, the political rights measure used in this study ranges along a scale from one to seven, and is taken from a widely used measure known as the Freedom in the World Index (Freedom House 2015). The index is scored like a game of golf: lower is better. A score of one, in this case, is the best, and a seven is the worst. Liberal democratic countries such as Canada, the United States and the United Kingdom score a one on the political rights index. Highly repressive countries such as Chad and Swaziland score a seven. The rest of the countries of the world are spread between these extremes.

The outcome to be explained is the use of the Tor network in different countries per year, with a specific focus on the use of what are known as bridges. Tor bridges are another name for the relay computers in the game of anonymous telephone. The one distinction is that unlike normal relays, bridges are not listed publicly, which makes them a better tool for people to circumvent censorship and surveillance in repressive regimes.

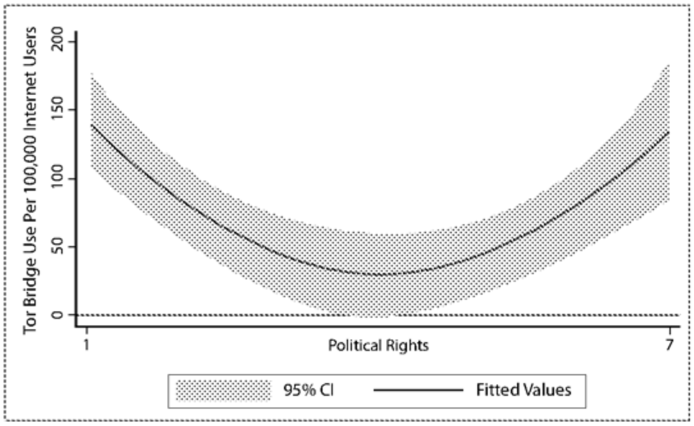
Since you would expect more people to use Tor (or for that matter anything) in a large population compared to a small one, the numbers for the outcome to be explained are expressed as a rate per 100,000 Internet users per year in a country. A simple example can demonstrate why normalizing the data in this manner is important: in 2013, the United States had 147,207 Tor bridge users, while Canada only had 23,795 users. On the face of it, it seems like Americans use the network a lot more than Canadians — and in one sense they do. But, as a population as a whole, America actually uses the network less. The United States has 55 Tor bridge users per 100,000 Internet users, while Canada has 79 users per 100,000 Internet users. Expressed in these terms, Canadians actually use Tor bridges at a 43.6 percent greater rate than their American cousins. The normalization matters.

Other factors in addition to political rights also drive use of the Tor network. So, to get a realistic picture of the effect of differing level of political rights, those conditions need to be factored into the equation. Wealth is important to take into consideration because it affects access to information technologies and national bandwidth capabilities. Internet penetration rates are important because someone needs to be able to access the Internet if they are going to actually use Tor. Exposure to foreign ideas and influences also matter, as people need to know about Tor in order to use it in the first place. Education matters because people need to have a certain level of comfort with information and communications technology in order to use something outside the norm such as Tor. Intellectual property rights regimes matter because they can increase the incentive to use Tor to download illegal movies and songs. The statistical tests include all these factors.[8]

Putting all these numbers to use and running some statistical regressions shows a clear relationship between Tor bridge use per 100,000 Internet users per year and a country's level of political rights. And while political rights do matter, they also *don't* matter in a straightforward way. Rather than use of the Tor network simply increasing as the political rights situation worsens in a country, the relationship between rights and the use of Tor is shaped like a "U." In other words, political rights tend to drive usage rates the most in both highly liberal countries such as Canada and highly illiberal countries such as Swaziland.

The figure below shows how the relationship unfolds across the actual data. As the political rights situation moves from a country such as the United States (political rights = 1) to a country such as Honduras (political rights = 4), political rights tend to drive use of the Tor network less and less. Beyond that low point, a worsening political rights situation starts to drive people toward using the Tor network again, as evidenced by the right hand side of the U-shaped relationship.

Figure 1: Political Rights and Tor Bridge Usage



Source: Jardine (n.d.).

The magnitude of the effect is knowable, too. The table below shows on average just how much a change in the level of political rights in a country matters. Moving from a 1 to a 4 on the political rights scale results in a total reduction of 174.99 users of Tor bridges per 100,000 Internet users per year. Going the other way, from a 5 to a 7 on the political rights scale, leads to a total increase of 68.42 Tor bridge users per 100,000 Internet users per year. In short, political rights matter a fair bit for use of the network.

Table 1: Changing Political Rights and Tor Bridge Use per 100,000 Internet Users per Year

Change in political rights	Change in Tor bridge users per 100,000 Internet users
1 to 2	84.77 less
2 to 3	58.33 less
3 to 4	31.89 less
4 to 5	5.45 less
5 to 6	20.99 more
6 to 7	47.43 more

Source: Jardine (n.d.).

The obvious question at this stage is why do political rights matter in this way? Why form a U-shaped relationship? The reason is that a political regime drives the domestic population's opportunity to use Tor, as well as their need to do so, with the former factor declining as repression increases and the latter rising as political rights decline.

Opportunity, for instance, starts out high in liberal countries, as there are few restrictions on the use of encrypted or anonymous technologies such as Tor. Indeed, a large portion of the Tor Project's funding comes from the US government and the genesis of the program is in US military research labs. As the level of political rights declines, the opportunity to use the anonymity-granting technology worsens, as repressive regimes throw up roadblocks — for example, legislation and technical blocking mechanisms — to prevent people from using the system. China, for instance, has been fairly successful at blocking Tor (MIT Technology Review 2012). Russia, a six on the political rights scale, has offered $110,000 to the person or organization that can crack the encryption and anonymity of the Tor network (BBC 2014b).

Opportunity counts for a lot, so, if it is nearly costless to do so, people will use programs such as Tor for illegal reasons, to circumvent censorship and surveillance by both states and corporations, or simply to support the idea that the anonymous use of the Internet should be something that is valued in society. The result of high opportunity is the high use of anonymity-granting technologies in highly liberal countries.

Need, for its part, is low in liberal countries. People don't have to use Tor in order to do their legal online activity in liberal countries with a strong tradition of rights protection, although the extent to which people should take more steps to be anonymous online, even in liberal regimes, is an open question. As the level of political repression goes up within a country, the need to use anonymity-granting programs like Tor rises.

[8] Issues of multicollinearity are discussed in detail in Jardine (n.d.).

This growing need drives people to use Tor in repressive regimes. Here again, the motives vary. Some will do so for illegal purposes. But others will use the network to blow the whistle on corruption, to freely express their political viewpoints, to circumvent censorship and to avoid direct surveillance of their online activity.[9]

The basic point is that repression and the violation of political rights does drive people to use the anonymity network. Oftentimes, people in repressive regimes simply cannot freely express their points of view, circumvent the censorship of important information or avoid the prying eyes of the state without encrypted and anonymous programs such as Tor. Some of what people do online with Tor in repressive regimes will be innocuous and some will even be illicit or illegal, but much of it will be virtuous and aimed at nothing more than exercising some fundamental political rights.

THE POLICY DILEMMA: A DUAL-USE TECHNOLOGY

As demonstrated, Tor is basically a dual-use technology: it can be used for truly awful purposes as well as for good. How it is used matters most, similar to other tools that humanity has invented. We discovered how to harness fire to keep us warm, but then learned that it can be used to ravage and burn. We discovered steel and now use it to make buildings that touch the sky, but before that we learned it can be used to make swords or guns to take lives. The human story is riddled with the invention of technologies that can be used for both good and ill.

Discussions of the use of the Tor network, like discussions of encryption in general, are highly polarized. The one side asserts that the technology needs to be as close to unbreakable as possible so that nefarious actors cannot gain access. A back door into an encrypted system cannot be given only to law enforcement and somehow kept from criminals and political despots. Once an entryway exists, the system is vulnerable. Indeed, purposeful back doors can lead to less privacy, more vulnerabilities as new systems interact with past software and even make governments and service providers tantalizing targets of cybercrime, as they possess the proverbial keys to the kingdom (Abelson et al. 2015).

