HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 065 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Thursday, June 15, 2017

Chair

Mr. Blaine Calkins

Standing Committee on Access to Information, Privacy and Ethics

Thursday, June 15, 2017

● (1535)

[*English*]

The Chair (Mr. Blaine Calkins (Red Deer—Lacombe, CPC)): Good afternoon, colleagues. I apologize for the brief delay. We are all just arriving at the committee room, which is in one of the buildings farthest away from the House of Commons, where we just concluded a vote only to find out that we will be summoned back to the House of Commons for another vote in short order.

I'm proposing that we hear as much testimony as we can from our witnesses.

We thank you for being here today. We will probably have to excuse ourselves for a few minutes to go back to vote. Given the amount of time that that will likely take, we'll make a determination at that point whether or not I'll ask you guys to patiently wait for our return. Thank you for your patience so far.

We have with us as witnesses, first, from the Canadian Civil Liberties Association, Brenda McPhail, who is no stranger to the committee.

It's great to see you, Brenda.

We also have, from the British Columbia Civil Liberties Association, Micheal Vonn, who is also no stranger to the committee, together with Meghan McDermott. From the American Civil Liberties Union, we have Esha Bhandari, the staff attorney. You are all coming to us by video conference, except Brenda, whom we're glad to have in our presence here now.

This is the 65th meeting of the Standing Committee on Access to Information, Privacy and Ethics, where we're studying the privacy of Canadians at airports, borders and when travelling in the United States.

It will be a very brief study, so without further ado, I will ask Ms. McPhail to lead us off for up to 10 minutes.

Ms. Brenda McPhail (Director, Privacy, Technology and Surveillance Project, Canadian Civil Liberties Association): Thank you very much to the committee for inviting the Canadian Civil Liberties Association to speak on this important topic.

The CCLA, as you know, is an independent national and non-governmental organization that has fought for civil liberties in Canada since 1964.

I'm going to focus on three topics today, the first at some length and the others very briefly. First is the need to update laws and policies regarding device searches at the border in a way that reflects the heightened privacy expectations that adhere to these devices. Second is the great need for public transparency and accountability regarding the way current laws are being interpreted at the border, and the policies and procedures in place regarding particularly privacy-invasive searches, and, very briefly, the need to ensure that the new preclearance act, Bill C-23, maintains or enhances privacy protections for Canadians and travellers on Canadian soil and does not diminish them.

I'm not going to speak at any length to President Trump's executive order excluding non-U.S. citizens from privacy protections under the U.S. Privacy Act, but I do want to just note that CCLA agrees with the concerns reflected in the Privacy Commissioner's letter of March 8, and we share his call to our government to ask the United States for improved privacy protection for Canadians under that act.

This study is both timely and extremely badly needed in light of the stories we've all heard about individuals facing intrusive and humiliating questions about religious faith, ethnic origins, sexuality, and political beliefs at both sides of the border, Canadian and American, and conversely the rhetoric we're hearing about extreme vetting that plays on pervasive fear of terror and “the other”.

I'm going to speak about law in principle for the most part, but I want to stress at the outset that the reason we need to think long and hard about how to improve privacy at the border has to do with the cost to individuals and to public trust from failing to do so.

The CCLA runs a public inquiry line, and on that line border questions have increased dramatically in the last six months. We've had calls from Muslims and Christians, and men and women of different skin colours and different sexual orientations, and they're all afraid of the same thing. They're afraid they are going to be subjected to privacy-invasive searches or questions when they cross the border. Some of them are afraid to travel at all.

We can't do much about how Canadians are treated at the United States border, but we can and we must address the problems that exist at our own. I would go further and suggest that the time is right for Canada to take a global leadership position regarding rights respecting border security laws, policies, and practices.

It is widely believed that borders are special zones in which privacy rights are reduced because of the compelling duty to protect state sovereignty and the populace. We don't disagree with that duty or with the need for effective border security that follows from it, but it is important to note that "reduced" expectations of privacy cannot and should not ever mean "non-existent", and we argue that to be genuinely effective in the best sense, security must be both rigorous and rights-respecting in equal measure.

This is particularly true in relation to searches of electronic devices, including cellphones, laptops and wearables. We're living in a world where the tools that we increasingly use to navigate our daily lives, sometimes by design and often by default, contain, create, and connect information about us that is profoundly personal and sensitive. We have to quit trying to fit these technologies into a legal and regulatory structure created at a time when both these devices and the quantity and quality of information they can contain was inconceivable.

I know this committee has heard very similar variations on this theme in relation to its studies of the Privacy Act and PIPEDA, and it is similarly and urgently relevant here for this study.

I would argue that it is entirely possible for us to do better. When it comes to law enforcement outside the border context, we are actually in a small way starting to figure out how to address dealing with these devices, the information they store, and the potential for even seemingly insubstantial bits of information to have privacy implications. It's a work that's still very much in progress, but there has arguably been some advancement. In particular, we've recognized that the privacy-invasiveness of an electronic device search requires a clear framework under domestic law to ensure that the search itself is reasonable, that it's conducted in a reasonable manner, and that it's otherwise charter-compliant, usually by requiring prior judicial authorization—a warrant—and adequate grounds on which to base the search.

There is no compelling reason why we can't develop clear laws that allow us to do the same at the border, even taking into account its unique context. The current practice of CBSA is not sufficient. CBSA agents conduct warrantless searches of electronic devices with no defined threshold for grounds, based on largely unexplained interpretations of legislation that originally meant to apply to carriages and cars and boxes and bags. Nor has the manner of such searches yet faced a meaningful public or judicial scrutiny.

Information that is collected from devices searched or detained by CBSA is taken without public knowledge about what it will be used for; whether, how, or for how long it will be retained; and whether, how, or with whom it could be shared. Many individuals, from members of the business community to journalists, researchers, doctors, and lawyers, also have professional obligations to maintain the confidentiality and integrity of their data. The present law is entirely unequipped to deal with that reality.

There are also current constitutional challenges coming forward in the lower courts relating to device searches. While the trend up until now seems to have been to settle and make them go away, at some point these questions will have to be dealt with in the court. They should be dealt with, I would argue, by our lawmakers. It's long past time we updated the Customs Act and other legislation that applies in the border context to recognize the distinction between a bagful of underwear and a device that contains or provides access to our most intimate, personal conversations, our political musings and affiliations, our religious faith, our financial records, our commercial secrets, our health information, and many more types of information.

We also have to note in this context that certain groups—for instance, Muslim individuals, or individuals perceived to be Muslim, which are not always the same thing—have demonstrably been subject to greater scrutiny at the border, perhaps even more so since the U.S. executive order popularly known as the "Muslim travel ban". Any measure that gives border officials powers to conduct invasive searches or that allows for continued ambiguity, uncertainty, and unchecked discretion in these matters runs the risk of disproportionately affecting these groups.

