[00:00:01 The CSPS logo appears on screen.]

[00:00:03 Tom Dufor appears in a video chat panel.]

Tom Dufour, Statistics Canada: Good afternoon and welcome back to the 2022 data conference on driving data value and insights for all Canadians. Good afternoon and welcome back to the 2022 Data Conference, Driving Data Value and Insights for All Canadians. We hope you enjoyed the simultaneous sessions this afternoon.

As a reminder, we are taking questions through this webcast interface. Please go to the top right corner of your screen and click the participate button and enter your questions. This is our last keynote address. It gives me great pleasure to invite my colleague, Éric Rancourt, Director General of Modern Statistical Methods and Data Science at Statistics Canada, to introduce our next guest, Chantal Bernier, who will discuss privacy and data protection frameworks for the public good. Over to you, Éric.

[00:01:02 Two more panelists join.]

Eric Rancourt, Statistics Canada: Thank you very much, Tom. Nana, hello. Hello. Good afternoon and welcome to today's keynote address. I'm Eric Rancourt, and I will be your session moderator. I would like to give a friendly reminder that we have simultaneous interpretation available through teleconference lines for this discussion. You may also access the CART services and the sign language interpretation through the webcasting platform. So, let's start the session.

This is about privacy frameworks and data for public good, but what does that mean? I've been hovering through the sessions yesterday and today in the data conference. These were topics that came out explicitly or in passing in many of the sessions. Because there are two aspects of the work that we have to do with data. So, it's about personal interests. It's about mutual and collective interests. It's about enabling the use of data for people and for Canada. So, the issue is about how to find an optimal point between these aspects. So, there is a clear link to legal aspects, but also more generally frameworks, principles and approaches. So, to discuss these issues, it is my great pleasure to welcome Chantal Bernier. Hello, Chantal.

Chantal Bernier, Dentons: Bonjour.

Eric Rancourt: Chantal is an expert in the legal system and the whole foundation that supports, what can you do with data, how it frames, privacy, how it frames access, and we're going to discuss that in the next hour. Chantal Bernier leads Dentons Canadian Privacy and Cyber Security Practice Group. She is also a member of the firm's Government Affairs and Public Policy group. As assistant and interim privacy commissioner of Canada, Chantal led national and international privacy investigations in the public and private sectors, as well as privacy audits, privacy impact assessment

reviews, technological analysis, and privacy policy development and research. Chantal provides strategic advice for her clients and brings to the table her experience as a senior public servant in the Government of Canada. She currently sits on Statistics Canada's Advisory Council on Ethics and Modernization of Microdata Access. She also sits on the steering committee of the Standards Council of Canada's Canadian Data Governance Standardized Collaborative. So, welcome again, Chantal.

Chantal Bernier: Thank you.

Eric Rancourt: So, for this session, I will be asking a few questions to Chantal, and then I will turn to questions from the audience. So, to get us started Chantal, let's start with an introduction of the overall issue. We all know when we have seen and heard pretty much in all discussion forum that involve data, that privacy protection draws high interest. At the same time, data constitutes a magnificent asset to produce public good and propels Canada forward. So, how should we go about making both work?

Chantal Bernier: Well, Eric first of all I want to say how happy I am to join you all after 27 years in the public sector and the government of Canada. Yes, I have gone back to private practice now, but I will never forget my all the family. And it's just a great joy to be with you again today. So, you've just summarized the tension, Eric. You spoke of the magnificent potential of data, and then the fundamental right to privacy. Why is there a tension? There is a tension in fact, increased from what we used to need to reconcile. We used to have pretty static data. Meaning for example, every year I tell the Canada Revenue agency, how much I earn and they use those figures to determine how much I should contribute to the public person that is static. The huge, the critical difference that we are in front of now, is dynamic data.

