HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 064 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, June 13, 2017

Chair

Mr. Blaine Calkins

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, June 13, 2017

● (1200)

[*English*]

The Chair (Mr. Blaine Calkins (Red Deer—Lacombe, CPC)): I am pleased to have this special meeting of our standing committee. This is meeting number 64. We are very pleased to have with us today from Rome, Italy, Mr. Giovanni Buttarelli, who is the supervisor and is going to be talking to us about the general data protection regulations of the European Union.

Thank you, sir, for making time for us. As you know, here in Canada we're reviewing the legislation. Of course, it's been brought up by many people here in Canada that, because of the Canada–European Union trade agreement, there are going to be potential issues and also some potential solutions we need to work towards to make sure our respective trading bodies are in alignment. I welcome you to the committee.

I'll remind members to please speak slowly. My understanding, Mr. Buttarelli, is you're fluent in English. Is that correct?

[*Translation*]

Mr. Giovanni Buttarelli (Supervisor, European Data Protection Supervisor): Unfortunately, the working language we use most often in our organization is English.

[*English*]

The Chair: No worries—you're doing better than me.

[*Translation*]

Mr. Giovanni Buttarelli: Allow me to speak to you in English.

[*English*]

The Chair: Okay.

Colleagues, please speak clearly and concisely when we're communicating. Mr. Buttarelli, we will give you the floor for your opening comments—I'm certain you have some—and then we'll proceed to questions after that. Thank you so much for joining us today.

Mr. Giovanni Buttarelli: It is my pleasure. Chair, and distinguished members of this committee. I really appreciate this kind invitation for me to speak to you today. Let me say that I'm very honoured.

I'm not the EU legislator. I am not formally in charge of any adequacy finding. I represent an independent institution, like the Privacy Commissioner of Canada. We share in all the EU duties and powers of national data protection authorities. Being Brussels-based, however, we also are influential as the special and first adviser of the Council of the European Union and the European Parliament. We're better positioned to be of help.

My third introductory remark relates to our excellent working relations with the Privacy Commissioner of Canada. In general terms, we've always had a very close and fruitful strategic partnership with Canada. We also had the occasion, just to give you an example, to submit our pleadings to the European Court of Justice concerning the Canadian PNR. We had a chance to interact with some of our colleagues in Canada so as to be fully in touch with your legal framework.

I'm very pleased to be at your disposal and to answer any questions you may have about the process and the content of revising PIPEDA. I've been intimately involved in the reform of the European data protection rules. We are here to advise legislators. We adopted many opinions. We have been in touch with the rapporteurs and shadow rapporteurs. It was a process that took almost a decade from consultation, to proposal, to very long negotiations. Now we are focusing on implementation.

My institution will be one of the members of the newly established European Data Protection Board, the new EU body that will replace the existing advisory board, the Article 29 Working Party of the European Commission. In addition, the EDPS, the European data protection supervisor, will also serve the board as secretariat. So 20 people from my staff will be delegated full-time to this initiative.

We are investing all our energies to be ready on day one, May 25 of next year. The GDPR, general data protection regulations, adopted last year and published last year on May 4 in the official journal, comes into force next year in May. Today nothing prevents a data controller from starting with real implementation, although full implementation, with enforcement, can only start at midnight on May 24 next year, when we come to convene all colleagues for the first meeting of the European Data Protection Board.

We are also putting our energies into complementary and necessary reforms. We need, notably on electronic communication privacy, the so-called e-privacy regulation, which is likely to replace the existing e-privacy directive. We have more or less the same approach as for the GDPR versus the 1995 directive. In addition, we are also expecting new rules applicable to the big galaxy of the European Union institutions and bodies subject to my supervision.

We're doing the work of a generation, and the challenge is to make sure people get to enjoy the new rights on the online world. The GDPR is going to be in place for, I predict, at least 15 years, which is more than a decade.

● (1205)

We can see that we have legislated not only for millennials, but perhaps also for the mid post-millennials who have only ever known a connected world. Therefore, the challenge is to consider the reinforced rise in the GDPR and the new rise such as those concerning privacy by design and privacy by default that can be called big data rights.

We really want to be more conversant with new technologies, to be future oriented, and to be, let's say, neutral from a technological viewpoint. You will not see any specific legislation on social networks or other specific applications, though the new rules on profilings, the right to be forgotten, and the rate of data portability are designed to be horizontal.