It's also impossible to talk about device searches without at least touching on related topics of compelled password disclosure and forced access to social media credentials. These practices truly highlight the illogic of treating electronic devices as equivalent to any other good that crosses the border. While it should remain within the purview of CBSA, of course, to detain devices, get a warrant, and conduct a forensic search on reasonable grounds, individuals shouldn't have an obligation to participate in that process.

We know from a 2015 interim document that was released via an access request that the CBSA believes it has the power to impose penalties on travellers who decline to provide a password for a given device. CCLA would argue that, at least in some cases, compelling that disclosure of a password that exists only in an individual's mind could interfere with the individual's charter rights to silence and against self-incrimination. This is in addition to the other privacy rights clearly at play.

Currently Canada doesn't ask for social media passwords or credentials that would allow them to access data stored remotely, and there's no legislative authority that would justify such a request. We simply want to warn against ever moving in that direction, because it would be both ineffective and likely to raise serious constitutional issues.

Social media is a place where people can and do play with identity, which would render the information profoundly unreliable. Of course we know—social science tells us—that people who think they're being watched change the way they behave and the materials they feel free to look at and explore and learn from and study. This means that such scrutiny could also have a profoundly chilling effect on other fundamental freedoms that we value, including freedom of association and freedom of expression.

The second topic I'd like to mention very briefly is the need for greater public transparency and accountability in the way in which our current laws, including the Customs Act and the Immigration and Refugee Protection Act, are being interpreted at the border, especially as they pertain to privacy-invasive searches and questions. I mentioned that we have access to a small number of policy documents. They actually reside on the website of our friend the BCCLA. However, a couple of documents received from an access request in 2015 hardly fulfills the requirement for public accountability or transparency. We don't even know if they're complete, accurate, or up to date. In contrast, if we look at our neighbours to the south, they actually have proactively published their policy documents about this kind of search, a privacy impact study that they conducted, and statistics regarding the electronic searches they conduct. There's no reason we can't do the same.

For an ordinary person at a Canadian border, it's difficult, even impossible, to evaluate whether the way a search has taken place meets constitutional standards. In other words, those scared people I was talking about at the beginning have no way to figure out if the way they're being treated at the border is lawful and fair if they have no access to the policies and procedures that are supposed to have been followed. Of course, with no independent oversight of CBSA, although there is hope that this will change, it's extremely hard to seek recourse.

● (1540)

In my last six seconds, I'll ask you to please take a look at Bill C-23 for its privacy implications, particularly in regard to the ability of American officers to perform strip searches if a Canadian officer declines to do so. It opens up a very dangerous territory. Borders require special consideration not just because they're zones where we need security, but also because they're the first place where people coming into Canada interact with what we hope is a free and democratic country. We need to show them who we are by making sure that our policies and laws at the border reflect our values.

The Chair: Thank you very much, Brenda.

We will now move to the British Columbia Civil Liberties Association.

Micheal, I would imagine that you're leading us off.

● (1545)

Ms. Micheal Vonn (Policy Director, British Columbia Civil Liberties Association): I am.

Thank you to the committee for the invitation to participate in this very timely study.

Obviously, Canadians are increasingly concerned about their privacy in the context of the border and cross-border data flows. Our association assists individuals to understand their privacy rights. Just this morning, in fact, the Canadian Internet Registration Authority announced that they are jointly funding our project with CIPPIC to produce a privacy and security guide for electronic devices at the border. We're doing this because Canadians need reliable and practical advice in this realm, but they also need appropriate protection in law and policy.

There are obviously a vast number of topics that could be discussed in this context, and only a few can be addressed in a given presentation. I am going to be discussing the U.S. Privacy Act and information-sharing agreements, while my colleague is going to be discussing appropriate thresholds for searches, the new preclearance bill, and solicitor-client privilege.

We, like our colleagues at the CCLA, recommend following the OPC's concerns relating to Canada's being added to the list of designated countries whose citizens are covered by the U.S. Privacy Act. As they set out in their March 8 letter to the Ministers of Justice, Public Safety, and Defence, this would increase the level of data protection for Canadians to that granted to individuals from various European countries.

Now, it's important to note—and perhaps our colleague at the ACLU will be picking up on this—that the U.S. Privacy Act offers only limited privacy protections, given a great number of significant exemptions, including those for law enforcement and national security. Nevertheless, Canadians who have come to understand that they are denied even these limited protections, in contrast to individuals from other countries, are right to call for this to be remedied.

The recently released report of Canada's first-ever consultation on the national security framework clearly provides important context to this committee in its study. It is evident that Canadians care very deeply about privacy and are adamant that the powers of investigation and data collection for law enforcement and national security must be demonstrably necessary, proportionate, and accountable. A deeply problematic secrecy has created a growing mistrust with respect to cross-border data flows and a concern about the genuine harms to Canadians that have resulted.

Recall, if you will, a flurry of news stories that broke out just a few short years ago about individuals in Canada denied entry to the U.S. on the basis of mental health information accessed by U.S. border officials. The Office of the Information and Privacy Commissioner of Ontario had to do an investigation to even find out how U.S. border officials were coming by this sensitive Canadian health information. The privacy commissioner's report outlines how this information was being logged in the CPIC, the Canadian Police Information Centre's database, and accessed by the FBI via a memorandum of co-operation with the RCMP. That agreement allowed the FBI to further decide who else to give that information to, and they decided that the entities of the Department of Homeland Security, including border officials, should have access as well.

Those are just some of the tentacles of personal information flow facilitated by a single memorandum. We should note quickly, as I said, given the exemptions in the U.S. Privacy Act, that we would not see any remedy for those data flows if we were covered by that act.

The important question is, how much and what kinds of personal information are Canadian agencies providing to U.S. agencies through such information-sharing agreements? To our knowledge, no one knows the answer to that question.

We understand that the OPC had some years ago attempted an audit of such agreements and was unable to get the completed information. The OPC has again requested the co-operation of agencies within the government to collect the information on what information-sharing agreements exist in order to have a comprehensive picture of what important information flows are actually amounting to. We trust that this committee will appreciate the imperative of an audit of current information-sharing protocols and agreements and call upon the government to ensure full co-operation with the OPC in this urgently needed work.

● (1550)

Meghan.

Ms. Meghan McDermott (Policy Officer, British Columbia Civil Liberties Association): I'll begin by discussing preclearance and the thresholds for searches.