The other side of the debate asserts that encrypted and anonymous technologies such as Tor hinder law enforcement. FBI Director James B. Comey exemplifies this position. In October 2014, he pointed straight to the other half of the polarization in a speech at the Brookings Institution in Washington, DC:

> Encryption isn't just a technical feature; it's a marketing pitch. But it will have very serious consequences for law enforcement and national security agencies at all levels. Sophisticated criminals will come to count on these means of evading detection. It's the equivalent of a closet that can't be opened. A safe that can't be cracked. And my question is, at what cost? (Comey 2014)

Indeed, at what cost? In one way, the policy issue as it specifically relates to the Tor network boils down to a question about whether the technology does more harm than good. What matters is a net assessment of the impact of the technology. There is no straightforward answer to this question, but the evidence presented here suggests a painful underlying truth — how you frame the parameters of the cost-benefit calculus affects the answer you get.

The uncomfortable reality is that liberal democratic nations that developed and host much of the Tor network are actually having to deal with most of the negative consequences of the system while reaping few of the benefits. The opportunity to use the technology in liberal countries means that Silk Road, trolls and anonymous child abuse websites proliferate, but the gains (dodging the prying eyes of state or corporate content surveillance and circumventing censorship) are fairly minimal. Other, less cumbersome programs (private search engines, such as Duck Duck Go, and VPNs) exist and have roughly the same effect as Tor with more download speed and less potential for abuse, as they retain user data and can cooperate with law enforcement if approached with a valid warrant. Therefore, unless people are engaged in outright illegal activities, the need to use a full-blown anonymity program such as Tor in liberal democratic countries is also limited, because of the presence of constitutional and legal protections of citizen rights, although it is important to not under-represent the extent to which the rapidly evolving nature of the technology of the Internet has outpaced the ability of the legal system to deal with new challenges to citizen's fundamental rights. Based upon the evidence presented above, the idea that Tor provides net benefits to society in liberal democratic countries is unlikely. It most likely does more harm than good.

If the frame of reference is shifted to the net costs or benefits of Tor in a highly repressive country, however, the cost-benefit outcome changes radically. Dissidents, journalists, human rights activists and even ordinary citizens in repressive countries all benefit from the Tor network, even if some of these people might use it for nefarious purposes. In the end, the Tor anonymity network in regimes with low political rights is definitely more beneficial overall.

[9] Because Tor has distinct encryption, repressive regimes can often tell when someone is using the program, even if they cannot tell what is being done with the system. Paradoxically, this effort to dodge surveillance of content might put an individual under more scrutiny as the use of encrypted technologies raises red flags in many repressive regimes.

The implicit policy question to come out of this is whether people in liberal countries are willing to pay the cost of the existence of a system such as Tor, given that the benefits are not evenly distributed globally. People in Western countries might decide that the costs are simply not worth it and opt for a state-driven clamp down on the system. This decision would have serious implications for the effectiveness of the Tor network as it functions well in repressive regimes only because most of its infrastructure (computers and servers) reside in liberal countries. Without innumerable volunteered computers around the world, the anonymity of the network would be limited and the ability of Tor to cloak those in need in repressive regimes would be stymied.

WHAT IS TO BE DONE? POLICING

Even if people in liberal countries decide that a program such as Tor is not worth having, the odds of destroying anonymity-granting technologies in general in an era of a global Internet are pretty slim. Tor might be knocked offline, but other programs would simply emerge and take their place. Unless you break the global Internet (which would be excessively expensive in terms of lost GDP), it is simply not possible to prevent people from building technologies that ensure the anonymous use of the Web. In other words, the problem of a dual-use technology like Tor is not likely to go away any time soon. We are stuck with both the good and the bad.

Rather than looking for quick and final fixes (such as destroying Tor outright or altering the technology through back doors in encryption for law enforcement), a more realistic way forward is to focus on actively policing the network.

In the offline world, peace and order are maintained in every segment of society through judicious policing. Socially destructive behaviours are deemed illegal. Crimes are recorded. And criminals are arrested, prosecuted and sent to jail. It is actually ridiculous to think that as more of our daily lives and activities shift online, the online world would not also need to see a rapid expansion of policing efforts to accommodate the shift in our attention and activity.

There has already been some movement in this direction by police forces around the world (Omand, forthcoming). This movement shows that online policing of the Dark Web is in fact possible, expedient and often at least as effective as offline policing.

Despite the use of the Tor network to host the various Silk Road illegal marketplaces, for example, the owners and operators of the sites — as well as many of the largest sellers — were identified and arrested. These arrests show the effectiveness of online policing. The takedown of Silk Road 1.0 is instructive. Police caught the Dread Pirate Roberts through a combination of technological means and the double-edged sword of online anonymity.

Tor is obviously a technically heavy system.And technology played a role in the capture of the server hosting the Silk Road and the ultimate arrest of Ross Ulbricht. In the initial prosecution filing against Ulbricht, the FBI indicated that it found the location of the Silk Road server in Iceland due to a misconfiguration on the illegal market's login page, which allowed investigators to type in "miscellaneous" characters in a CAPTCHA window that returned IP address information.[10] Upon further snooping, the FBI realized that the IP address provided by the login page did not correspond to a known node in the Tor network, and was likely the actual physical address of Silk Road rather than a relay in the system (Greenburg 2014a). Technology is a fickle mistress and it betrayed those that were relying upon it to do harm.

Of course, others doubt whether the characters typed into the CAPTCHA by the FBI were really miscellaneous, charging instead that they were actually lines of code designed to hack the login page by duping it into thinking the entries were actually administrative commands (Greenburg 2014b). Both accounts are plausible. Silk Road 2.0, for example, wasn't vulnerable to the same flaw, suggesting either that Silk Road 1.0 was taken down by a configuration issue or perhaps by a now-patched vulnerability (Brandom 2015). Indeed, Ulbricht's defence during his trial that there was an illegal search due to how the FBI found the Silk Road server fell apart. He was sentenced to more than life in prison (Thielman 2015).

Silk Road 1.0 was also taken down because of the very thing that allowed it to operate in the first place: anonymity. Anonymity, that core feature provided by the Tor browser, doesn't stop law enforcement. Instead, it actually makes law enforcement efforts, in some ways, easier. Buyers or sellers on Silk Road, trolls and child abusers cannot say for sure who they are dealing with in an online world. Anonymity limits attribution, but it cuts both ways. No further evidence is needed than the Dread Pirate Roberts, who offered money to an undercover cop to undertake an assassination of a former site administrator. Child abuse sites are also routinely infiltrated by law enforcement. Police from the United Kingdom and Australia, for example, infiltrated one online child abuse ring of up to 70,000 members "to identify the members who posed the greatest danger to children. Police also sometimes posed as children online as part of the investigation" (NBC News, n.d.).

Online policing is also as expedient as offline policing. The anonymity of Tor does not necessarily slow down law

[10] CAPTCHAs are those website windows with blurry letters and numbers that are designed to fool spamming machines, but allow humans to access a site.

enforcement efforts. The fact that the Silk Road networks were taken down, often within a year of their launches, shows the speed at which online policing can work. As a parallel analogue example, Project DISTRESS was launched in Manitoba, Canada, in October 2013, and culminated 15 months later in the arrest of 14 suspects in a major drug trafficking ring (RCMP 2014). The scope of this real-world effort is smaller than Operation Marco Polo to take down Silk Road 1.0, but the timelines are roughly the same. If anything, the online version was a larger endeavour but took less time to complete. Online policing seems to be at least as quick as its analogue cousin.

The fact that new Silk Road marketplaces, trolls or child abuse sites keep popping up in the wake of arrests and shutdowns is also nothing new, and should not be taken as evidence that online policing is not effective. Offline, the arrest of a street-corner drug dealer often leaves a void that is quickly filled by someone else. This doesn't mean that we should stop arresting drug dealers. It means that we are stuck with the problem of people selling drugs, at least until the demand for what is being sold goes away or the arrest and prosecution for such activity is certain. The same logic applies online. Yes, new sites will always pop up as the old ones are taken down and arrests are made, but this just means that governments need to keep policing the network. It is part of the cost of the Internet. To obtain all the benefits that the Internet provides, we need to ensure it is as safe as possible, but we don't want to destroy it completely, which is the only way prevent crime from occurring online.