I see a line of continuity between current legislation and the future one in making existing and new rights and freedoms meaningful for ordinary people and more effective in practice. We will have to depart from former requirements and focus more on substantial safeguards. Therefore, there is a convergence across the world on how these rules are to be drafted and applied, and I see Canada as part of this convergence. I see a growing consensus.

We're now in a position today to focus on transfer of personal data, which is a key factor in this debate. You may be interested to know what is new in the GDPR as compared to the directive and, of course, I can only quote Daniel Therrien, the federal commissioner, to say that the GDPR contains some provisions that did not appear in the current directive and also do not appear in PIPEDA: portability, erasure, privacy by design, and privacy by default. Therefore, we have to analyze together the differences in the two statutes.

I am pleased answer any questions about the major differences between the directive and the GDPR about the process for determining PIPEDA's adequacy status under the GDPR, although neither the current directive nor the GDPR provide for any specific process, but we know what the approach could be.

I guess you will be interested to verify the criteria for determining the adequacy status, what it means after the Schrems case, digital rights versus Ireland, judgment for the European Court of Justice, what it means, and an adequate level of protection of personal data essentially equivalent to the one in the EU. Would you expect consultations with Canadian authorities, for instance, in the evaluation of the new approach in Canada, if any? What about the timelines, and more specifically, what are the long-term implications of the Schrems decision that were confirmed by the Court of Justice in coming decisions? One of them relates to the Canadian PNR.

If this is the right approach, we may focus then on specificities concerning either the retention of data or the protection of children. Many companies are interested to verify, for instance, which consent is to be re-collected once the GPR enters into force. I think we have enough food for a fruitful discussion.

I don't want to abuse your time, and I think it's much better to now go into specificities in answer to your questions or focus on more detailed issues.

● (1210)

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

Our process here is to have rounds of questions from various members from various political parties. Our first round is a seven-minute conversation, and then we'll move on from there.

Our first member of Parliament is Mr. Saini for about seven minutes, please.

Mr. Raj Saini (Kitchener Centre, Lib.): Good evening, Mr. Buttarelli, and how are you enjoying Rome? We could have come to see you.

Mr. Giovanni Buttarelli: It's not only sunny but extremely hot.

Mr. Raj Saini: Thank you very much for your opening comments.

My questions are a bit specific. I want to start off with article 25 of the GDPR, when we talk about adequacy.

Especially with the focus on CETA having recently been signed, now that you have the GDPR and you are going to judge other countries' regimes against your own, what kind of test will you apply? What will that test look like? What kind of process will it be? Will it be checklists? Just give us an idea of how you will measure other countries' privacy regulations against your own so that we have an understanding.

Mr. Giovanni Buttarelli: This is the million-euro question. Let me say first that there is no regulated process that expresses [*Inaudible—Editor*] in the GDPR. We should build on the basis of the criteria. First of all, existing adequacy decisions will remain in force up until the moment they are updated or repealed. There is a line of continuity.

Second, we have a lot of clarification in the GDPR as compared to existing direct.... For instance, the commission will now be able to adopt those adequacy decisions also for the law enforcement sector. It's much more clear that the new GDPR will allow for an adequacy determination to be made with respect to a particular territory of a third country, or even to a specific sector or industry—so partial adequacy findings.

Although the GDPR provides for a *rebus sic stantibus* approach, a periodic review of every adequacy finding, including existing decisions by the European Commission at least every four years, we're not in a hurry to put Canada on top of our decisions. You should now verify on the basis of the new, extensive list of criteria now listed in the GDPR for the assessment of that adequacy, what is needed.

My first recommendation before entering into details is to realize that chapter 5 of the GDPR is much less relevant compared to today. Today we apply the European Union legislation on data protection, mainly the two directives, to companies established in one of the European Union countries. Therefore you have to discuss to what extent a controller is established here.

As of May 25 of next year, the principle will be different. It will no longer be a mix of territoriality and establishment, but a system where we pay attention to the place where the services are delivered. The entire set of provisions in the GDPR will be fully applicable, including but not only, those on transfers to controllers offering goods and services into the EU remotely, or profiling people at a distance.