Currently, electronic devices are considered goods in the context of the Canadian border and in preclearance areas at Canadian airports, and there are no statutory safeguards to protect them from arbitrary search by border agents. Preclearance areas are those designated zones in some Canadian airports where U.S. agents have been empowered to process U.S.-bound travellers.

Bill C-23, an act respecting the preclearance of persons and goods in Canada and the United States, was introduced last June and is intended to repeal and replace the existing act from 1999. Bill C-23 contemplates that preclearance areas will be expanded beyond airports and could be established at rail, marine, and land border crossings. It expands the powers that U.S. agents have and, in our view, unjustifiably limits the rights of travellers in the preclearance areas. We've expressed our concerns with this bill in testimony to the committee on public safety and national security, and we'll make our written submission available to this committee as well. Under both the existing and the contemplated preclearance law, a traveller cannot be arbitrarily strip-searched. An agent must have reasonable grounds to suspect in order to have the legal authority to detain the traveller for a strip search.

The OPC has recommended that an identical threshold for the searching of digital devices be written into Bill C-23. In a letter to the committee on public safety, the OPC asks that “Bill C-23 be amended to place border searches of electronic devices on the same footing as searches of persons and therefore their performance should require reasonable grounds to suspect.” The BCCLA endorses this position, as well as the OPC's further recommendation to make a consequential amendment to the Customs Act to similarly protect the privacy of Canadians who are returning home through Canadian borders. We agree with the OPC that “the idea that electronic devices should be considered as mere goods and therefore subject to border searches without legal grounds is clearly outdated and does not reflect the realities of modern technology.” Interestingly, the interim policy documents of the CBSA do appear to acknowledge that it is not appropriate to classify digital devices as “mere goods”. A CBSA operational bulletin from 2015 does not provide for suspicionless searches, but rather states that searches may be conducted if there are “a multiplicity of indicators” that ”evidence of contraventions” may be found on the digital device. We support the OPC's call to codify this policy through legislative amendments. The law should require a border agent, whether CBSA or American, in a preclearance area to have reasonable grounds to suspect that a contravention of law has occurred before they may lawfully search an electronic device. Such legislation would provide legal clarity and transparency to Canadians while also giving existing policy the force of law. It would also support the recognition by the Supreme Court of Canada that the search of electronic devices is an extremely privacy-intrusive procedure.

Finally, I have just two short points. The first is about solicitor-client privilege. This is a matter that the Canadian Bar Association flagged for the committee on public safety, and it applies to ordinary border crossings as well as preclearance areas. Neither we nor the CBA can tell whether Canada has a defined policy about claims of privilege over documents or electronic records on our digital devices. As this privilege is fundamental to our legal system, we want the government to shape a policy that recognizes solicitor-client privilege and entitles travellers to make this claim of privilege over physical or electronic information when they are crossing the border.

Secondly, we'd like to draw your attention to our recommendation to curtail the powers of U.S. officers to strip-search travellers in Canada under Bill C-23. Last month at the committee on public safety, we strenuously objected to conferring any power on U.S. preclearance officers to perform strip searches in preclearance zones in Canada. Under current law, a U.S. agent has no legal authority to strip-search anybody in Canada. If he or she has reasonable grounds to suspect that a strip search is necessary, a Canadian agent must agree that such grounds exist, and only then can they perform that search. We maintain that only Canadian officers should have the power to perform strip searches in Canada, and only in limited circumstances, according to law.

● (1555)

That concludes our prepared remarks. We look forward to your questions.

The Chair: Thank you very much.

Colleagues, I have CPAC streaming live here on my phone. The Speaker is calling the question right now, which means that the bells will start ringing within a few seconds. I would ask for unanimous consent to hear the next 10 minutes of testimony. That way, all of our witnesses will have an opportunity to give their testimony before we depart for a vote.

Do I have unanimous consent to do that?

Some hon. members: Agreed.

The Chair: Thank you very much.

Ms. Bhandari, you have up to 10 minutes.

Ms. Esha Bhandari (Staff Attorney, Speech, Privacy, and Technology Project, American Civil Liberties Union): Thank you very much.

I'm Esha Bhandari, and I'm a staff attorney with the American Civil Liberties Union. We appreciate the opportunity to provide testimony before the committee today.

I will address two topics. The first is privacy at the border, and specifically searches of electronic devices. The second is the President's executive order stripping Privacy Act protections from non-U.S. persons.

Regarding searches of electronic devices at the border, the current position of the U.S. government is that a regime of suspicionless searches is permissible per U.S. Customs and Border Protection Policy. This policy, dating from 2009, allows the government to search any and all travellers, regardless of citizenship status, and search specifically their electronic devices without a warrant, probable cause, or any suspicion whatsoever. This claimed authority has not yet been ruled on by the Supreme Court of the United States. There are a handful of lower court cases addressing this, but it remains in an area of legal uncertainty, and specifically with respect to whether U.S. constitutional limitations provided by the fourth amendment would apply here. The ACLU's position is that border agents should not be able to search electronic devices without probable cause at a minimum, but that a warrant is in fact constitutionally required.

The nature of searches happening at the border can vary. There may be manual or cursory searches, which happen on site when a traveller arrives at the border. Those searches could include searches of information contained on the device. They could also include searches of cloud-based data that is accessible through the device, including through social media and email applications. Our concern is that when border patrol agents ask individuals for the passwords for their devices, they have access to an unlimited trove of information through these Internet-connected cloud-based apps. While U.S. citizens or lawful permanent residents may be able to refuse to provide passwords to their devices or their cloud-based applications, visitors risk being turned away if they refuse to do so.

The other type of search that is happening is a forensic search. When this happens, U.S. Customs and Border Protection will seize the device, whether it's a cellphone or a laptop, and most often transport it to another location to be hooked up to a device that allows a full forensic search of the device. This is essentially a computer strip search. It gives the government access not only to everything that is in fact stored on the device but also to metadata and deleted files that the traveller may not have even been aware were still accessible through the device.

When a device is seized in this way, CBP is supposed to retain it for only five days initially, but per its policy, this can be extended in seven-day increments. We have heard stories of individuals having their devices seized for up to weeks at a time. According to the government's policy, any information that can be retained must be that information relating to “immigration, customs, and other enforcement matters if such retention is consistent with the privacy and data protection standards of the system of records in which such information is retained.” However, we're very concerned about information such as that belonging to journalists and their sources and attorney-client privilege information, which the policy does not adequately protect. Individuals may assert that this type of information is contained on their devices before they are searched, but apart from a requirement to consult with a supervisor, there is no limit on the U.S. government searching even this privileged information.