The call for greater online policing is not the same as saying the state should be allowed to intervene indiscriminately into people lives. Offline, the police cannot go into people's homes whenever they want, but they can patrol the streets and catch people in the act of committing crimes. The same sort of logic should apply online. Police should not be allowed to access the data on a person's computer or their ISP records without a warrant. At the same time, they are allowed to sit in chatrooms to monitor conversations and even pose as potential victims to catch predators. They are also allowed to pose as sellers or buyers on illegal markets to track down people who are actually committing crimes. In short, the new "beat" is shifting from the street to the websites and chatrooms of the Internet. This is the reality of the digital age. Certain tactics remain off limits — and law enforcement should not purposefully take advantage of the presence of legal ambiguity to overreach — but the Internet won't work as a global free-for-all.

This policing should also avoid politicizing the core infrastructure of the Internet. As Samantha Bradshaw and Laura DeNardis (n.d.) note, attempting to police intellectual property rights regimes, for example, through the core infrastructure of the Internet (in their case, the Domain Name System) can lead to unintended consequences that risk damaging or even breaking the network. Instead, policing of the Dark Web should occur largely on top of the infrastructure at the social or content level. Law enforcement officers should have a presence inside an online chatroom frequented by pedophiles, but they should not manipulate the infrastructure that supports the creation of online chatrooms in the first place.

There is a bit of a tension between the legitimate use of technological methods to identify those that are breaking the law and the idea that manipulating core infrastructure should be off limits. The use of technology to fight crime falls along a continuum. At one end are legitimate technical investigations, such as the methods used to take down Silk Road 1.0. This kind of activity is acceptable because it exploited a weakness in a particular site, rather than trying to break the whole system. At the other end, trying to simply knock Tor offline is a more fundamental politicization of the infrastructure of the system, affecting both the good and the bad indiscriminately, and therefore should be disallowed.

At the margin, there is a lot of ambiguity about what is acceptable. The takedown of Silk Road 2.0 points out the blurry line. To identify the users of Silk Road 2.0, the FBI volunteered "reliable IP addresses" to the Tor hidden services network upon which the newest incarnation of the illegal marketplace was based. This allowed the FBI to subtly change the coding so that they could pinpoint the identity of users that had employed their relays to reach the illegal marketplace. The operators of Tor noted this trick after six months, and provided a patch that once again improved the anonymity of Tor. For Silk Road 2.0 and Blake Benthall, it was too late. The FBI had tracked down the server and 78 sellers and buyers (Brandom 2015). Exploiting the voluntarist nature of the Tor infrastructure is right at the line of unacceptable use of core infrastructure for policing. It was an indiscriminate attack on all Tor users, so it probably went a bridge too far. Either way, the Silk Road 2.0 example highlights the tension.

LIMITATIONS TO ONLINE POLICING AND AREAS FOR POLICY INTERVENTION

There are limits to the effectiveness of online policing that concerted policy actions can help to overcome.

One limitation is that online criminals can be global, even while most law enforcement agencies (Interpol excepted) are local. If a criminal is not in the same jurisdiction as the police that identify his or her actions as illegal, policing gets immensely more complicated. The problem is even more pronounced when Tor bounces your signal around the world, effectively involving multiple jurisdictions. In some cases, policies are in place to allow states to cooperate by sharing evidence across borders. Foremost among these mechanisms are what is known as mutual legal assistance treaties (MLATs).

The problem is the MLAT process is in massive need of reform. Proposals exist for how it should be reformed. One study maintains that MLAT reform must emphasize proportionality, the protection of human rights, transparency, heightened efficiency and scalability if they are to become an effective tool in the international police officer's tool kit (Woods 2015). That would be a good start.

MLAT reform can certainly help to make the process of Internet policing more effective, but it won't solve the root of the problem, as online crime is highly mobile and can drift to countries that are outside of the effective MLAT regime. For MLATs to work, two states need to have an agreement in place and both need to view something as illegal in order for the process to be effective. Cooperation through the MLAT process is quite likely between liberal democratic countries because they share legal principles and political dispositions. Cooperation on cybercrime is less likely between Western countries and nations such as China and Russia, which disagree on so many fundamental issues. Moreover, at the end of the day, MLAT reform might fail as the Internet governance system is becoming increasingly contentious (Bradshaw et al. 2015). This is not a small hurdle, but it is not insurmountable either.

Other specific efforts at international coordination of law enforcement agencies can do nothing but help. Interpol's Global Complex for Innovation is a prime example. It aims to build relationships between police forces, increase various countries' understanding of digital security issues and facilitate capacity building to overcome the fact that many local and national police forces just don't have the resources, training and wherewithal to deal well with cybercrime. More international coordination should help with the trans-border portion of the cybercrime problem.

But coordination failures are not just a problem between nations. Most countries have internal layers of police, ranging from the national to the local. Coordination failures between these levels can often stymie effective efforts at policing cybercrime. Local and national police have both critical resources and deficiencies in the battle against cybercrime. Local police can often be the first to learn of a cybercrime (say, identity theft or cyber harassment), but often lack the capacity and jurisdiction to act effectively.[11] National law enforcement usually has the capacity and jurisdiction to act effectively, but can lack knowledge that a particular cybercrime is occurring.

The strengths and weaknesses of local and national-level law enforcement are complementary. By working together, the knowledge of local police can be paired with the resources and capacity of national law enforcement. Specialization remains efficiency-enhancing here, so local police should not be trying to bust international online fraud rings and national-level law enforcement should not be trying to get local victims to report crimes directly to them (although national-level crime reporting is increasingly effective at scale). Each level should stick to its strengths, but work together in a coordinated way to limit online crime.

Even with greater coordination, more training and capacity are still needed. Local law enforcement, in particular, tends to be undertrained and under-resourced to deal with cybercrime. As Darrel Stephens, executive director of the Major City Chiefs Police Association, noted in 2013, "Most local police do not have the capacity to investigate these cases even if they have jurisdiction" (cited in Sullivan 2013). Stephens is also cognizant of how local police departments will need to adapt, stating further that, "Police will need to become more equipped to deal with cybercrime in the future" (ibid.). And that "most major cities have a limited capability, but more will be required" (ibid.). Many crimes are shifting online, so resources that are otherwise dedicated to policing offline crime could be usefully moved to combat online crime instead. Even with the redistribution of efforts, more resources are needed to effectively combat online crime.

Obtaining more resources at the local level is likely to come with some growing pains. More resources typically follow greater need, but local police face a perverse incentive when it comes to something as foundational to crime fighting as recording that a crime has even occurred. A physical burglary or violent crime in a jurisdiction will faithfully be recorded accurately and quickly in most cases. A cybercrime of harassment or theft is far less likely to be counted. The reason is that it is harder for local police to address these crimes, given resources, capacity and the jurisdiction in which they work. As a result, these crimes are more likely to remain off the books.[12] To include them would inflate the crime rate in an area and probably the unsolved crime rate as well, all of which reflects poorly upon the local police department.

However, by trying to avoid a rising crime rate, local law enforcement is hamstrung in their ability to solicit or collect new resources or capacity over the long term. Heads might roll if the crime rate goes up in the short run, but this could be a window of opportunity for local police departments that need more training and resources to combat cybercrime. In most cases, a growing need (higher crime rates) is matched with more resources. In the long term, the only way to strengthen local police departments to

[11] Many countries have national-level information collection agencies, so information about ongoing crimes is not always clustered at the local level. This varies by country and likely by crime type as well.

[12] At the 2015 Global Conference on Cyberspace in The Hague, Richard Clayton pointed out that this happens. To the extent that I may have misunderstood his point, the fault is my own.

help them fight cybercrime is to recognize that cybercrime has local victims, even if perpetrators could be anywhere in the world and the jurisdictional lines are blurry.