It means that if, for a company, there is a perspective to have a continuous processing of personal data, not only in a one-way direction to Canada, attention is to be paid to the full set of provisions, not only to chapter 5. Assuming that we are only considering a minor dimension, which is the one of transfer, we have to pay attention to a second important approach. The GDPR was drafted and prepared for final adoption before the Schrems case, which relates to October 6, 2015, when it was too late to change the wording.

Adequacy now is a little different. We started in the seventies with the requirements of essential equivalence. If we look to the convention 108, adopted in 1981, the system in another country should be equivalent. The directive adopted in the EU in 1995, so 14 years later, has been focusing on something lighter, what is simply adequate. Then we have criteria to verify when a country or a system or a territory is offering an adequate level of protection.

Now, because of the new legal status of the Charter of Fundamental Rights and because of the Lisbon treaty, which is de facto the European Constitution, the European Court of Justice has said that these criteria are to be read jointly, with the condition expressed by the same court in the Schrems case.

● (1215)

They read what is adequate as now being essentially the equivalent.

Mr. Raj Saini: You've also come up with the police directive, which has not been discussed. Is there a checklist or some sort of adequacy test for that also? I know that's a very important fundamental part of the privacy regulations right now in the European Union.

Mr. Giovanni Buttarelli: Yes. It's a very similar approach, and indeed, the adequacy will also relate to the law enforcement sector. This sector can be evaluated in two different areas. One is the processing of personal data by private controllers. The other is the accessing of data by police forces and by members of the judiciary. The directive is to be implemented by members states differently than the regulation, by May 6 of next year. We are now looking for a coherent approach to prevent the member states from departing from the right approach and introducing some, let's say, strange details.

● (1220)

Mr. Raj Saini: When will the police directive appear? Do you think you will get it done next year?

Mr. Giovanni Buttarelli: The police directive is in force. However, because it's a directive and not a regulation, member states have until May 6 next year—so 19 days before the full entry into force of the GDPR—to transpose it into the national system. This is because it has more implications for domestic processing of personal data by police forces.

The Chair: Thank you, Mr. Saini.

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

Mr. Matt Jeneroux (Edmonton Riverbend, CPC): Thanks for the leeway, Mr. Chair.

Mr. Buttarelli, I appreciate your joining us today. Thank you for coordinating around our schedule somewhat. As we know here in Canada, different time zones are often challenging.

I want to talk to you a little bit about our privacy commissioner. There have been ongoing discussions for a number of years now in terms of order-making powers that he has and hasn't wanted in the past.

I'm looking at your mandate, and from what I can understand, as a European data protection supervisor you have the power to advise institutions, handle complaints, and conduct inquiries.

Can you provide a bit more detail on your powers and whether they include order-making powers?

Mr. Giovanni Buttarelli: This is one of the areas where we have novelties in the EU.

First off, there are three important rulings from the European Court of Justice concerning independence of supervisory authorities. They relate to Germany, Hungary, and Austria. In these three cases, the countries have been found in breach of the existing directive and there are important recommendations to the legislators to bring forth independence, autonomy of supervisory authorities.

Secondly, the Court of Justice has said that the exercise of all existing powers in directive 95/46/EC is essential in terms of raising the independence, particularly the advisory role, the existence of a robust supervisory role. Therefore, now the regulation and the directive provide for a full list of reinforced powers, an entirely new scheme in terms of budgetary lines, requirements in terms of appointment, and relationship with government and relevant parliaments, depending on the legal system in each country.

Each DPA should be equipped with substantive powers in terms of warnings, with a view to admonish relevant comptrollers. Another novelty relates to the application of administrative fines. It is now mandatory for all member states to keep independent supervisory authorities with the duty and power to apply those fines where appropriate. The novelties are not only in terms of enforcement, but also with a view to consider all seven functions of a DPA listed by a famous Canadian professor, Colin Bennett, together with Charles Raab. They drafted the book listing seven missions of DPAs, including those concerning awareness, with a view to creating also a culture in terms of data protection.