Meaning that the data I provide, we can make more personal data with. That's the profiling, that's the algorithms. And so, we have said, you must have heard that phrase so many times, "Data is the new oil." Jim Balsillie says, "Data is the new plutonium." And I like that image because it expresses the explosive nature, meaning that it doesn't just stay static. "I give you this data, you do this with it." It is dynamic because with the data I give you, you can draw lots more about me. How do we reconcile that with the fundamental right to privacy? How do we reconcile the fundamental right to privacy with the fact that we have a treasure, truly a treasure to inform public policy in a manner that will make it so much more efficient and effective. I will state outright, and we will go into further detail in our conversation, that the restraints upon you should be revised. They are too restrictive to allow true optimization of data. We can't protect privacy and drive data value at the same time. We do not have quite the legislative framework to do it now, but let's use what we have now.

So, the guiding posts that you have is first of all, the charter. The charter does allow the use of personal data as long as it is reasonably demonstrably justified in a democratic society. You have the Privacy Act that allows the collection of personal data and use of personal data, as long as it is directly related to the programing activities of the institution who collects them. And then you have treasury board directives on

privacy impact assessments, and they truly constitute a map to actually consider what kind of personal data do we need? How much do we need? Why do we need it? And it formalizes this analysis in a very concrete structure that documents, essentially, your application of both section one of the charter and section three and four and five on consistent use of the Privacy Act.

So, I would say to you, let's just start with that, that if you can demonstrate that there is necessity for data, then of course, as long as that necessity remains valid, secondly, as long as the collection and use of data is proportionate to that necessity and that it is effective and that there's no less intrusive alternative, you have a solid constitutional grounding to use personal data. If you do not have that grounding, you cannot demonstrate that it's necessary. For example, a longitudinal study on a specific issue could be fabulous for Canada. But really necessity, can't be really demonstrated, then consent. Then you have to have valid consent from the individuals. And if neither of those is possible or practical, then you have an anonymization, anonymization at source, meaning that you would collect the data without ever collecting the identifiers in a manner that the data remains irreversibly anonymized. Can never be related to the individual. So, those are the building blocks in general. We'll go into great detail, but these are generally the building blocks of harmonizing the search for value and data while protecting privacy.

Eric Rancourt: Thank you. You stress the great importance of necessity. And I would like to go on a bit more on that because I think as a government enterprise in general, and at Stat Can, we've done that. But in general, organizations have struggled to really explain in terms of what are the needs of Canadians, not the needs of this department or the need of the stakeholder. So, can you say a few things about the importance of speaking in terms of needs to Canadians rather than need for this program or need for that program, or I need this file to enhance this other file. Could you say a few things about that?

Chantal Bernier: Well, you see, you just pointed to one area where the law needs to be rethought, because right now the Privacy Act allows the use of personal data in a very siloed way. It says “the institution can collect and use personal information provided it is related to its programs and activities." It doesn't speak to the collective good. So, that's definitely something I would put on the policy table for the reform of the Privacy Act. What you can do now is tie the use of the data you would make to your program and how your program fits into the common good. Of course, the common good is also a bit of an amorphous notion, but I have seen particularly when I was at the Office of the Privacy Commissioner of Canada, very audacious uses of personal data. I'll give you a concrete example where it worked and I'll explain to you, I'll tell you the story.

And that's when the body scanners were introduced in Canada, highly intrusive. So, it's not what you're talking about in the sense of a voluminous use of personal data to draw trends, but it was very intrusive. So, what CATSA did? First of all, involved the OPC from day one. Explained the necessity for example saying, "We have authoritative intelligence that the highest risk right now for airline safety is nonmetal explosives. So,

we need to address that." We have done tests with our staff for pat downs. And we realized that being prudish, thank you, CATSA officers were not patting everywhere and had reluctancy in patting certain people. So, the test showed a lot of planted nonmetal explosive were going through. And that the body scanners were really the only way. They made it proportionate, meaning the person who saw the passenger go into the scanner was not the officer who was seeing the image.

The image was blurred. Then in fact, the image was reduced to merely a stick figure that shows you forgot to remove the change you in your pocket. So, it was totally proportionate. They had a coaching case for effectiveness, actually two months after they announced the implementation of the body scanners, the famous underwear bomber was caught. So, there was something very solid.