Increasingly, coordination must also occur between governments and private sector actors. One example of this coordination in action is the recent breakup of a large botnet by European law enforcement and Microsoft (Microsoft News Center 2013). Private companies own and operate much of the software, hardware and networks of the Internet, while law enforcement has the jurisdiction to pursue criminals. Public-private partnerships between law enforcement and private companies will likely be the way of the future. When done well, public-private collaboration can be a massive force multiplier, leading to the more effective policing of the Dark Web.

Policing anonymity-granting technologies is also challenging because the system is decentralized, based upon volunteered servers and does not retain data. The messaging application Wickr is an analogous example. They will readily comply with warrants that require access to their servers; however, since they do not retain any data generated by the users of their service, law enforcement cannot find any useful information by searching the system. Tor is similar in that it does not retain data. Additionally, the volunteered nature of the network means that even if someone were logging traffic through Tor relays (which the system is not designed to do), law enforcement in any one country would be hard pressed to find this data. Changing the legal rules so that companies and organizations such as Tor would be required to retain data for a period of time — for instance, six months — would be one way to allow for semi-anonymous communications, but ensure that when law enforcement is cued to a potential crime, they can get access to what they need. The big problem with this approach is how it would be applied in repressive regimes. In those countries, even a six-month retention of data can lead to imprisonment for activists, journalists and human rights workers. As a result, those behind Tor would never accept a mandated retention period of data.

A final limitation is that cybercrime is rapidly increasing, which threatens to overwhelm any and all available policing capacity of nations. Cybercrime is certainly going up, but it is not as bad as we commonly think it is. The key reason is that cyberspace is actually growing as fast, and sometimes faster, as the growth in new vulnerabilities, web-based attacks and the costs of cybercrime. In other words, the rate of crime is not as bad as the picture often portrayed in the media and is, in some cases at least, even improving (Jardine 2015). In other words, law enforcement still has a reasonable chance, and is doing a fairly good job, of holding web-based crime at bay. Policing the Dark Web can be successful.

CONCLUSION

Overall, Internet policing is maybe not ideal. It would be better if people just stopped using anonymity networks such as Tor to do illegal things. That would allow the network to be used to circumvent censorship and surveillance in repressive countries without any of the socially damaging spillover that online anonymity produces.

The network is fragile, despite its resilience, and if we try to find a quick and easy technological fix to problems that are actually social, we run the very real risk of breaking the Internet. Rather than discarding Tor or breaking the anonymity and encryption of the system through back doors for law enforcement, the focus should instead be on policing what goes on upon the network itself. Policing has the advantage of minimizing the costs that the Dark Web imposes on society, while allowing the Dark Web to have the maximum potential positive effect globally. It is not perfect, but it is the best we can probably do.

Acknowledgements

This paper has benefitted from the eyes of, in no particular order, Secretary Michael Chertoff, Laura DeNardis, Bill Graham, Gordon Smith, Pindar Wong and Leanna Ireland. It has also been polished by Carol Bonnett and Vivian Moser. Despite the collective wisdom of all these eyes, problems might linger. These are my errors alone.

WORKS CITED

Abelson, Harold, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter and Daniel J. Weitzner. 2015. *Keys Under the Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*. Computer Science and Artificial Intelligence Laboratory Technical Report. http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8.

Bartlett, Jamie. 2014. *The Dark Net: Inside the Digital Underworld*. London, UK: William Heinemann.

BBC. 2014a. "Child abuse image investigation leads to 660 arrests." BBC News, July 16. www.bbc.com/news/uk-28326128.

———. 2014b. "Russia Offers $110,000 to Crack Tor anonymous Network." BBC News, July 28. www.bbc.com/news/technology-28526021.

———. 2015. "50 arrests in NI online abuse images probe in past year, say police." BBC News, March 15. www.bbc.com/news/uk-northern-ireland-31896685.

Bradshaw, Sam and Laura DeNardis. n.d. "The Politicization of the Internet's Domain Name System: Implications for Internet Security, Universality, and Freedom." Unpublished manuscript.

Bradshaw, Sam, Laura DeNardis, Fen Hampson, Eric Jardine and Mark Raymond. 2015. "The Emergence of Contention in Global Internet Governance." Global Commission on Internet Governance Paper Series No. 17. https://ourinternet-files.s3.amazonaws.com/publications/no17.pdf.

Brandom, Russel. 2015. "Feds found Silk Road 2 servers after a six-month attack on Tor." The Verge, January 21. www.theverge.com/2015/1/21/7867471/fbi-found-silk-road-2-tor-anonymity-hack.

Butterly, Amelia. 2013. "'Growing trend' of cyberbullying on social networks." BBC News, October 2. www.bbc.co.uk/newsbeat/article/24364361/growing-trend-of-cyberbullying-on-social-networks.

Chertoff, Michael and Tobby Simon. 2015. "The Impact of the Dark Web on Internet Governance and Cyber Security." Global Commission on Internet Governance Paper Series No. 6. https://ourinternet-files.s3.amazonaws.com/publications/GCIG_Paper_No6.pdf.

Christin, Nicolas. 2012. "Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace." Working paper, November 30. http://arxiv.org/pdf/1207.7139.pdf.

Comey, James. C. 2014. "Speeches." www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

Cook, James. 2014. "FBI Arrests Former SpaceX Employee, Alleging He Ran The 'Deep Web' Drug Marketplace Silk Road 2.0." Business Insider, November 6. www.businessinsider.com/fbi-silk-road-seized-arrests-2014-11.

Electronic Frontiers Foundation. n.d. "Anonymity." www.eff.org/issues/anonymity.

Europol. 2011. "Operation Rescue." www.europol.europa.eu/content/operation-rescue.

Freedom House. 2015. "Freedom in the World: Aggregate and Subcategory Scores." https://freedomhouse.org/report/freedom-world-aggregate-and-subcategory-scores#.Va6gr_lVhBc.

Global Voices. n.d. "Anonymous Blogging with WordPress & Tor – ARCHIVED." Global Voices.

Greenburg, Andy. 2014a. "The FBI Finally Says How It 'Legally' Pinpointed Silk Road's Server." Wired, September 5. www.wired.com/2014/09/the-fbi-finally-says-how-it-legally-pinpointed-silk-roads-server/.

———. 2014b. "FBI's Story of Finding Silk Road's Server Sounds a Lot Like Hacking." Wired, September 8. www.wired.com/2014/09/fbi-silk-road-hacking-question/.

Human Rights Watch. 2006. *Race to the Bottom: Corporate Complicity in Chinese Internet Censorship*. Human Rights Watch. www.hrw.org/reports/2006/china0806/china0806webwcover.pdf.

Jardine, Eric. 2015. "Global Cyberspace is Safer than You Think: Real Trends in Cyberspace." Global Commission on Internet Governance Paper Series No. 16. https://ourinternet-files.s3.amazonaws.com/publications/no-16_Web.pdf.

———. n.d. "Tor, What is it Good For? Political Rights and the Use of Anonymity-Granting Technologies." Unpublished paper.

Knibbs, Kate. 2014. "Silk Road 3 Is Already Up, But It's Not the Future of Darknet Drugs." Gizmodo, November 7. http://gizmodo.com/silk-road-3-is-already-up-but-its-not-the-future-of-da-1655512490.

Koebler, Jason. 2012. "Online Black Market Drug Haven Sees Growth Double." *U.S. News*, August 7. www.usnews.com/news/articles/2012/08/07/online-black-market-drug-haven-sees-growth-double.

Microsoft News Center. 2013. "Microsoft, the FBI, Europol and Industry Partners Disrupt the Notorious ZerAccess Botnet." December 5. https://news.microsoft.com/2013/12/05/microsoft-the-fbi-europol-and-industry-partners-disrupt-the-notorious-zeroaccess-botnet/.

MIT Technology Review. 2012. "How China Blocks the Tor Anonymity Network." April 4. www.technologyreview.com/view/427413/how-china-blocks-the-tor-anonymity-network/.

Murray, Andrew. 2014. "The dark web is not just for paedophiles, drug dealers and terrorists." *The Independent*, August 18. www.independent.co.uk/voices/comment/the-dark-web-is-not-just-for-paedophiles-drug-dealers-and-terrorists-9920667.html.