In terms of more co-operation and more transparency, DPAs should be more selective in exercising their functions. One of the key pillars of the new regulation is accountability, which means that each private and public comptroller is requested to go beyond mere compliance, to have an internal policy to demonstrate that they comply in practice, to have an answer to every pressing need, including the allocation of resources and responsibilities. We would like to treat all comptrollers more responsibly, as adults, we might say. Therefore, DPAs should be more effective when appropriate, but also more selective, and more transparently define their priorities. They should publish a program and they should be more predictable, more accessible, and more protective.

So it's a less prescriptive approach, with more engagement, more interaction with new technology. It's also from the perspective of making new rules on accreditation, certification, seals, and privacy by design and privacy by default more effective in practice.

● (1225)

Mr. Matt Jeneroux: Okay, great.

Shifting a little to the right to be forgotten and the right to erasure, we've had a number of witnesses before us who have weighed in on this, particularly in light of what's coming through the GDPR. We're looking at what that means and whether we should put anything in prescriptively or leave it up to the Privacy Commissioner, who still has an ongoing study.

Do you mind providing the committee with your interpretation of the differences between the two, and then perhaps make a suggestion on what you see as the future of the right to be forgotten and the right to erasure within legislation?

Mr. Giovanni Buttarelli: This is a question where I risk displeasing you. Let me speak as a member of the judiciary, as I am, to say that the GDPR contains very little news on the right to be forgotten. You will not find any specific reference.

If you interview the rapporteur of the Costeja González case, he will furiously react to say that there is no wording in the judgment mentioning the right to be forgotten. He will say that it is actually a right to be delisted. He will say that there is no novelty in the ruling by the Court of Justice, and that the only novelty relates to the faculty of the data subjects involved to directly address the search engine instead of contacting other controllers.

In terms of perspectives, we attach real importance to the coming case before the Court of Justice. Once again, it's a preliminary ruling. It comes from the French council of state. Right after the Costeja González case, together with other national DPAs, we coordinated our enforcement actions, so we clarified which principles are to be defined.

Google, Bing, and other search engines have agreed on the principle. If we look at the statistics published by all of them, you will see that after the initial peak we are now in a reasonable trend. The large majority of requests by data subjects are properly considered, and where they are forwarded to the competent authorities—it could be a court or a DPA—the conclusion by those two is not different from the search engines'.

There is a convergent approach in identifying good reasons in terms of public interest not to delist the relevant information.

The area of disagreement relates to the territorial scope of application of the ruling. While DPAs consider that this should be global, and the French authority has adopted the decision to challenge it before the Court of Justice to say that we should also consider the dot.com domains, Google is of a different opinion, and this is why we are waiting for a conclusion.

The GDPR does not contain any reference to areas where the right to be forgotten is currently regulated by the civil penal code, common rules in all member states. Here I see that regardless of the GDPR, let's say it's business as usual.

● (1230)

The Chair: Okay, thank you very much.

I will now move on to Mr. Blaikie for around seven minutes please.

Mr. Daniel Blaikie (Elmwood—Transcona, NDP): Mr. Buttarelli, thank you for sharing part of your evening with us.

Coming back to the theme that Mr. Saini had started off on, I wanted to come back to the question of the adequacy provisions in the GDPR. I just wondered if you could highlight for us some of the uses or abuses of data by third parties foreseen by the GDPR that its adequacy test is meant to prevent.

Mr. Giovanni Buttarelli: The GDPR provisions on transfer of data apply to all controls in the public and the private area without any distinction. We have different criteria now for the assessment. They basically allow for it to say that it should be a global evaluation and not purely a legal one.

The criteria are the following. First of all, there is the rule of law, so we have to look to relevant legislation in force, both general and sectorial, including—this is an important specific novelty—that concerning public security, defence, national security, and criminal law. This is why we now have the case on the Canadian PNR but also professional rules, security measures, which are complied with in a third country or by an international organization. We would like to see to what extent certain rights are effective and enforceable, so we look to effective administrative and judicial redress for data subjects.

A second element relates to the existence and effective actioning of at least one independent supervisory authority. How they advise and assist with regard to the data depends on the extent to which they may co-operate with supervisory authorities in other countries, but also on the international commitments they may have as an international organization.

The commission adopted a communications package on January 11 this year to focus, as a priority for the next two years and up, the mandate of the current commission. They have declared that we'll look first to start with a new dialogue where necessary. Then we'll look at the extent of the European Union's even potential commercial relationship with that country, including the existence of a free trade agreement or ongoing negotiations. Then we will look at the extent of personal data flows from the European Union.