While we have heard of an anecdotal rise in the number of searches, we are also aware of a statistically documented rise. In fiscal year 2015, the U.S. government reports that it searched 8,503 electronic devices at the border. In fiscal year 2016, that number went up to 19,033. While these numbers represent a small percentage of overall travellers to the United States, the steep rise in numbers between 2015 and 2016 is concerning, as is the lack of any constitutional protections of “suspicion” being imposed on these searches.

● (1600)

There is still a greater need for transparency. We do not know how many of these searches are conducted with respect to U.S. citizens or with respect to non-citizens and, if the latter, which countries' individuals are being searched and for what reason.

I will now speak about the executive order from the President's stripping of Privacy Act protections from non-U.S. persons. President Trump's executive order stripping Privacy Act protections essentially means that every non-U.S. person, meaning anyone who is not a U.S. citizen or a lawful permanent resident, is no longer entitled to the Privacy Act protections. These protections include the ability for individuals to access their records, correct their records, and limit the dissemination and collection of information by agencies, subject to exceptions that were previously mentioned, including law enforcement use.

As a matter of long-standing practice, many U.S. agencies had extended Privacy Act protections to include the personally identifiable information of non-U.S. persons, including the many visitors and students and business people who travel to the United States from Canada. Those agencies included the State Department, the Department of Homeland Security, the Department of Justice, and the Department of Health and Human Services. In particular, in 2007, when the Department of Homeland Security adopted the policy of extending Privacy Act protections to all individuals, it noted that doing so would have the benefit of supporting data integrity, advancing cross-border information sharing, facilitating trade and travel, and encouraging protection of U.S. persons' privacy overseas.

When the executive order was signed, the ACLU sent a letter to all federal agencies, arguing that implementation of the memo as written would be contrary to law, including procedural and substantive legal roadblocks. We also wrote to the European Parliament and the European Commission, letting them know that U.S. assurances underpinning the privacy shield agreement and the U.S.–EU umbrella agreement to permit data sharing between the two regions would now be called into question by this executive order.

Nonetheless, at least the Department of Homeland Security has released guidance thus far, in April, indicating that it intends to go ahead with the terms of the executive order. This guidance from the Department of Homeland Security has made it clear that non-U.S. persons, including immigrants and non-immigrants, can only request their records through the Freedom of Information Act rather than through the Privacy Act, and that there will now be a balancing test that weighs the public interest in the information when deciding whether to disclose those individuals' personal information. That includes potential disclosure to third parties requesting information about immigrants and visitors to the United States.

Visitors to the United States and immigrants to the United States who are not U.S. persons may not amend their records through the Privacy Act anymore. Instead, the Department of Homeland Security has said that it will now apply the fair information practice principles to non-U.S. persons' information. It is unclear what this will mean, practically speaking. A large concern remains that non-U.S. persons' private information, sensitive information about immigration status, and health information may now be subject to public disclosure because the Privacy Act protections no longer exist.

I will end my testimony there. I welcome any questions.

Thank you.

The Chair: Thank you very much, Ms. Bhandari.

Colleagues, given that the vote clock shows that we have just over 20 minutes, I recommend that we suspend the meeting and go to do our duty in the House and vote.

I tried to seek consent that we could pair, but I don't think that will work. It never has before, but I thought I would try anyway.

If the witnesses don't mind being patient then, we'll suspend the meeting while members go to vote.

Members, if you could get back here immediately, or as soon as possible, we should have close to 40 minutes left to ask questions. We'll begin with the seven-minute rounds, and we'll be able to get at least that much in out of respect for our witnesses' time.

Again, I apologize to our witnesses that we are unable to have a full committee meeting, but this is what happens at this time of the year. I would just ask you to be patient while we go to vote. We'll see you in about 40 minutes.

● (1600)

(Pause)

● (1645)

The Chair: Thank you very much for your patience, colleagues and witnesses, as we continue to fulfill our democratic responsibilities here.

I will now proceed to the seven-minute round of questions, and we are going to start with Mr. Long.

The floor is yours, sir, for seven minutes. Let's try to keep our questions and answers as concise as possible, because we have only 40 minutes of committee time left.

Mr. Wayne Long (Saint John—Rothesay, Lib.): Thank you for that advice, Chair.

Thank you to our witnesses. It was very interesting testimony and a kind of a refreshing change for the committee.

About two years ago I went across the border. My riding is Saint John—Rothesay in southern New Brunswick, and we're close to the Maine border, obviously, which is about one hour away. We went through, and the U.S. Customs obviously pulled us over. They told us to go into the building and asked us to leave our cellphones in the car.

We went into the building, and were questioned for probably 10 or 15 minutes. My son was in motocross, so we were frequently at the border. We waited upwards of probably 20 to 25 minutes. They told us that we could leave and we went back to our car. There were no phones in the car.

We went back in and they gave us the phones back, but there was maybe a 30- to 40-minute period when we didn't have the phones. They came out with the phones and they asked my son to unlock his phone. He did, and again they disappeared. To make a long story short, we got the phones back, but it was certainly concerning and unsettling for all of us.

How concerned are each of you about cloning and mirroring devices, because I hear that agencies are increasingly cloning and mirroring devices. Obviously, they could follow and track what happened long after we left that border. Is that something you think is becoming more relevant as we move forward in this age of heightened security?

Ms. Bhandari.

Ms. Esha Bhandari: Thank you very much for your question, Mr. Long.

I'm actually a native of Saint John and a proud graduate of Saint John High School. It's nice to speak with you.

We are trying to track the technology that U.S. Customs and Border Protection is acquiring. One of the main areas we've been focusing on has been the use of devices such as Cellebrite that allow the forensic searches.

There has been work done through freedom of information requests and various investigative journalism efforts to track the expenditure of money on particular technology. But while it's a concern, I think we don't yet know enough about what those capabilities are at the border specifically—and in your case in particular, which was presumably at a land border for a short period of time when your phones were out of sight, as opposed to their being seized and taken to a facility where there would be greater access to technology.

We're very concerned about any technology that's being acquired in this realm and being deployed at the border, but I don't think we have enough information right now.

● (1650)

Mr. Wayne Long: Okay.

Is there anything from B.C.?

Ms. Micheal Vonn: The only thing I would note is that we have often said that we need greater transparency about all of the devices available to conduct surveillance, and that all of them, if and however they are being used at the Canadian border, should see privacy impact assessments that go to the OPC. We know that this is simply not occurring in Canada in relation to mass surveillance devices.

But yes, we share the ACLU's efforts to track these.

Mr. Wayne Long: Ms. McPhail, is there anything you want to add to that?

Ms. Brenda McPhail: I would reiterate that we also share the concern.

Part of the call for transparency and accountability at the border should be a call for us to understand—and I said it in my presentation—what is happening when our devices are being seized with the information on them.