NBC News. n.d. "Massive Online Pedophile Ring Busted by Cops." www.nbcnews.com/id/42108748/ns/us_news-crime_and_courts/t/massive-online-pedophile-ring-busted-cops/#.VcirBPlVhBc.

Omand, David. forthcoming. "The Dark Net: Policing the Internet's Underworld." *World Policy Journal.*

Owen, Gareth and Nick Savage. 2015. *The Tor Dark Net.* Global Commission for Internet Governance Paper Series No. 20.

RCMP. 2014. "Project DISTRESS." www.rcmp-grc.gc.ca/mb/news-nouvelles/2014/project-projet-distress-20141211-eng.htm.

Sullivan, Eileen. 2013. "Local Police Get Into Cybercrime Fighting Business." *Huffington Post Tech*, April 13. www.huffingtonpost.com/2013/04/13/police-cybercrime_n_3075427.html.

Thielman, Sam. 2015. "Silk Road operator Ross Ulbricht sentenced to life in prison." *The Guardian*, May 29. www.theguardian.com/technology/2015/may/29/silk-road-ross-ulbricht-sentenced.

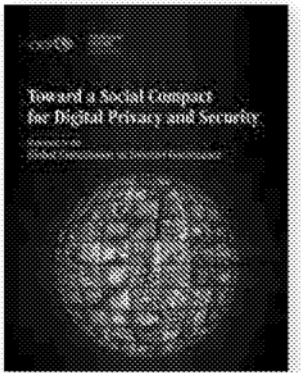
Woods, Andrew. 2015. *Data Beyond Borders: Mutual Legal Assistance in the Internet Age*. Global Network Initiative. January. https://globalnetworkinitiative.org/sites/default/files/GNI%20MLAT%20Report.pdf.

Zetter, Kim. 2013. "How the Feds Took Down the Silk Road Drug Wonderland." *Wired*, November 18. www.wired.com/2013/11/silk-road/.

CIGI PUBLICATIONS
ADVANCING POLICY IDEAS AND DEBATE

Global Commission on Internet Governance

The Global Commission on Internet Governance (GCIG) was established in January 2014 to articulate and advance a strategic vision for the future of Internet governance. The two-year project conducts and supports independent research on Internet-related dimensions of global public policy, culminating in an official commission report that will articulate concrete policy recommendations for the future of Internet governance. These recommendations will address concerns about the stability, interoperability, security and resilience of the Internet ecosystem. Launched by two independent global think tanks, the Centre for International Governance Innovation and Chatham House, the GCIG will help educate the wider public on the most effective ways to promote Internet access, while simultaneously championing the principles of freedom of expression and the free flow of ideas over the Internet.

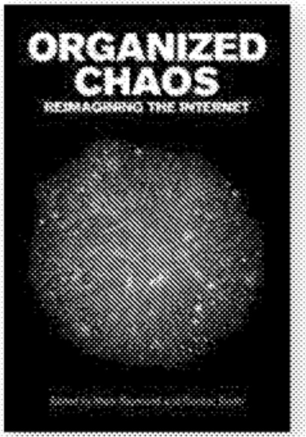


Toward a Social Compact for Digital Privacy and Security

Statement by the Global Commission on Internet Governance

On the occasion of the April 2015 Global Conference on Cyberspace meeting in The Hague, the Global Commission on Internet Governance calls on the global community to build a new social compact between citizens and their elected representatives, the judiciary, law enforcement and intelligence agencies, business, civil society and the Internet technical community, with the goal of restoring trust and enhancing confidence in the Internet. It is now essential that governments, collaborating with all other stakeholders, take steps to build confidence that the right to privacy of all people is respected on the Internet. This statement provides the Commission's view of the issues at stake and describes in greater detail the core elements that are essential to achieving a social compact for digital privacy and security.

Available for free download at www.cigionline.org/publications



Organized Chaos

CDN$25

Edited by Mark Raymond and Gordon Smith

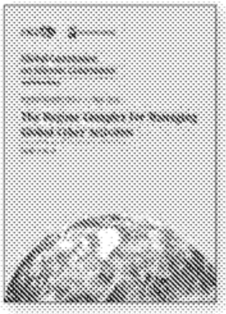
Anonymous. Cybercrime. Hacktivist. Cyber security. Now part of the lexicon of our daily language, these words were unknown a decade ago. The evolution and expansion of the Internet has transformed communication, business and politics, and the Internet has become a powerful influence on everyday life globally. But the Internet is a medium that is not controlled by one centralized system, and the debate over who will govern the Internet has commanded attention from a wide range of actors, including states, policy makers and those beyond the traditional tech industries.

Organized Chaos: Reimagining the Internet examines the contemporary international politics of Internet governance problems, exploring issues such as cybercrime, activities of the global hacktivist network Anonymous and "swing states," and highlighting central trends that will play a role in shaping a universal policy to govern the Internet. In this book, some of the world's foremost Internet governance scholars consider the critical problems facing efforts to update and refine Internet governance at an international level and the appropriate framework for doing so. This volume provides the basis for developing a high-level strategic vision required to successfully navigate a multi-faceted, shifting and uncertain governance environment.

Available for purchase at www.cigionline.org/bookstore

CIGI Centre for International Governance Innovation
www.cigionline.org

GLOBAL COMMISSION ON INTERNET GOVERNANCE PAPER SERIES



The Regime Complex for Managing Global Cyber Activities
GCIG Paper Series No. 1
Joseph S. Nye, Jr.

Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate
GCIG Paper Series No. 2
Tim Maurer and Robert Morgus

Legal Mechanisms for Governing the Transition of Key Domain Name Functions to the Global Multi-stakeholder Community
GCIG Paper Series No. 3
Aaron Shull, Paul Twomey and Christopher S. Yoo

Legal Interoperability as a Tool for Combatting Fragmentation
GCIG Paper Series No. 4
Rolf H. Weber

Innovations in Global Governance: Toward a Distributed Internet Governance Ecosystem
GCIG Paper Series No. 5
Stefaan G. Verhulst, Beth S. Noveck, Jillian Raines and Antony Declercq

The Impact of the Dark Web on Internet Governance and Cyber Security
GCIG Paper Series No. 6
Tobby Simon and Michael Chertoff

On the Nature of the Internet
GCIG Paper Series No. 7
Leslie Daigle

Understanding Digital Intelligence and the Norms That Might Govern It
GCIG Paper Series No. 8
David Omand

ICANN: Bridging the Trust Gap
GCIG Paper Series No. 9
Emily Taylor

A Primer on Globally Harmonizing Internet Jurisdiction and Regulations
GCIG Paper Series No. 10
Michael Chertoff and Paul Rosenzweig

Connected Choices: How the Internet is Challenging Sovereign Decisions
GCIG Paper Series No. 11
Melissa E. Hathaway

Solving the International Internet Policy Coordination Problem
GCIG Paper Series No. 12
Nick Ashton-Hart

Net Neutrality: Reflections on the Current Debate
GCIG Paper Series No. 13
Pablo Bello and Juan Jung

Addressing the Impact of Data Location Regulation in Financial Services
GCIG Paper Series No. 14
James M. Kaplan and Kayvaun Rowshankish

Cyber Security and Cyber Resilience in East Africa
GCIG Paper Series No. 15
Iginio Gagliardone and Nanjira Sambuli

Global Cyberspace Is Safer than You Think: Real Trends in Cybercrime
GCIG Paper Series No. 16
Eric Jardine

The Emergence of Contention in Global Internet Governance
GCIG Paper Series No. 17
Samantha Bradshaw, Laura DeNardis, Fen Osler Hampson, Eric Jardine and Mark Raymond

Landmark EU and US Net Neutrality Decisions: How Might Pending Decisions Impact Internet Fragmentation?
GCIG Paper Series No. 18
Ben Scott, Stefan Heumann and Jan-Peter Kleinhans

The Strengths and Weaknesses of the "Brazilian Internet Bill of Rights": Examining a Human Rights Framework for the Internet
GCIG Paper Series No. 19
Carolina Rossini, Francisco Brito Cruz, Danilo Doneda

The Tor Dark Net
GCIG Paper Series No. 20
Gareth Owen and Nick Savage

Available for free download at www.cigionline.org/publications

CIGI
Centre for International Governance Innovation
www.cigionline.org

ABOUT CIGI

The Centre for International Governance Innovation is an independent, non-partisan think tank on international governance. Led by experienced practitioners and distinguished academics, CIGI supports research, forms networks, advances policy debate and generates ideas for multilateral governance improvements. Conducting an active agenda of research, events and publications, CIGI's interdisciplinary work includes collaboration with policy, business and academic communities around the world.