There is the pioneering role. This is an essential role for South America, for instance, that the first country plays in the field of privacy data protection, so it is something that could serve as a model for other countries.

Finally, there is the overall political relationship with the third country in question.

We focus on data protection but not only. There is no procedure to apply for adequacy as I said, but I can describe in detail which best practices are observed in practice.

Mr. Daniel Blaikie: If I could jump in, I'm curious to know whether you have an idea about the Comprehensive Economic and Trade Agreement that was signed recently between Canada and Europe. We've had experiences in Canada in which legislation that was passed for Canadians' public interest has been ruled out of order by international trade tribunals under the auspices of like agreements.

Is there any concern in your office that elements of the GDPR might be found to be a non-tariff trade barrier under CETA? Do you know how the authorities work and which document would take precedence in the event of a conflict?

● (1235)

Mr. Giovanni Buttarelli: With regard to the EU position, not just the one of my institution, you may look at the latest state of the union speech by President Juncker, which says we need coherence and consistency. Europe, regarding the GDPR with the directives I mentioned, would like to have one coherent single harmonized legal framework so that any trade agreement, including the one you mentioned, does not depart from the system but is fully in line.

The commission doesn't want to have substantive provisions relevant to a data protection viewpoint or to interpret existing or future trade agreements with a view to having *lex specialis* from a data protection viewpoint, although we are all aware that you may have some specific need to address certain specificities, whether a principle in terms of territoriality, or something concerning cloud computing servers, or something related to trade secrets.

In terms of general obligations for data controllers and data subjects that arise, the idea is to have everything in the GDPR and only in the GDPR.

Mr. Daniel Blaikie: Okay, and that includes not just inside Europe but outside Europe as well.

Mr. Giovanni Buttarelli: Yes.

We have published a paper to recommend, in case of future talks —an upgrade or very familiar existing provisions, including those in the GATT area—to assist the approach I've just described.

Mr. Daniel Blaikie: My final question in the time we have is, what do you see as the instrument? Would signing on to the GDPR in a similar legislative framework, then, be a condition of trade agreements with Europe going forward? What's the mechanism for enforcing that over time?

Mr. Giovanni Buttarelli: In the communication of the commission that I mentioned, they declare that on top of their priorities now, they have, for this year and early next year, Japan and South Korea. Both countries want—and this was a point discussed even at the G7 meeting in Taormina—to sign trade agreements. Europe is ready for it, but the message from Brussels was: okay, but without any provisions in terms of data protection, the two areas are to be kept separate and working in parallel; the substantive approach on data protection should only be on one side.

The Chair: Okay, good.

Thank you, Mr. Blaikie.

For our last seven-minute conversation, the floor goes to Mr. Erskine-Smith

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Great.

First, thanks very much.

I have a couple of quick questions and then want to get into some of the larger concepts you raised.

We had a number of witnesses from the business community to suggest that a right of erasure or a right to be forgotten—and I know there are different iterations of that—would be very burdensome on the business community. We had some lawyers attend before us to say that the right of erasure would be important, especially as it relates to minors. One lawyer in particular noted that for those 16 and under there should be a right of erasure.

In your experience, given your role, do you think a right to be forgotten—even a modest one for those under the age of 16—would be too burdensome for the business community?

Mr. Giovanni Buttarelli: Yes, it is.

We would like to see how things will evolve. This was a point made for a compromise approach by member states. It could be that some countries might decide differently, although, for instance, the first piece of legislation introduced by the EU with regard to EU institutions and bodies follows the line.

Age is not the main point. There are many other important details, such as the verification mode. This has to be carefully analyzed. This is one of the key points of the action plan of the Article 29 Working Party, where important guidelines are also planned. My institution is also working with other colleagues on a way to exercise data subjects' rights, with particular regard to erasure and to children.

● (1240)

Mr. Nathaniel Erskine-Smith: Another area of dispute we've had is with respect to powers. Our Privacy Commissioner, Mr. Therrien, has an ombudsman model currently. Of course there are other jurisdictions, including the U.K., that have fining powers. We're looking at potentially recommending an alternative to the ombudsman model.

In your experience, do you think giving powers such as the ability to penalize companies by way of fines would be a useful new set of powers for our commissioner?