I would just note that we are concerned not only about what kinds of technologies are being used and whether or not it's possible to take information from the phones but also very much about how that information gets shared with others.

Mr. Wayne Long: Okay.

Seeing that Ms. Bhandari is from Saint John, I'm going to go back to her again.

Your numbers were off a little bit from mine. I read a report stating that between October 2015 and September 2016, “five times as many electronic media searches—23,877—were conducted by U.S. agents”. I believe you said it was around 19,000. The report said that “NBC reported this week 5,000 searches were conducted in February alone”.

How do we stop that trend? Obviously, it's trending up sharply, and it's going to continue. Are we at risk such that, if we want to enter the U.S., we're just going to have to basically give agents whatever they want? It's quite clear they can deny entry for really almost anything now, right?

Ms. Esha Bhandari: The numbers you saw were originally provided by the U.S. government, but they have since revised them downward, which explains the discrepancy between the 23,000 and the 19,000. Nonetheless, even with the revision downward, it's clear that there's been a sharp spike.

We have been pushing for change on this on a number of fronts. One is, of course, litigation, which in U.S courts is pending at various levels and is often coming up in a criminal context where there is a criminal prosecution and someone is challenging the search of their phone that happened at a border. It is possible that litigation will lead to a higher standard that is required for searches—some level of suspicion.

Notably, there has been one appeals court decision, from the ninth circuit, one of the western circuit courts, which did impose a reasonable suspicion requirement for forensic searches, namely, searches that take place off-site and are the more invasive searches. We have been seeking records of compliance with that decision and so far have gotten no evidence that there has been any change in policy to acknowledge at least this higher level of suspicion, but litigation continues and is a priority.

The second area is legislation. There has been domestic legislation introduced. It would require a warrant for searches of devices, but only for U.S. citizens and lawful permanent residents, so it would provide no protections to Canadians who are visiting. That's not contemplated by this bill.

The last is our push for transparency. We think the numbers aren't enough. Specifically, we think we need to know the nationalities of individuals searched and the reasons given. It's hard to ascertain a pattern of why particular individuals might have their phones searched or not, especially when there is that policy allowing for suspicionless searches.

● (1655)

The Chair: Thank you very much.

We'll now move to Mr. Jeneroux, please, for seven minutes.

Mr. Matt Jeneroux (Edmonton Riverbend, CPC): Thank you, Mr. Chair.

Thanks to all of you for being here and preparing for us today, and for waiting for us to vote. It is not a fun part of the votes.

I want to throw this question out for everybody. In reading some of the background material on this, I see that there is a lower expectation of privacy at border crossings at airports, and on land as well. This comes from two specific cases: the Privacy Commissioner's own document, entitled "Your privacy at airports and borders", and also the 1988 Supreme Court case, R. v. Simmons, which mentions that "travellers seeking to cross national borders fully expect to be subject to a screening process". I didn't really think about that much until reading this. There does seem to be a lower expectation, in that we go through security and now go through scanners.

Perhaps you can comment on whether that is based on legislation that's in place, in your opinion, or is it just societal norms that have changed from the beginning of airports to now?

Maybe we'll start with you, Ms. Bhandari.

Ms. Esha Bhandari: Sure. Thank you very much.

I think a few things that underlie that assumption no longer hold when we're talking about searches of electronic devices. One is the idea that travellers have been able to control what they carry across the border with them, and therefore there may have been this assumption in previous jurisprudence and legislation and policy that travellers, fully aware of what they're bringing across the border, know that they will be searched under a customs rationale for contraband and things that cannot be carried across the border.

Those assumptions just do not hold when we're talking about electronic devices because of the wealth of information they store. There's the idea that because someone's phone is connected to the Internet and, therefore, connected to their email, their social media, all of their accounts, and their financial records, they are somehow, in a meaningful sense, transporting those records across the border in a way that opens them up to be searched. I don't think that rationale holds, and I think that's why we need to really push back against this notion of extending to electronic devices the customs rationale for searching.

I think this is particularly shown in the practice of forensic searches. As I mentioned, people can even have deleted items searched. The government can get access to those. Again, in no meaningful sense do people have control over what they are bringing across the border, so I don't think we would say that people have a diminished expectation of privacy in their entire digital lives.

Mr. Matt Jeneroux: Ms. Vonn and Ms. McDermott.

Ms. Micheal Vonn: Yes, absolutely, we would concur with all of that.

I would merely point out that a diminished expectation of privacy doesn't mean no expectation of privacy. The question of what is constitutional at the border is constantly being reframed through not only issues of new media and electronic devices but also the other items that were referenced by, for example, our colleague at the CCLA—the question of passwords, compulsion in relation to all of those, and whether or not that constitutes obstruction. In all of those policies we have so much grey in terms of shaping the constitutional framework that we are operating in a definite information deficit.

Mr. Matt Jeneroux: Ms. McPhail.

Ms. Brenda McPhail: I'm going to be harmonious and agree with both of the previous speakers.

I think it's really important to speak to the difference between a phone, which is like a window to your life, and a suitcase, which contains socks and underwear and maybe a couple of pairs of jeans. They are qualitatively different things, and we're dealing with them in the same way. We argue that it simply doesn't make sense.

Even if we think it's very important that we have strong security at our borders because we don't want bad things to come in—that was one of the rationales behind the Customs Act, that we don't want bad things crossing our border—electronic documents on a device are not a "thing" in any sense. They're not being imported into Canada in any real way, because they exist whether or not they're coming across the border. They could cross the border with the human or without—online. There's no real physical importation of a document that makes that document any particular risk to national security or to the sovereignty of Canada. Those are the principles on which we say there should be expanded powers of search at the border, because those two things, national security and sovereignty, are so important. That's why we really think it's time to update the legislation and think about the fundamental differences between electronic devices and suitcases.

● (1700)

Mr. Matt Jeneroux: Perhaps I can provide some comment in the hope that you guys can weigh in on the other side of this. Knowing that there would be a hesitation to send material, whether it be illegal documents, electronically.... You're then worried about a secure server and so on, as opposed to bringing an electronic device, putting it in front of somebody, and saying "Here", that being the illegal document.

There still appears to be a threat there. Somebody could bring something across on their phone that they wouldn't necessarily feel comfortable sending over some sort of server.

Ms. Brenda McPhail: I think issues of threat probably deserve some examination in relation to documents that relate to solicitor-client privilege, which was sort of the framing of the question. Where documents are private because they're in connection to a case, and we recognize that privilege in every other setting, there's no reason why they shouldn't have the same privilege elsewhere. They're no more dangerous at the border than they are sitting here in this room.