CIGI's current research programs focus on three themes: the global economy; global security & politics; and international law.

CIGI was founded in 2001 by Jim Balsillie, then co-CEO of Research In Motion (BlackBerry), and collaborates with and gratefully acknowledges support from a number of strategic partners, in particular the Government of Canada and the Government of Ontario.

Le CIGI a été fondé en 2001 par Jim Balsillie, qui était alors co-chef de la direction de Research In Motion (BlackBerry). Il collabore avec de nombreux partenaires stratégiques et exprime sa reconnaissance du soutien reçu de ceux-ci, notamment de l'appui reçu du gouvernement du Canada et de celui du gouvernement de l'Ontario.

For more information, please visit www.cigionline.org.

ABOUT CHATHAM HOUSE

Chatham House, the Royal Institute of International Affairs, is based in London. Chatham House's mission is to be a world-leading source of independent analysis, informed debate and influential ideas on how to build a prosperous and secure world for all. The institute: engages governments, the private sector, civil society and its members in open debates and confidential discussions about significant developments in international affairs; produces independent and rigorous analysis of critical global, regional and country-specific challenges and opportunities; and offers new ideas to decision-makers and -shapers on how these could best be tackled from the near- to the long-term. For more information, please visit: www.chathamhouse.org.

CIGI MASTHEAD

Executive

President	Rohinton P. Medhora
Director of the International Law Research Program	Oonagh Fitzgerald
Director of the Global Security & Politics Program	Fen Osler Hampson
Director of Human Resources	Susan Hirst
Director of the Global Economy Program	Domenico Lombardi
Vice President of Finance	Mark Menard
Chief of Staff and General Counsel	Aaron Shull

Publications

Managing Editor, Publications	Carol Bonnett
Publications Editor	Jennifer Goyder
Publications Editor	Vivian Moser
Publications Editor	Patricia Holmes
Publications Editor	Nicole Langlois
Graphic Designer	Melodie Wakefield
Graphic Designer	Sara Moore

Communications

Communications Manager	Tammy Bender	tbender@cigionline.org (1 519 885 2444 x 7356)

CIGI

67 Erb Street West
Waterloo, Ontario N2L 6C2
tel +1 519 885 2444 fax +1 519 885 5450
www.cigionline.org

CHATHAM
HOUSE
The Royal Institute of
International Affairs

10 St James's Square
London, England SW1Y 4LE, United Kingdom
tel +44 (0)20 7957 5700 fax +44 (0)20 7957 5710
www.chathamhouse.org

FSC
www.fsc.org
RECYCLED
Paper made from
recycled material
FSC® C023070

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Friday, October 09, 2015 5:05 PM
To: [redacted] (FD) (FBI)
Subject: foreign travel

b6 -1
b7C -1

Hi [redacted] It's been a while. My work with the Dir's office is going smoothly and is truly rewarding. But I want to make sure I follow all security procedures for foreign travel. In mid December, I will be going on a week-long "Academic Exchange" to Israel -- sponsored by the Rabin Institute, RAND, and the Milken Foundation. There will be a lot briefings on Mideast Politics etc. I don't a program for this year yet but do have one for last year's exchange. Could you please tell me what if anything I need do?
thx & have a lovely weekend
dan richman

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Friday, October 09, 2015 6:20 PM
To: Oconnell, Sasha C. (DO) (FBI)
Subject: RE:

Added thought on this - It would be great to have someone from Google. Even as the company wants to meet & beat Apple's device encryption promise, their interest in accessing data is quite different. A very useful perspective

____

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Friday, October 09, 2015 2:33 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE:

Hmmm. Do you have any thoughts? I think I have offered all of our productive engagement folks but I will look through my stack of cards here...

-----Original Message-----
From: Richman, Daniel C. (DO) (OGA)
Sent: Friday, October 09, 2015 1:10 PM
To: Oconnell, Sasha C. (DO) (FBI)
Subject:

It is true that [redacted] and I are concerned about the size of the group next fri and being quite grudging about adding people. But as I look at the number of govt vs. non-govt coming, my new thought is that if, in the wake of the post-hearing "clarity," a really well placed industry person wanted in, I'd lean toward inviting. But not just anyone :) b6 -1 b7C -1

Oconnell, Sasha C. (DO) (FBI)

From:	Oconnell, Sasha C. (DO) (FBI)
Sent:	Saturday, October 10, 2015 1:44 PM
To:	Richman, Daniel C. (DO) (OGA)
Subject:	Fwd: NY Times

-------- Original message --------
From: "James B. Comey" <jcb.dir@ic.fbi.gov>
Date: 10/10/2015 1:34 PM (GMT-05:00)
To: "Hess, Amy S. (DO) (FBI)" [redacted] "Rybicki, James E. (DO) (FBI)" [redacted] "Oconnell, Sasha C. (DO) (FBI)" [redacted] "Harbach, David V. (DO) (OGA)" [redacted] (DO) (FBI)" [redacted] 'Giuliano, Mark F. (DO) (FBI)" [redacted] "Kortan, Michael P. (DO) (FBI)" [redacted]
Subject: NY Times

b6 -1,2
b7C -1,2
b7E -3

You may recall me wondering how folks were going to paint the PC as the end of the Going Dark effort. Now we know. They didn't bother with [redacted] who wrote an accurate piece. Instead they have produced this beauty in the Times. Mike: did these writers even try to ask us?

> http://www.nytimes.com/2015/10/11/us/politics/obama-wont-seek-access-to-encrypted-user-data.html?hp&action=click&pgtype=Homepage&module=first-column-region&region=top-news&WT.nav=top-news

Oconnell, Sasha C. (DO) (FBI)

From:	Oconnell, Sasha C. (DO) (FBI)
Sent:	Friday, October 09, 2015 7:02 PM
To:	Richman, Daniel C. (DO) (OGA)
Subject:	RE:

So we had a mtg with them. It was several months back but it was not particularly productive. There was one guy from their threat group...he did not give us a card remember but let me see if anyone has a bead on his info.

--

-------- Original message --------
From: "Richman, Daniel C. (DO) (OGA)" [redacted] b7E -3
Date: 10/09/2015 6:23 PM (GMT-05:00)
To: "Oconnell, Sasha C. (DO) (FBI)" [redacted]
Subject: RE:

Added thought on this - It would be great to have someone from Google. Even as the company wants to meet & beat Apple's device encryption promise, their interest in accessing data is quite different. A very useful perspective

____
From: Oconnell, Sasha C. (DO) (FBI)
Sent: Friday, October 09, 2015 2:33 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE:

Hmmm. Do you have any thoughts? I think I have offered all of our productive engagement folks but I will look through my stack of cards here...