Mr. Giovanni Buttarelli: We have not in the past been forcing third countries to copy the European Union, although an inefficient legal system is also to be dissuaded. I successfully persuaded the legislators to say that administrative fines are not to apply in a *tot capita, tot sententiae* approach, in the sense that they should necessarily, in 100% of the cases, follow any breach.

Article 83 of the GDPR says that when a fine is to be applied, because the exercise of other powers has been effective—warnings, for instance, or admonishment—then the criteria are the following. There is—

Mr. Nathaniel Erskine-Smith: If I may, with respect to the fine powers currently in the EU, you're suggesting there are certain instances where it would, perhaps, not be appropriate and that a resolution without a fine may be more appropriate.

In our circumstance, there have been situations where our commissioner has made a finding, the companies simply flout the finding and, in fact, the commissioner then has to go to court or the injured party has to bring an application to court to seek justice.

Do you think it would be appropriate to improve upon our ombudsman model by giving fine powers?

Mr. Giovanni Buttarelli: I'm not best placed to—

Mr. Nathaniel Erskine-Smith: Okay, that's fair.

Mr. Giovanni Buttarelli: Let me say that the vast majority of DPAs in EU member states are currently not equipped with the duty to apply sanctions. The near future is exactly the opposite. There is a provision in the GDPR saying that member states may, at the end, decide that the DPA brings a controller before the court. This could be the system in perhaps one or two member states. But your ombudsman approach seems to be much less effective.

Mr. Nathaniel Erskine-Smith: I only have about a minute and a half left.

We haven't heard a lot about the right to portability of data before our committee, but it strikes me as an incredibly important right, especially as we look to the Internet of things, particularly for consumer choices as customers wish to move from one company to another and take their data and their preference history with them.

Perhaps you could explain to the committee a little bit more about the right to portability, and also give us some key delineation of the right to privacy by design or privacy by default. We have that concept here in Ontario, by virtue of our former privacy commissioner, Ann Cavoukian, but it's a larger concept than only a legal concept.

Perhaps you could speak to those two concepts.

Mr. Giovanni Buttarelli: Privacy by design and privacy by default are no longer recommendations. They are now legal grounds and clear obligations for every controller. It means that systems are to be designed with a user-friendly and less invasive approach. There are obligations addressed to controllers, but there is a system to make designers, producers, and developers engaged in practice.

Privacy by default means that in case of plurality of different settings, the starting one should be the one closer to the data subject's rights.

● (1245)

Mr. Nathaniel Erskine-Smith: Portability is a new concept in the GDPR as well.

Mr. Giovanni Buttarelli: Portability is less new than originally expected. It means that if I move to another provider, there is no detrimental approach in practice. The Article 29 Working Party has adopted guidelines recently. They appear on one point to be controversial with regard to the interpretation of article 25 of the GDPR, because the GDPR says that portability only relates to data provided by the business. We know and experience shows that many other data are on the device or are accessible to the provider, to the controller, although they are not, formally speaking communicated by the data subject. This is an area of limbo where the Article 29 Working Party has decided to consider this area as part of the portability.

Mr. Nathaniel Erskine-Smith: Thanks very much.

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

We'll now move to the round of questions where the conversation should be around five minutes. We'll go to you, Mr. Kelly.

Mr. Pat Kelly (Calgary Rocky Ridge, CPC): Thank you for attending our meeting.

Perhaps this will take us in a similar vein. In your opening comments, you mentioned the four areas that our commissioner had identified as being areas where PIPEDA, our existing law, may be deficient. You identified our commissioner's concern over the right of erasure, right of privacy by default, and privacy of design, but what was the fourth one? The fourth one was portability. Is that the other area of concern around PIPEDA identified by our commissioner?

Mr. Giovanni Buttarelli: Yes, it is an area of major concern, but I would like to take this opportunity to draw your attention to a recent position by the Article 29 Working Party, according to which our opinion for the assessment by the commissioner will be based on more than those principles.

We would like to draw attention first to the basic rules for the data protection purpose limitation principle, data quality and proportionality, transparency—to reach a standard on how data subjects are effectively informed, security—the security of a database's data and systems, the exercise of rights of access in opposition—not only portability, and something that is particularly highlighted in the GDPR, which is onward transfer. There are a few other additional points on sensitive data, direct marketing, and automated individual decisions, but I would like to recommend that you not focus too much on the novelties in the GDPR, such as design, default, and portability.