Mr. Matt Jeneroux: Okay.

Is my time up?

The Chair: I think so.

Monsieur Dubé, you have seven minutes. Go ahead, please.

[*Translation*]

Mr. Matthew Dubé (Beloeil—Chambly, NDP): Thank you, Mr. Chair.

I have a question for the representative of the American Civil Liberties Union, or ACLU, but first I want to speak to the two Canadian associations.

Thank you for being here with us. Like my colleague before me, I want to thank you for your patience during the votes and all of the interesting moments we experience at the end of a parliamentary session.

There have been many references to a ministerial guideline from the Minister of Public Safety concerning the search of electronic devices. We must remember that this guideline is not a law; that distinction is important. We believe that the guideline, contrary to what has been claimed, is much too permissive and gives far too much power to borders services agencies.

Would the representatives of the Canadian Civil Liberties Association and the British Columbia Civil Liberties Association have any comments on that?

[*English*]

Ms. Brenda McPhail: I have to apologize profoundly. I don't have a device for translation, and I don't understand.

The Chair: Oh, boy.

[*Translation*]

Mr. Matthew Dubé: Would our friends from the British Columbia Civil Liberties Association like to make any comments?

[*English*]

Ms. Micheal Vonn: Certainly.

I take it by "executive order", you mean the recent U.S. executive order and how—

Mr. Matthew Dubé: No, I mean on the Canadian side, the ministerial directive concerning cellular phones, which the government references in response to any questions we ask.

Ms. Micheal Vonn: So this is the internal directive of the CBSA?

Mr. Matthew Dubé: That's correct.

Ms. Micheal Vonn: Okay. Thank you.

Our point about that is that it's two-fold. One, there seems to be a recognition within that directive that something other than a suspicionless search is appropriate in the context of electronic devices. But, as you say, this is not codified in law anywhere. This is merely guidance.

We would like to see and the OPC would like to see that guidance given teeth, the actual strength and ability to be enforceable through the enacting of a consequential amendment to the Customs Act that would essentially make that practice, if it is indeed a practice, and we have no means of actually knowing that at this juncture, codified in law so that we can count on it and say this is the way it is.

● (1705)

[*Translation*]

Mr. Matthew Dubé: Let's talk about a specific example related to Bill C-23 and to the fact that this is not stated in the law.

Based on the protection afforded by the Canadian legislation, it is possible to conclude that if there were an American presidential decree, and if the Canadian law remains silent on this point, travellers would not be protected from searches of their cell phones, for instance. Is that correct?

[*English*]

Ms. Micheal Vonn: Yes, that's our understanding, absolutely.

[*Translation*]

Mr. Matthew Dubé: Ms. McPhail, I will ask you again about the guideline with regard to the agency. Do you have any comments to make on this?

[*English*]

Ms. Brenda McPhail: I think it's a very good example of the way that you can't rely on laws to stay the same. You can't say it's okay that we have a bad law, because the person in charge is not going to do anything wrong with it. We need to be cautious, to make sure that what we have here says what we mean it to say and to make sure that it provides the protection that we want to provide.

The examples we have in the States, where laws are essentially being made by executive order, are very good examples of the way that the rule of law is at risk if we don't have strong, effective, and not vague laws in the first place, which are harder to challenge.

[*Translation*]

Mr. Matthew Dubé: Thank you.

[*English*]

To Ms. Bhandari, on the American side of things, how are the risks of profiling increased through the information that you can find on someone's cellphone? I'll just give a specific example to contextualize the question.

There was a case a few months ago of a gentleman from Vancouver, who was crossing into Washington State and was turned away at the border because when they discovered, through his cellphone, his sexual orientation, they wrongly assumed that this person would be going to the U.S. to be a sex worker, which was obviously a gross situation of profiling.

Is there a concern as well on that end of things not only because of the invasiveness of going into the cellphones but also since you're basically creating a longer list of stereotypes and prejudice that can be used against a traveller in an inappropriate way like that?

Ms. Esha Bhandari: We're very concerned about that. We have commented publicly in the context of new so-called extreme vetting procedures that have been applied to certain visa applicants. The U. S. government has now begun seeking social media information on these applicants from particular countries. I think the same concerns hold true when you're talking about information that's gleaned from a cellphone, which, as I mentioned, could include social media. Without policies explaining the guidelines for use of that information, without rules constraining the discretion of an individual officer, and without really specifying what use is to be made of these, an avenue is essentially opened up for individual visa officers or border agents to profile individuals, to take information out of context, and to deny people entry or rights without giving those individuals any opportunity to even respond. We think that the search of electronic devices greatly raises that risk of having information gathered without context and with no explanation of how it can be used to determine admissibility.

Mr. Matthew Dubé: There's always talk of these executive orders, and you mentioned one bill that's before Congress, if I'm not mistaken. What's the sense of the direction this is going to go in on your side of things?

Ms. Esha Bhandari: It's hard to predict. Litigation may deal with some of these issues. Court decisions may deal with the sort of baseline search requirements. I think there's going to have to be advocacy to change policies when we're talking about gathering social media information. I think that goes even for information that's available publicly. We're very concerned about the impact on freedom of expression and human rights worldwide if it becomes a condition of travel that people even have to turn over their social media handles. That can have a big impact on people who have anonymous accounts, for example—many activists have anonymous accounts—and many individuals who may not be out about their identity. So I think this kind of gathering of information in multiple contexts has broader freedom-of-expression concerns for us.

● (1710)

The Chair: Thank you very much, Mr. Dubé.

We now go to our last seven-minute question from Mr. Saini. Then I think we'll have time for a couple of five-minute rounds and then just a couple of minutes at the end for some committee business.

Mr. Saini, go ahead, please.

Mr. Raj Saini (Kitchener Centre, Lib.): Good afternoon, everybody.

Ms. Bhandari, my first question is for you since you're in the United States.

I have a very hard time understanding this, because you're talking about something in the United States right now such that there is this very heightened sense of national security. On the one hand, you have an executive order, which is not going to protect the privacy of non-U.S. citizens. You have one major privacy shield between the European Union, which is 28 countries, and the United States; and you have a similar understanding with Canada and probably other countries in the world. Is it not sort of ironic that the United States is demanding that the privacy of U.S. citizens should be equal to or as important as that of non-U.S. citizens to make sure there is reciprocity with the rest of the world? What is the feeling there? I do not understand. Can you provide some commentary as to why they are doing this? To me, it seems as though they're lessening their national security, because they're exposing to risk their own citizens, because in some cases, other countries may not be as prudent about protecting their privacy rights. Could you just kind of highlight why this is happening?