-----Original Message-----
From: Richman, Daniel C. (DO) (OGA)
Sent: Friday, October 09, 2015 1:10 PM
To: Oconnell, Sasha C. (DO) (FBI)
Subject:

It is true that [redacted] and I are concerned about the size of the group next fri and being quite grudging about adding people. b6 -2
But as I look at the number of govt vs. non-govt coming, my new thought is that if, in the wake of the post-hearing "clarity," b7C -2
a really well placed industry person wanted in, I'd lean toward inviting. But not just anyone :)

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Saturday, October 10, 2015 2:08 PM
To: Oconnell, Sasha C. (DO) (FBI)
Subject: RE: NY Times

the problem is that this particularly NSC has been fully encrypted. The words "on the table" have to be used. Perhaps with a little picture of a table

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Saturday, October 10, 2015 1:43 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: Fwd: NY Times

--

-------- Original message --------
From: "James B. Comey" <jcb.dir@ic.fbi.gov>
Date: 10/10/2015 1:34 PM (GMT-05:00)
To: "Hess, Amy S. (DO) (FBI)" [redacted] "Rybicki, James E. (DO) (FBI)" [redacted] 'Oconnell, Sasha C. (DO) (FBI)' [redacted] "Harbach, David V. (DO) (OGA)" [redacted] (DO) (FBI)" [redacted] "Giuliano, Mark F. (DO) (FBI)" [redacted] "Kortan, Michael P. (DO) (FBI)" [redacted]
Subject: NY Times

b6 -1,2
b7C -1,2
b7E -3

You may recall me wondering how folks were going to paint the PC as the end of the Going Dark effort. Now we know. They didn't bother with [redacted] who wrote an accurate piece. Instead they have produced this beauty in the Times. Mike: did these writers even try to ask us?

http://www.nytimes.com/2015/10/11/us/politics/obama-wont-seek-access-to-encrypted-user-data.html?hp&action=click&pgtype=Homepage&module=first-column-region®ion=top-news&WT.nav=top-news

Oconnell, Sasha C. (DO) (FBI)

From:	Oconnell, Sasha C. (DO) (FBI)
Sent:	Saturday, October 10, 2015 2:14 PM
To:	Richman, Daniel C. (DO) (OGA)
Subject:	RE: NY Times

Agreed. Or the sword metaphor. Or the question/answer about what we will do if voluntary doesn't work. We will see what Kortan says...

--

-------- Original message --------
From: "Richman, Daniel C. (DO) (OGA)"[redacted] b7E -3
Date: 10/10/2015 2:09 PM (GMT-05:00)
To: "Oconnell, Sasha C. (DO) (FBI)"[redacted]
Subject: RE: NY Times

the problem is that this particularly NSC has been fully encrypted. The words "on the table" have to be used. Perhaps with a little picture of a table

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Saturday, October 10, 2015 1:43 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: Fwd: NY Times

--

-------- Original message --------
From: "James B. Comey" <jcb.dir@ic.fbi.gov>
Date: 10/10/2015 1:34 PM (GMT-05:00)
To: "Hess, Amy S. (DO) (FBI)"[redacted]"Rybicki, James E. (DO) (FBI)"[redacted] "Oconnell, Sasha C. (DO) (FBI)"[redacted]. "Harbach, David V. (DO) (OGA)[redacted] [redacted](DO) (FBI)[redacted]"Giuliano, Mark F. (DO) (FBI)[redacted]"Kortan, Michael P. (DO) (FBI)"[redacted]
Subject: NY Times

b6 -1,2
b7C -1,2
b7E -3

You may recall me wondering how folks were going to paint the PC as the end of the Going Dark effort. Now we know. They didn't bother with [redacted] who wrote an accurate piece. Instead they have produced this beauty in the Times. Mike: did these writers even try to ask us?

http://www.nytimes.com/2015/10/11/us/politics/obama -wont-seek-access -to-encrypted-user-data.html?hp&action=click&pgtype=Homepage&module=first -column-region&region=top-news&WT.nav=top-news

Richman, Daniel C. (DO) (OGA)

From:	Richman, Daniel C. (DO) (OGA)
Sent:	Saturday, October 10, 2015 2:29 PM
To:	Oconnell, Sasha C. (DO) (FBI)
Subject:	RE: NY Times

Perhaps Kortan can arrange a two-fer: Both reaching out to the reporters to correct the story, and flag the EDNY decision Friday (maybe even the SEC decision too) as instances of a new spate of court battles (in the absence of legislation or voluntary compliance) about Apple encryption

____

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Saturday, October 10, 2015 2:14 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: NY Times

Agreed. Or the sword metaphor. Or the question/answer about what we will do if voluntary doesn't work. We will see what Kortan says...

--

-------- Original message --------
From: "Richman, Daniel C. (DO) (OGA)"[redacted] b7E -3
Date: 10/10/2015 2:09 PM (GMT-05:00)
To: "Oconnell, Sasha C. (DO) (FBI)"[redacted]
Subject: RE: NY Times

the problem is that this particularly NSC has been fully encrypted. The words "on the table" have to be used. Perhaps with a little picture of a table ________________________________
From: Oconnell, Sasha C. (DO) (FBI)
Sent: Saturday, October 10, 2015 1:43 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: Fwd: NY Times

--

-------- Original message --------
From: "James B. Comey" <jcb.dir@ic.fbi.gov>
Date: 10/10/2015 1:34 PM (GMT-05:00)
To: "Hess, Amy S. (DO) (FBI)"[redacted]"Rybicki, James E. (DO) (FBI)" b6 -1
[redacted]"Oconnell, Sasha C. (DO) (FBI)"[redacted]"Harbach, b7C -1
David V. (DO) (OGA)"[redacted](DO) (FBI)" b7E -3
[redacted]"Giuliano, Mark F. (DO) (FBI)"[redacted]"Kortan,

Michael P. (DO) (FBI)"[redacted]
Subject: NY Times

b6 -2
b7C -2
b7E -3

You may recall me wondering how folks were going to paint the PC as the end of the Going Dark effort. Now we know. They didn't bother with [redacted] who wrote an accurate piece. Instead they have produced this beauty in the Times. Mike: did these writers even try to ask us?

http://www.nytimes.com/2015/10/11/us/politics/obama-wont-seek-access-to-encrypted-user-data.html?hp&action=click&pgtype=Homepage&module=first-column-region®ion=top-news&WT.nav=top-news

Oconnell, Sasha C. (DO) (FBI)

From:	Oconnell, Sasha C. (DO) (FBI)
Sent:	Saturday, October 10, 2015 2:38 PM
To:	Richman, Daniel C. (DO) (OGA)
Subject:	RE: NY Times

And symphony. Let me see what he is thinking....

--

-------- Original message --------
From: "Richman, Daniel C. (DO) (OGA)"[redacted] b7E -3
Date: 10/10/2015 2:32 PM (GMT-05:00)
To: "Oconnell, Sasha C. (DO) (FBI)"[redacted]
Subject: RE: NY Times

Perhaps Kortan can arrange a two-fer: Both reaching out to the reporters to correct the story, and flag the EDNY decision Friday (maybe even the SEC decision too) as instances of a new spate of court battles (in the absence of legislation or voluntary compliance) about Apple encryption

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Saturday, October 10, 2015 2:14 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: NY Times

Agreed. Or the sword metaphor. Or the question/answer about what we will do if voluntary doesn't work. We will see what Kortan says...

--

-------- Original message --------
From: "Richman, Daniel C. (DO) (OGA)"[redacted] b7E -3
Date: 10/10/2015 2:09 PM (GMT-05:00)
To: "Oconnell, Sasha C. (DO) (FBI)"[redacted]
Subject: RE: NY Times

the problem is that this particularly NSC has been fully encrypted. The words "on the table" have to be used. Perhaps with a little picture of a table

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Saturday, October 10, 2015 1:43 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: Fwd: NY Times

--

-------- Original message --------

From: "James B. Comey" <jcb.dir@ic.fbi.gov>
Date: 10/10/2015 1:34 PM (GMT-05:00)
To: "Hess, Amy S. (DO) (FBI)" [redacted], "Rybicki, James E. (DO) (FBI)" [redacted] "Oconnell, Sasha C. (DO) (FBI)" [redacted], "Harbach, David V. (DO) (OGA)" [redacted] [redacted] (DO) (FBI)" [redacted] "Giuliano, Mark F. (DO) (FBI)" [redacted] "Kortan, Michael P. (DO) (FBI)" [redacted]
Subject: NY Times

b6 -1,2
b7C -1,2
b7E -3

You may recall me wondering how folks were going to paint the PC as the end of the Going Dark effort. Now we know. They didn't bother with [redacted] who wrote an accurate piece. Instead they have produced this beauty in the Times. Mike: did these writers even try to ask us?

http://www.nytimes.com/2015/10/11/us/politics/obama -wont-seek-access -to-encrypted-user-data.html?hp&action=click&pgtype=Homepage&module=first -column-region&region=top -news&WT.nav=top-news