And that's how they managed public opinion. They had such a strongly documented case. Not that there was no outrage- you'll remember there was. But they did have the arguments. It lasted three days. I remember, I think I did 21 interviews in three days because critically, what they did is that they had ticked every box with us. So, those are the instruments you have now. You do have valid objectives within your program's activities to drive value from personal data, you do have privacy impacts that structure your justification for your driving value from data. And you have the Office of the Privacy Commissioner who will not approve the PIAs. They don't approve, but if you follow their recommendations, you could land in a spot that will allow you to perform the driving value of data that you want to perform within public trust in how you protect privacy. Those are the instruments you have now.

Eric Rancourt: Thank you so much. I hope people are taking good notes because this is some kind of recipe, not to guarantee that we can do what we need to, but to really guide us well. You closed on trust, and I'd like link it to what you said about data being the oil and the plutonium. I think society realizes that data are important. And sometimes when we, government, ask data of Canadians, they might say, "Well, you already have that. I gave it to the other department," but at the same time, plutonium needs to be well guarded because it cannot breach. So, we hear media reports about breaches and these breaches may erode the public trust. So, how do we educate the public to understand that a breach is not the same thing as the importance of sharing data among the different arms, for instance, of government, these are not breaches. These are data sharing.

Chantal Bernier: Exactly. So, a breach, as we all know, is unauthorized access to personal data. Data sharing is the sharing through a governance process with protocols of authorization. And that is truly what makes the difference. As I was mentioning a moment ago, I saw a lot of daring ways to share data. Let me mention you now, the four filters approach. So, the four filters approach is in the context of crime prevention. And so, it is a protocol that multidisciplinary tables of intervention share data. Concretely, you will have the police, the school, the hospital, the social services, for example, sometimes also the housing services come together to assist at-risk families. We're talking about crime prevention.

They start, the first filter is one of them will bring to the table that there is a case completely unidentified. Just, we are wrestling with this kind of multiple issue in this family. Then the group will decide as to whether this should go to the second filter, meaning that it really should bring together the actors who could make a difference. If it goes to the second filter, then a little bit more information is provided. And if it then goes to the third filter, then personal information, identifying information is shared. And the fourth filter is when they truly work together to get to an integrated outcome. Meaning it's a very tight... Going back to your point a moment ago, you said plutonium needs to be contained. It's a very tight governance framework to allow the protective sharing of personal information. And the protection comes from that protocol of all of the interveners, where they agree exactly on how to share and protect that information. That's another example.

Eric Rancourt: Okay. Thank you very much. I wonder how we could educate or help the public to understand these principles, and these steps. I think that between producers, actors, users of data, we convince each other quite well, we improve our processes and our protocols and our governance. But how do we . . . in your experience, how do we help the public to better understand?

Chantal Bernier: Transparency, transparency and I'll give you some concrete examples. I'm going to talk about MetroLinks, so MetroLinks, a few years ago, well, maybe 20 years ago, installed surveillance cameras in their transit system in Toronto. And of course, it wasn't unanimous, but they had the approval of the then Information and Privacy Commissioner of Ontario. So, there was necessity, proportionality, but MetroLinks added something to that. Every year, MetroLinks publishes a transparency report in which they say how many requests they've received from the police for personal information, because it's with—there's the surveillance cameras, but also the smart cards for using transportation, that also gives routes. So, how many requests they got from the police for this personal information, how many they accepted, how many they refused and the reasons. So, it was to find a lost person. It was to find a stolen item. There were all sorts of reasons. So, over the years, year after year, it built trust.

On the federal side, I think the idea of publishing privacy impact assessments (PIAs) is extremely useful. I know very well that there are some of these assessments, the PIAs, that contain information that is protected. Well, okay, they're removed, but posting the PIAs on your website, that, I think, can help tremendously. Also, make an announcement. Don't take Canadians by surprise. I'm looking at what your colleagues at the Public Health Agency are going through right now. I don't have any information to tell you if their plan to go after cell phone data was legitimate or not. All I know is that there was no effort to prepare the public.

It's probably completely legitimate, what the Agency is doing, and it's known around the world, that tracking cellular data is relevant to controlling a pandemic. But I think we have to be very sensitive in particular to the sensitivities of Canadians with respect to the protection of their privacy, and so we have to take action in front. And

even if, you said it very well earlier, we're completely convinced because well, we have our programs, we know that it's good to get personal data because our program is good, but more than that, we can also know that we aren't going to get personal data. For example, in the case of the Public Health Agency, they say, "But no, we're not going to look for personal data," it's dissociated from the identifier. But the fact is that Canadians are very sensitive, so you have to go even beyond that, could it appear to be using personal data? So, really understanding the sensitive nature of the issue and so being, as they say, proactive. And disseminate information to prepare Canadians for these personal data projects.