Ms. Esha Bhandari: With respect to the Privacy Act, I think that the executive order was passed, quite frankly and unfortunately, to enable this office to be created for victims of crimes committed by immigrants. There is unfortunate rhetoric going on about publicizing crimes committed by immigrants and therefore needing to strip Privacy Act protections in order to share that information with the public. We've already seen one unfortunate effect of this, which is that a recently published database that purported to be providing information about immigrants who had allegedly committed crimes contained information about victims of domestic violence and abuse, individuals whose information should be protected. It certainly puts them at risk if this this information is publicly shared. I think the goal of creating that office is connected to the Privacy Act executive order.

Certainly in our letter to the European Parliament and the European Commission, we highlighted how this undermines that agreement and, again, in our advocacy in the United States, we also point out that the reciprocity concern is real. Americans travelling to other countries may be asked for similar information—social media passwords, email addresses, and for access to their phones—which should be a huge concern to the U.S. government as well.

Mr. Raj Saini: The second question I have is open to everybody.

I'm sure you're aware that the United States Congress recently rolled back regulations put in by the Obama administration for regulating ISPs. The online advertising market is worth $83 billion, and now there is a recusal of ISP providers from having to follow the same protocols with regard to someone's browsing history, usage of apps, and location. All of that is now exposed and it's all held in the United States, so for people travelling back and forth, is there a worry about the exposure?

I'm specifically talking about Canadians and other people visiting the United States.

Anyone can start.

Ms. McPhail.

Ms. Brenda McPhail: I think whenever we hear about this regressive rolling back of privacy protections that were hard fought for, of course there is concern.

It's not clear to me the degree of risk that Canadians face, but the reality is that our online lives are not constrained by borders. We deal with U.S. companies, and we browse sites owned by U.S. companies. I don't know for sure, but my speculation would be that we should be concerned, because our information is bound to be caught up in exactly the same net that American information is going to be caught up in, in that there is no regulation about not sharing this kind of information.

Where there is some level of protection in Canada, obviously when we're talking about a law referring to ISPs, is that most of us probably have subscriptions with a Canadian service provider here in Canada, but then many of these telecommunications companies have global reach and are networked together in ways, some of which we know and some of which, as ordinary citizens, many of us don't. But, again, that would put information at risk potentially through those kinds of connections.

● (1715)

Mr. Raj Saini: Ms. Vonn.

Ms. Micheal Vonn: I have nothing substantial to add to that.

Mr. Raj Saini: Is there anyone else?

Ms. Bhandari, I hate to pick on you, but since you're in the United States, do you know of any privacy...? If you look at what's happening with the FTC, especially with its concept of net neutrality, it can go either way. Do you see anything or foresee anything? Do you see the situation getting worse or getting better, or is there any kind of outcry in the United States, or any kind of push-back to correct that executive order, or at least try to sort out the friction between the FTC and the FCC, especially with regard to net neutrality?

Ms. Esha Bhandari: Yes, I think there is going to be a huge push-back and there already has been. The first battle over net neutrality was waged here. I think people are expecting round two.

This is a huge issue. The same community and the same coalition that fought for net neutrality the first time around is still engaged. I would say the same on the issue of ISPs.

I think, in fact, perhaps Congress was surprised by the extent to which this issue actually received a lot of coverage and a lot of attention, and got a lot of push-back, more than expected.

Mr. Raj Saini: Thank you very much.

The Chair: Thank you, Mr. Saini.

We'll now go to Mr. Kelly, please, for a five-minute round.

Mr. Pat Kelly (Calgary Rocky Ridge, CPC): Thank you.

I'd like to try to get the measure of some of the problems that have been identified by anecdote. I don't mean to criticize identifying problems by anecdote. As elected officials, we do it all the time. Constituents come to us with problems, and we know many Canadians want a predictable, smooth, and efficient process at the border. They also want to be kept safe from external threat, so there are a lot of complicated issues that go along with border security.

I was struck by one bit of data that we got with respect to devices searched at the border. If I got it down correctly, there were just over 8,500 in 2015, and 19,000 in 2016, or double the number. That's a trend, one could say, doubling in a year. I don't know what 2017's number might be.

What is known about these device searches? Do we have any idea about the identity of the devices, by nationality, searched at U.S. borders?

Ms. Esha Bhandari: We don't know much beyond those numbers. There is currently a pending lawsuit seeking more information, seeking specifically the records that you mentioned: nationality of individuals searched along with the reasons.

Mr. Pat Kelly: Okay, so we don't know if they're mostly Canadians, for example. We have really no idea.

Ms. Esha Bhandari: We don't. The ACLU got some records in about 2008 to 2010, and about half of the searches conducted in that period, I would say, were of U.S. citizens, but we don't know about the other half.

Mr. Pat Kelly: Okay. Do we even know what type of information is being sought in a device search? Do we have even anecdotal information? Mr. Dubé referred to one particular case of a Vancouver resident. What is being sought in these device searches, and what are some of the other complaints of those who have had devices searched, and what have been the outcomes of those searches?

Ms. Esha Bhandari: We don't know systematically. Individuals who are U.S. citizens who have been aggrieved by a device search may sometimes file an administrative complaint seeking access to the records that were retained from their phone. That might give individuals an indication of what was taken from their phone, what records or notes were kept by the government. But we don't have a systematic policy stating what's being searched, what the search terms are, what's being retained. We do know that the government is supposed to destroy copies of information from a search if it finds no probable cause of an offence having been committed. Again, we don't know how often they find probable cause, how often they destroy information as they are supposed to according to the policy. This is all information that hasn't been revealed.

● (1720)

Mr. Pat Kelly: Okay. I understand the point that Ms. McPhail has made, that a telephone is not in and of itself contraband, for example, in the same sense that people have long been accustomed to being searched at the border for. What kind of rationale and what types of information have law enforcement or, indeed, what complaints have Canadians made about items that have been found or behaviours that are perhaps being searched for by border authorities?

Ms. Brenda McPhail: We don't know a lot in the Canadian context. CBSA has not provided the numbers that ACLU can provide for electronic device searches in the U.S. We don't even know the rough number of devices searched, never mind what they're looking for. We don't know what they're looking for necessarily. We don't know what's being retained. We don't know how long they can keep it. So there's a really big information vacuum.

If you go back to the level of anecdote and away from systematic collection of data, we hear stories about phones that are ostensibly being searched to look for receipts for goods that are being brought across the border, which makes perfect sense, and then the email is closed and they go off on a hunt through photos just to see if they might have anything racy.

Mr. Pat Kelly: Very quickly, because I'm just about out of time, does anybody know in comparison to the 20,000 searches, what's the total number of crossings into the United States?