Oconnell, Sasha C. (DO) (FBI)

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Saturday, October 10, 2015 4:31 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: Fwd: [redacted] b7E -3
[redacted]

-------- Original message --------
From: "Kortan, Michael P. (DO) (FBI)" [redacted] b6 -1,2
Date: 10/10/2015 4:28 PM (GMT-05:00) b7C -1,2
To: "Comey, James B. (DO) (FBI)" <James.Comey@ic.fbi.gov>, "Hess, Amy S. (DO) (FBI)" b7E -3
[redacted] "Rybicki, James E. (DO) (FBI)" [redacted]
(DO) (FBI)" [redacted] "Giuliano, Mark F. (DO) (FBI)"
[redacted] "Harbach, David V. (DO) (OGA)" [redacted] "Oconnell,
Sasha C. (DO) (FBI)" [redacted] "Baker, James A. (OGC) (FBI)"
[redacted]
Subject: [redacted]

All: [redacted] is writing about the below order from Mag. Judge Orenstein and report that he has made this public (noting that he did not make any of the case particulars public) to extend his role in privacy-secuirity issues and reveal the government's strategy in this case...although she believes and may report that EDNY did not coordinate with Main Justice
M.

From: [redacted] b6 -2
Sent: Saturday, October 10, 2015 9:30 AM b7C -2
To: Kortan, Michael P. (DO) (FBI)
Subject: Going Dark - Apple order

https://ia801501.us.archive.org/27/items/gov.uscourts.nyed.376325/gov.uscourts.nyed.376325.2.0.pdf

MIke, I'm writing about this today. Interesting how the application was filed the same day Comey testified that the discussions w/ companies were "productive." Call if you need to talk- [redacted]

From: James B. Comey
Sent: Saturday, October 10, 2015 3:00 PM
To: Kortan, Michael P. (DO) (FBI)
Cc: Hess, Amy S. (DO) (FBI); Rybicki, James E. (DO) (FBI); Oconnell, Sasha C. (DO) (FBI); Harbach, David V. (DO) (OGA);
[redacted] (DO) (FBI); Giuliano, Mark F. (DO) (FBI) b6 -1
Subject: Re: NY Times b7C -1

I'm hoping the WH will now release the SOC from the PC. Don't recall that it is classified. Or perhaps the Times will ask its "sources" to read it to them (and then watch the hemming and hawing).

On Oct 10, 2015, at 2:21 PM, Kortan, Michael P. (DO) (FBI)
[redacted] wrote: b7E -3

No, nor did any of our NYT regulars reach out

--

-------- Original message --------
From: "James B. Comey" <jcb.dir@ic.fbi.gov<mailto:jcb.dir@ic.fbi.gov>>
Date: 10/10/2015 1:34 PM (GMT-05:00)
To: "Hess, Amy S. (DO) (FBI)"[redacted]"Rybicki, James E. (DO) (FBI)" b6 -1,2
[redacted] "Oconnell, Sasha C. (DO) (FBI)" b7C -1,2
[redacted] "Harbach, David V. (DO) (OGA)" b7E -3
[redacted](DO) (FBI)"
[redacted]"Giuliano, Mark F. (DO) (FBI)"
[redacted] "Kortan, Michael P. (DO) (FBI)"
[redacted]
Subject: NY Times

You may recall me wondering how folks were going to paint the PC as the end of the Going Dark effort. Now we know. They didn't bother with [redacted] who wrote an accurate piece. Instead they have produced this beauty in the Times. Mike: did these writers even try to ask us?

http://www.nytimes.com/2015/10/11/us/politics/obama -wont-seek-access -to-encrypted-user-data.html?hp&action=click&pgtype=Homepage&module=first -column-region&region=top-news&WT.nav=top-news

Oconnell, Sasha C. (DO) (FBI)

From:	Oconnell, Sasha C. (DO) (FBI)
Sent:	Sunday, October 11, 2015 6:40 AM
To:	Richman, Daniel C. (DO) (OGA)
Subject:	Fwd: With court order, federal judge seeks to fuel debate about data encryption from The Washington Post

-------- Original message --------
From: Sasha O'Connell [redacted]
Date: 10/11/2015 6:29 AM (GMT-05:00)
To: "Oconnell, Sasha C. (DO) (FBI)" [redacted]
Subject: With court order, federal judge seeks to fuel debate about data encryption from The Washington Post

b6 -1
b7C -1
b7E -3

http://wpo.st/F9Cg0

Sent from my iPhone

Richman, Daniel C. (DO) (OGA)

From:	Richman, Daniel C. (DO) (OGA)
Sent:	Sunday, October 11, 2015 9:45 AM
To:	Oconnell, Sasha C. (DO) (FBI)
Subject:	RE: With court order, federal judge seeks to fuel debate about data encryption from The Washington Post

Thx. Suspect it would be useful if [redacted] reached out to the edny folks to coordinate b6 -5 b7C -5

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Sunday, October 11, 2015 6:39 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: Fwd: With court order, federal judge seeks to fuel debate about data encryption from The Washington Post

--

-------- Original message --------
From: Sasha O'Connell [redacted] b6 -1
Date: 10/11/2015 6:29 AM (GMT-05:00) b7C -1
To: "Oconnell, Sasha C. (DO) (FBI)" [redacted] b7E -3
Subject: With court order, federal judge seeks to fuel debate about data encryption from The Washington Post

http://wpo.st/F9Cg0

Sent from my iPhone

Oconnell, Sasha C. (DO) (FBI)

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Sunday, October 11, 2015 9:59 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: With court order, federal judge seeks to fuel debate about data encryption from The Washington Post

Yes they have stand by got a short summary.

--

-------- Original message --------
From: "Richman, Daniel C. (DO) (OGA)" [redacted] b6 -5
Date: 10/11/2015 9:47 AM (GMT-05:00) b7C -5
To: "Oconnell, Sasha C. (DO) (FBI)" [redacted] b7E -3
Subject: RE: With court order, federal judge seeks to fuel debate about data encryption from The Washington Post

Thx. Suspect it would be useful if [redacted] reached out to the edny folks to coordinate

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Sunday, October 11, 2015 6:39 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: Fwd: With court order, federal judge seeks to fuel debate about data encryption from The Washington Post

--

-------- Original message --------
From: Sasha O'Connell [redacted] b6 -1
Date: 10/11/2015 6:29 AM (GMT-05:00) b7C -1
To: "Oconnell, Sasha C. (DO) (FBI)" [redacted] b7E -3
Subject: With court order, federal judge seeks to fuel debate about data encryption from The Washington Post

http://wpo.st/F9Cg0

Sent from my iPhone

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, October 12, 2015 1:36 PM
To: Baker, James A. (OGC) (FBI); [redacted] (ODAG) (JMD); Oconnell, Sasha C. (DO) (FBI)
Subject: GD roundtable at Columbia

b6 -5
b7C -5

Dear Sasha, Jim & [redacted] -- Given the NYT's mucking up of the Admin GD position, it would be extremely helpful if Jim B, in his opening remarks, could definitely clarify the "legislation has to be on the table" position. That would help spur attendees' "voluntary" muscles into action. Would that be possible?

Oconnell, Sasha C. (DO) (FBI)

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Monday, October 12, 2015 1:46 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: GD roundtable at Columbia

I will make sure of it :)

--

-------- Original message --------
From: "Richman, Daniel C. (DO) (OGA)'[redacted]
Date: 10/12/2015 1:39 PM (GMT-05:00)
To: "Baker, James A. (OGC) (FBI)"[redacted](ODAG) (JMD)"
[redacted]"Oconnell, Sasha C. (DO) (FBI)"[redacted]
Subject: GD roundtable at Columbia

b6 -5
b7C -5
b7E -3

Dear Sasha, Jim &[redacted]- Given the NYT's mucking up of the Admin GD position, it would be extremely helpful if Jim B, in his opening remarks, could definitely clarify the "legislation has to be on the table" position. That would help spur attendees' "voluntary" muscles into action. Would that be possible?