Eric Rancourt: Thank you. It makes me think that Canadians are entitled to comment or object and expect to have the opportunity to comment or object. It doesn't mean that they'll object, in fact, maybe they'll never object to certain things that seem obvious to us, but it's about having the opportunity. It makes me think of a connection to consent, consent in the public and private context, there are different issues. So, maybe, if you hear people talking about, what is consent, and how does it come into play or not, in the context of data for the public good.

Chantal Bernier: So, that's the legal basis for the use of personal data in the public sector, it's need. Basically, the legal basis is that a government collects personal data because it needs to. And that is established. Now, there are uses, personal data. As I was saying earlier. For example, a longitudinal study of the relationship to the labour market in a certain demographic group, and so on. Where the notion of need is perhaps a bit forced. So, at that point, you have to get consent. And so, consent has to be intentional, it has to be informed. And individuals must also be informed of their rights related to their personal data. Let's take the example of a longitudinal study based on consent. We offer a demographic group to participate in a study. We're going to follow them over several years. They absolutely have to be identified because we need to track the data to have a reliable conclusion at the end and they have to know exactly what they are signing up for. They also need to know that they have the right to access their personal data, that if they want to make a request for access. "What do you have on me?" and so on. "I've been in this longitudinal study for five years, what do you have on me? What do you . . . " and so on? They have access.

They also need to be told that they have a right to complain, first to the department, to the institution in question, but then also to the office of the commissioner. So, we really have two quite separate situations. For the private sector, that is to say, where need fulfills the legal basis, no need for consent. The Canada Revenue Agency does not ask for my consent. And by the way, you who are Statistics Canada, you remember the debate a few years ago? You don't need consent to answer a census or not because we don't have a reliable census, if it's not mandatory, okay? Need. Where there is consent, then it must be free, informed and evident. And also, it must be able to be withdrawn. But that's a little bit complicated because with a longitudinal study, by definition, you want long-term data.

So, if a person- I don't know, has done five years of a study that is over 10 years, decides to withdraw consent, well, can that apply, can we destroy the data we already have on that person? So, this has to be evaluated, but the person has to know this in advance and they have to have the right to withdraw their consent or at least for the future. For the data to be collected. And the third option, we have need, we have consent, the third option, it's anonymity. But it has to be in a context where you don't need to keep the identifiers.

Eric Rancourt: Thank you. Speaking of anonymization, this is a good segue into talking about security practices, because this is very well linked. So, security practices in IT security systems, we need these to safeguard the data. So, I'd like you to talk about that and say a few words in what you see that are good practices in place and if you can identify actors of the data world in Canada that are good organizations that have a good track record about that.

Chantal Bernier: Well, you just reminded me of a story, Eric, where one day... This is when I was at the Office of the Privacy Commissioner of Canada. I got a phone call from a deputy minister who said "We would like to develop a privacy program, is there a department in town that you think is the gold standard?" And I said, "Absolutely, HRSDC. They are terrific." And a month later HRSDC came publicly that they had lost a hard disc with 500, maybe 3,000 people's financial information. So, how did this fabulous system fail? I want to tell you that I asked my staff at that time to do the investigation in order to produce a report that would be a reference document for all of you, for as long as it is applicable. Because HRSDC was really, really good. Where it failed there was on asset management. That hard disc was not assigned to a specific employee who was responsible for it.

There wasn't a register that said that "Chantal had the hard disc and she was the one who was supposed to protect it." But otherwise, HRSDC is extremely impressive. Now, let broaden that to the good actors I see in general. What do they have in common? All these organizations, why do I say that HRSDC is terrific? And what do I say of many others? I have clients now, private organizations that come to me and say, "We'd like to upgrade our systems. What do you think? Da, da, da." And I look and I go, "Wow, they really need me because it's so good." So, what do they have all in common? First of all, they have a very clear structure for internal compliance with privacy law. They have a person who is assigned to it, they usually call it the chief privacy officer. That person is properly resourced, and that person is high enough in the organization to have authority to assure compliance.