Mr. Raj Saini: It's 390 million.

Mr. Pat Kelly: Okay, thank you.

A voice: It's hundreds of millions.

Mr. Pat Kelly: Okay.

The Chair: Thank you, Mr. Kelly.

Mr. Erskine-Smith, bring us home, please.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): First, thanks very much.

I want to start with the Operational Bulletin PRG-2015-31, "Examination of Digital Devices...". They're interim guidelines, and I hear the concern expressed that these were released because of an access to information request and were not properly transparent from the outset. I appreciate that they don't formally have the force of law —which may be something we want to consider. I completely appreciate the testimony by the ACLU that there are major gaps in privacy protections in the U.S. right now.

Apart from the password issue, walk me through what's wrong with the interim guidelines.

The question is for the BCCLA and the CCLA.

I'll start with Micheal.

Ms. Micheal Vonn: You bet. The first thing that's wrong with the interim guidelines is that we don't know whether they're being followed. They don't have the force of law. They are guidance. We would hope that they're being used, but we don't actually know, and we have no means of enforcing them if they're not.

Mr. Nathaniel Erskine-Smith: On that point, let's say our recommendation is that they have the force of law. Is the content a problem? I want to get to the password protection issue and the ability to force individuals to give out their passwords, but bracket that conversation for the time being. Is there anything else in the guidelines that you would take issue with?

Ms. Micheal Vonn: In terms of the wording, they talk about "indicia". We would like to see that translated into what we consider to be standardized legal language, so that would be "reason to suspect", probably, on that one.

Mr. Nathaniel Erskine-Smith: I have a question on that.

I have the guidelines here. In fact, they reference statutes. IRPA, as an example, in subsection 139(1), talks about "reasonable" grounds, so there is a threshold under the Immigration and Refugee Protection Act. Under the Customs Act, the guidance suggests that it be "conducted if there is a multiplicity of indicators that evidence of contraventions may be found on the digital device or media". Is the area of concern that this is vague language?

Ms. Micheal Vonn: Yes. What that translates into in terms of legal standard should be clarified.

Mr. Nathaniel Erskine-Smith: It strikes me that this is probably a misinterpretation by the CBSA in the first place, because if you look at paragraph 99(1)(a), you see that it doesn't really make sense that it would apply to cellphones at all, but you can look at paragraph 99(1)(f), which would probably be better grounds for searching any goods, and that actually does set out a "reasonable grounds" criteria.

You don't have it in front of you, but if both the CCLA and the BCCLA could look at this and assess if paragraph 99(1)(f) actually makes more sense, would you be comfortable with that? It does set out reasonable grounds in the act. Maybe we could, rather than rewriting things, just specify that this would be the source of search. Paragraph 99(1)(a) doesn't make sense to me at all. For example, it says to "take samples of imported goods in reasonable amounts". How would that ever apply to a cellphone that has not been properly imported?

My second question is related to the password issue. In the guidance, it says that officers may “request the password” and that it's “not to be sought to gain access to any type of account...stored on-line”. In fact, the indication is that is should go on airplane mode or something like that. It also says that if the “traveller refuses to provide a password...the device...may be detained”. I understand that there is at least one case where there was an obstruction charge and an individual pleaded guilty and paid $500, although I do note that this does say something rather bizarre, which is that “[u]ntil further instructions”, they suggest not arresting a traveller for obstruction and maybe charging him after the fact.

What in the BCCLA's view would be appropriate language with respect to password protection at the border, if not this?

● (1725)

Ms. Micheal Vonn: I would have to consider that and be able to get back to the committee. I don't have it off the top of my head—

Mr. Nathaniel Erskine-Smith: That's okay. That's a better use of my five minutes, actually. If both the BCCLA and the CCLA could provide a submission in writing as to what the preference would be on dealing with passwords at the border, that would be great.

The other thing to clarify in the guidelines as you cut them apart is perhaps this. The CBSA guidelines also make clear that with respect to a search under paragraph 99(1)(a) of the Customs Act, it's for customs purposes only, so the idea that it's searching very broadly for other reasons wouldn't necessarily hold water. I guess what I really want to get at is that I understand we have to codify this in law in a better way. It does strike me as codified significantly already in the Customs Act and IRPA, and to the extent that we can do that better, that's great, but I would like to know what's wrong with the guidance and delineate that as much as possible.

I think I'm pretty well out of time. Those are my questions. Thanks very much.

The Chair: Thank you, Mr. Erskine-Smith.

I have a couple of quick questions, if I may, for Ms. Bhandari.

When a traveller comes across the border, can U.S. Customs agents discern the difference between data that is pulled to a phone, which is information that is willfully brought to the phone by the user of the phone, and information that is pushed to the phone, which is not done willfully or is maybe even unwanted information that is pushed to the phone? Are there any guidelines insofar as that?

Ms. Esha Bhandari: Certainly not in the policy that's been publicly released, and I haven't seen anything making that distinction in either recommendations or a policy.

The Chair: Is there any policy or guideline surrounding the data that might be found in a cloud, given the fact that many data plans and sharing plans have numerous devices on there from multiple users in the same family, business, or group unit that share the information on that same cloud? Are there any guidelines outlined there that Canadians should be wary of?

Ms. Esha Bhandari: There are no guidelines or even any reference to that in the 2009 policy. We have heard—again, anecdotally—of individuals having their social media accounts searched, presumably with no regard to whether it is shared with other individuals.

The Chair: Who was overseeing any of the tests in which cause could be found, and who was overseeing any of the tests to destroy or delete the information where no cause could be found?

Ms. Esha Bhandari: Concerns have sometimes been raised to the Office of the Inspector General in the Department of Homeland Security.

There was a civil liberties impact assessment conducted several years ago examining the practices and whether the policy guidelines were being complied with. Those are some of the avenues that advocates are taking, and then of course individuals may sometimes bring administrative complaints, with varying levels of success.

The Chair: Has there ever been an incident, that you're aware of, in which a foreigner's phone, or in particular a Canadian's phone, was held by United States customs agents and not returned when no charges were laid?

Ms. Esha Bhandari: I'm not aware of any incidents that I can describe.

● (1730)

The Chair: Thank you very much.

I'd like to thank all of our witnesses for their patience in this.

Colleagues, I want to have a quick two-minute in camera meeting to discuss committee business for next week.

I would like to thank the Canadian Civil Liberties Association, the British Columbia Civil Liberties Association, and the American Civil Liberties Union for their patience today.

Please submit to us any thoughts that you might have or any written responses that you have to some of the questions that were asked.

Colleagues, we're going to suspend. We'll go in camera for about two minutes.

[*Proceedings continue in camera*]