Of course, they will contribute to the review of the current assessment by the EU, but we have time. The European Commission has been requested to submit in three years from now—by spring of 2020—a record of the first round of implementation of the GDPR and of the approach to be taken with regard to existing adequacy findings.

If I go back to the one adopted for Canada, I have to go back to an opinion adopted by the Article 29 Working Party in 1998, to the Working Party 12 document. Default, design, and portability were not considered in that document, but we started at that time to consider the conditions on surveillance, which are now much more relevant.

We would encourage that there be a global approach and that you not have a sort of point-to-point replication of every single rule, so the adequacy test is an important message I would like to share with you. It relates to the substance of all privacy rights, globally speaking, in terms of implementation, enforceability, supervision—

● (1250)

Mr. Pat Kelly: If I may just jump in again, I want to ensure the clarity of what I heard you say. Your suggestion to us is not to fixate on the areas that our commissioner has identified, where our law may not be compliant.

Mr. Giovanni Buttarelli: No. I don't want to displease my—

Mr. Pat Kelly: I thought that's what you said.

Mr. Giovanni Buttarelli: I would welcome a similar approach on those areas, of course, but I'm saying that the evaluation by the EU side builds on a different approach, where they are part of the global analysis, but we look to many other things that are—in a few cases—more essential.

Being the one taking a decision by considering the EU approach, I would say that, for instance, the restrictions, exceptions, and derogations for law enforcement are more important than design and default. One member of my team will be part of the joint review of the privacy shield. Of course, we will consider privacy by default, privacy by design, and data portability as well, but law enforcement is at the top of our concerns. Globally speaking, it counts more.

This is what I want to say, then I can simply welcome that you harmonize as much as possible with this approach.

If I had a couple of minutes with you or one of your colleagues, I would like to share with you the latest update on what other countries are doing around the world, what's going on in 35 countries in addition to the 109 already equipped with a new generation of data protection rules.

Mr. Pat Kelly: I presume I'm out of time.

The Chair: You are making a very good presumption, Mr. Kelly. We thank you very much.

We now go to Mr. Ehsassi, please.

Mr. Ali Ehsassi (Willowdale, Lib.): Thank you, Mr. Chair.

Thank you, Mr. Buttarelli, for taking the time to be with us today.

Now, one of the issues that has yet to come up today is the issue of algorithmic decision-making.

Would you kindly explain to us what the provisions of the GDPR are with respect to that issue, and how much of a concern is it?

Mr. Giovanni Buttarelli: Are you relating to the adequacy finding?

Mr. Ali Ehsassi: Yes, algorithmic decision-making.

Mr. Giovanni Buttarelli: Okay.

Here we don't have too much novelty. The GDPR does not mention the artificial intelligence, but there is a provision which is in continuity with the current directive. It provides for this article 22, which provides for a line of continuity. The data subject will continuing having a right not to be subject to a decision based solely on automatic processes, including but not totally providing...when the decision is likely to produce legal effects concerning him or her, or with a view to significantly affecting him or her. There are some exceptions in the case of the necessity relating to a contract between the data subject and the data controller, explicit consent by the data subjects. What is needed is that in case of a derogation, some suitable measures be listed by the legislator to safeguard the data subjects and rights.

We see a line of continuity in having a human evaluation as part of the process. We recognize the ability of the controller to build largely on an automated individual decision-making process. However, the question is on what is at the end, how the decision is placed, and to which extent there is a human contribution. This is a specific right. The wording is “shall”, and therefore now the question is to what extent we may build on safeguards.

Let me say that with regard to artificial intelligence, we have posted on our website an important background document for the last conference of all data protection and privacy and information commissioners from all around the world—a meeting in Marrakech—with a view to going beyond the GDPR being part of the artificial intelligence debate by the data protection people, and a list of questions for a more synchronized approach by DPS. In case you fail to identify the web page, we can provide you with the relevant link.

● (1255)

Mr. Ali Ehsassi: Thank you.

In preparing for your appearance here, I had a chance to check out your website, and I noticed that you do a lot of outreach and educational workshops.