Secondly, they have buy-in from the top. So, that in your case, the deputy minister, the chief statistician, whatever your organization's structure is, you need buy in from the top. That person at the top needs to understand that data protection has become a central institutional risk. You have to treat it like that. Meaning that that person needs to have regular briefings. Where are we at? CPO, tell me. Where are we at? Did you check? The CPO has to be very well connected to the chief technology officer or chief information officer, but it can't be the same person. Because a chief

technology officer is the person who implements the policies and practices that the CPO will develop. And the CPO is the one who will check compliance. So, you can't have the CTO check compliance of his own work. You need two people, but very well connected. The other thing that these actors have is full engagement of staff.

Staff realize that they are both the first line of defense and the highest vulnerability. Read the news, you've seen rogue employee, for example. One mistake by an employee. So, the staff are fully engaged, and the staff are trained on an ongoing basis. For example, every year or every six months, depending on the level of sensitivity of the data to protect, there are training courses and the staff have one month to take the course. It's online. Online, they just click, do everything and they have to pass. They actually have to answer questions, they to pass. If they don't pass, or if they don't take the test, they lose access to the organization's networks.

And the final thing that I noticed was really important, is also a breach response plan that not only is very good, super clear steps, but is socialized throughout the organization. I remember one example where the company phoned me on a Sunday because the Sunday morning, one of their accountants had gone to the office to do some work and she noticed something irregular. And because the breach response plan had been so well socialized, she knew exactly what to do within 30 minutes. They had clamped down and they were rebuilding, therefore mitigating their damage tremendously. In one word Eric, the best practice is a top-notch governance framework for privacy compliance that is disseminated throughout the organizations that really brings the organization around it.

Eric Rancourt: Thank you. This ties the conversation very well to what Catherine Luelo said, the CIO of Canada, that there needs to be governance that is just stringent enough so that it creates the self-asking and transpires throughout the organization in getting ourselves ready to really face- not just face the consequences but think through in advance of what we do. And this ties into questions that are now popping up. I'd like to share that we share the floor with people. So, how do you see the balance between privacy and innovation? How can we use privacy to promote innovation instead of hindering it?

Chantal Bernier: One of my favourite topics. So, to me, privacy is never ever a hindrance to anything it's a modality. So, it cannot stop innovation. It brings a modality on how you innovate. Innovation can occur with our personal data, but there's tons of innovation potential that is entirely predicated upon the use of personal data. So, what have the great innovators done? And I will refer you to the Allen Turing Institute. You can go online, look at what they do going back to the governance of sharing information that applies here as well. And it has taken the form that I like very much, called “data trusts.”

So, it means that the organizations that will mine the data, share the personal data, will adopt a protocol or will create an entity, the data trust, who is the steward of their access and sharing of the information. In fact, what you do at Statistics Canada is just so close to that. You govern the access of researchers to the data holdings you have. And it's based on legitimate access, legitimate purposes, very limited access, and you have audit trails, you check them, these guys cannot do something else that what you've authorized them to do on your system or with the data and so on and so forth. So, my answer is that privacy applies to innovation in how we do it, not whether we do it. And that governance models are arising, are appearing, that are allowing us more and more to reconcile privacy and innovation.

Eric Rancourt: Thank you. Interesting questions. Another one, is there a role that a unique digital ID can play in improving privacy, similarly to what Estonia has been doing since the early 2000s?

Chantal Bernier: Exactly. And of course, Estonia is the model. Interestingly, digital ID seems to have privacy advocates go in two opposite directions. You have those who are screaming blue murder because they say, "Oh my God, this is government tracking citizens." And then you have the others who say, "Well, no. Because that allows empowerment of the individual to its data under an ID that in fact is almost like a code. Therefore, it is privacy protective." Certainly, Estonia is held as a model because the governance structure, it has an X road, it has a governance structure that allows the use and access by various institutions of the citizen ID. In short, I believe it has huge potential and should be looked at as a way to improve data driving as well as in fact, even improve privacy and improve data sharing among departments without compromising the right to privacy.

Eric Rancourt: Thank you. Let's see. When you were talking about the four filters, is this an area where we are looking to use AI as a means of streamlining and improving data sharing of personal data in law enforcement?

Chantal Bernier: The way the four filters are applied, there has been no application that I know of to AI. It really is community work. It is really to bring together community actors around... Crime prevent is really a multiple approach. You don't become a criminal out of one factor. With respect to AI as you know, the regulations are developing. The new Quebec law for the private sector on personal information now has provisions on the use of automatic decision systems. The government of Canada, you have the guidelines on transparency of AI. So, definitely the four filters approach, as far as I know, was never applied to AI, but there are other privacy protective measures that are being developed around AI. And the transparency is one, the transparency of the algorithms, because it allows exercise of the right to access to one special information. If you're going to use my personal information through AI and I want to know how you did it, well, you have to be able to track that and therefore you need transparency of the algorithms. So, that's an example of integrating privacy to AI.

Eric Rancourt: Yes. Thank you. The next question, I think is to get some precisions or explanation on what you said about consent. My understanding and advice we receive from Justice Canada is that asking for consent where legal authority does not exist, does not mitigate the risk of violating the privacy act. Do you agree with this interpretation?

Chantal Bernier: Oh, I do. Absolutely. Absolutely. They are putting forward the multiplicity of factors. So, you cannot decide that you're going to seek consent to get personal information about something that has nothing to do with your programs and activities. So, I totally agree with that. They're saying, "Oh yeah," consent doesn't mean you can do anything. It just means that if you can't meet the threshold that you want to do something optional, but it has to remain within the Privacy Act. Related to your privacy and programs collected directly from the person and then you will be able to have a more solid basis for what you're doing. But yes, they're absolutely right. It has to be within the confines of the Privacy Act.

Eric Rancourt: Thank you. The next question is about opening. So, how realistic would it be to implement an open by design framework for privacy and data sharing in the government of Canada?

Chantal Bernier: Well, you look at what Saskatchewan did. So, there are more and more initiatives coming out where we're looking towards data sharing. The idea of opening makes me a little concerned. I'm all in favour for more data sharing to drive value from the data, for better results for Canadians. But as you said a moment ago, it still has to be governed by a very clear system of why you share, who you share it with, how much you share, how it's protected and so on. So, the opening to me would certainly raise a concern of surveillance. I'll give you a concrete example. Privy Council Office, I was director of operations for machinery of government at the time we established FINTRAC. And the big question was, "Where do we put FINTRAC? Do we put it under what was then the Solicitor General now Minister of Public Safety?"

And the answer was "No, we can't do that." Because the minister who governs CSIS and the RCMP who want to access the FINTRAC data will be in a conflict of interest to block that. We need to make sure that access to the FINTRAC data, all of the financial data of Canadians is protected. And therefore, that access is not open, but rather regulated, which is why FINTRAC ended up under the Minister of Finance. So, I would say that while I believe we should develop ways to share, the idea of opening raises the concern of non-consistent use, surveillance. So, perhaps it's a question of semantics, but that's how I react to the word “open.”

Eric Rancourt: Thank you. The idea of open data, it makes me think of a space where data is really very open, which is social media, Twitter, Foursquare, etc. People are sharing information on levels that you might never have thought that they would dare to do. So, can society, can people, expect data to be used for the public good? We're talking about, it's open but it's not completely open. And people's understanding may

not be as mature or may not have matured at the same speed as the proliferation of systems. So, what do you think about that?

Chantal Bernier: Absolutely. In fact, there's an investigation report precisely on this subject, from the Office of the Privacy Commissioner of Canada that I issued at the time, an investigation that I led. There's a second one that came out. Again, on social networks recently, with Daniel Therrien, and the Office of the Privacy Commissioner, has established very well that social networks cannot be considered as essentially an abandonment of the right to privacy. Just because someone has taken, posted personal data on social networks does not mean that a government institution has the right to collect it. The *Privacy Act* says that institutions must collect the information directly from the person concerned. Now, that would be a violation of that provision.

Then there is the fact that there is a split, if you will, in the use. A person posts their personal data on the internet. With, for some purpose, certainly with the reasonable expectation that the government will not use that data for other purposes, purposes that are unannounced, that are . . . There's a break, really, in the expectation of privacy, which is a legal concept that prevents that use. So, if you look at the position of the Office of the Privacy Commissioner of Canada on this, you'll see that it's very clear. Data posted on social networks cannot be considered as no longer being personal and as being available to the government for all, any purpose at all.

Eric Rancourt: Thank you. We talked a little bit about people, about responsibilities. I'd like to talk about the employees and the skills and behaviours that are expected because there is an increasing amount of data. We know that, it's well established, there are more and more people who are going to be data manipulators and estimators, people who do modeling, who make predictions and all that, but it's not always people who are aware of privacy and data ethics issues. So, in your opinion, what are the skills and the types of capabilities that we should be looking for or try to put in place in the public service, in employees, with employees in general?

Chantal Bernier: Yes, so one thing we see throughout all the public or private organizations where there is good protection of personal data is that there is a culture of protection of personal data. And that this culture is shared because one thing I see a lot in my practice is exactly as you just said. A group, for example, of engineers, who see an extraordinary potential in personal data, but are not quite aware, let's say, of the privacy implications. That's normal, they have their expertise, they have their goals.

Or in the private sector, it's the marketing people who see a golden opportunity to mine personal data like this and they're really focused on this goal. It's normal, they're marketing people. So, since we can't change everyone, what's important is to bring everyone together around a framework of accountability, of data protection. And on that, I'll give an example, again, a concrete example. Google Street View, you may recall that in 2011, it was discovered that Google, through its Street View program where a small car drives around and films all the streets to then give us the Street View results, had

also captured entire communications, entire messages, over Wi-Fi. They had captured that.

So, it was the privacy commissioner in Hamburg, Germany, who discovered it and alerted all the other commissioners. We did our research, we [unintelligible] indeed, there was Canadian data on there too, so we investigated. What came out of all these investigations, the Federal Trade Commission also investigated. There was a governance problem, that is to say that Google gives 20% of free time to engineers to innovate. Creating is great. This engineer had developed code that, it was believed, could determine where the hot spots were, the routers' geography, a mapping of the routers. Ah, well, that's a great idea, put that in Street View, when nobody has verified that that's all it did. But it wasn't just doing that, it was capturing conversations, the whole discussion. So, it was a governance problem. This engineer, well, they did their job and all that, but they weren't connected to an organizational privacy compliance system. So, in my opinion, that's the solution. We can't change people, we can't change our expertise, but we can rally around a common goal, which is the protection of personal information.

Eric Rancourt: Thank you so much. We're running towards the end of our conversation. It just went like a few minutes. It's always a pleasure to have a discussion with you. I would like to summarize a little bit some of the things I retained from what you said, the principles of privacy, they are anchored on the charter and there's a number of laws like the Privacy Act. But as you said, you need to be updated. A crucial point in government sector for privacy is that it rests on necessity. This is very important to define and explain well.

It was good advice. I'm not going to list all the points, but two or three times, you said things point by point what can be done. And this will be very useful to many, I'm sure. You've also stressed the point that it's also about risk management from the top to throughout. And as you just said a moment ago, it has to do with the culture. It has to be a shared culture in the organization. And sometimes well, some people might tend to see privacy as a hindrance, but it's a modality. And like you said, it's not whether, it's how. And so, improvements in innovation can happen. So, maybe in 30 seconds, I wonder if you could say just a few main points that we should retain from what you said in the last hour.

Chantal Bernier: Well, I think that you've already summarized it quite well. That has public servants, you are governed by the charter, which prohibits the use of person information, unless it is reasonably justified in a free and democratic society. And that captures the fulfillment of your objectives with personal information. So, I think that if you ground your work in that paradigm, you will have a very strong position to drive value from personal data.

Eric Rancourt: Okay. Thank you so much, Chantal. It was a real pleasure. So, this concludes the session. I would like to thank Chantal and thank the audience. Thank you, merci, miigwetch.

[00:55:52 The video chat fades to CSPS logo and “canada.ca/school-ecole”.]

[00:55:59 The Government of Canada logo appears and fades to black.]