Could you tell us how important these initiatives have been in terms of elevating people's understanding of digital privacy rights and whether they're focused more on businesses or on consumers?

Mr. Giovanni Buttarelli: They are. Let me speak about my background.

I spent 12 years in a national data collection authority as a secretary general in my country of origin. I can say that awareness and data protection in privacy culture is more than essential. You may be the best one in terms of legal analysis, but if you fail in making people aware of their rights, if you fail in being engaged with the controllers in the process, you are not on the right track.

One of the novelties of the GDPR relates to the adoption of guidelines. We've replaced 25 out of 47 legal provisions, so the GDPR is speaking about new legislation, implementing delegated acts by the European Commission with flexible guidance from controllers. They are to be adopted on the basis of an inclusive process, in active consultation with data controllers. The decision-making process by the European Data Protection Board will be very different from the one currently followed by 29 working parties.

Recently, I also started an exercise to make more accessible data protection. It is extremely complicated. It's not simple from a legal viewpoint. It's horizontal. It relates to many sectors. You should make this principle digestible in practice. There should be not only warnings, but also, on the basis of your experience, proactive exercises to explain how they may be applied in practice.

By May of next year, together with the commission, we will take part in a European Union campaign to make people aware of the new data subject's rights, but also to speak more directly to data controllers and processors to make data protection digital. I would like to focus more on making this principle effective in practice, much less “Pater Noster, Ave, and Gloria,” and more substantive principles in practice.

The Chair: Thank you very much.

I'll go back to Mr. Kelly, please.

Mr. Pat Kelly: Thank you.

To perhaps return to my earlier question, what I would like to do is identify, as specifically as you're able to, areas of PIPEDA. That's what we're studying now. I understand that our Privacy Act and perhaps other laws are also areas of concern for compliance or compatibility with the GDPR, but it's PIPEDA that we're studying.

Please be as specific as you can. Are there shortcomings you've identified that you would suggest we apply ourselves to?

● (1300)

Mr. Giovanni Buttarelli: I'm not an expert on PIPEDA, but I understand that it applies only to private sector organizations. Initially, the act applies only to organizations that are regulated at the federal level, but also to the disclosure of personal information by certain organizations. Finally, I understand that the act also applies to all businesses in the territories as they are deemed to be federal work.

One question relates to this. What if a province passes privacy legislation, even if it is substantially similar? Second, what about government organizations? Would you like to work in a perspective to simply follow the line and remain in the specific context of the private sector organizations, or is there any interest to make the adequacy finding larger by considering other areas as well?

I think we will pay attention to onward transfers more than in the past, to the specific statutes for sensitive data, and pay a lot of attention to the e-privacy regulation to be applied soon. It enters into force by May 25 next year as well.

Some regulation is likely to specify and complement existing provisions in the general regulations in the online world, so you will have substantive provisions, for instance, on cookies, on the protection of confidentiality, and on search engines, particularly with regard to consent.

I had a chance to discuss with your federal commissioner consent in the GDPR as compared to consent in the current directive. One of the major concerns for controllers is whether to collect once again a new consent by the data subject. The answer is that it depends on whether you respect the essence of the future provisions. Did you really collect freely given, specific, and informed indication of the data subject's wishes? Did you provide for an explicit consent to process sensitive data? Could you say that for data other than sensitive data consent is unambiguous? Therefore, you have to discuss which consent is unambiguous in the online world.

This is extremely important, because in case you cannot work on reliable consent anymore, you have to verify which other legal ground is to be...collected, with particular regard to the balance of interest and to legitimate interest.

There are two opinions by the current Article 29 Working Party, plus another one on purpose limitation. I think they may be considered in terms of priority now, with a view to see to what extent certain protections or safeguards for the data subject are effective in practice.

Perhaps it would also be relevant to share my views with you on profiling and mass information—

● (1305)

Mr. Pat Kelly: I don't mean to cut you off, but I'm getting the look from the Chair and I think my time is up.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Perhaps we can get to that in future questions.

Mr. Long.

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

Mr. Giovanni Buttarelli, we want to thank you very much for taking your time this evening to help educate us. There's no question that we can learn a lot from you.

Mr. Giovanni Buttarelli: That's reciprocity. I am learning a lot also from you.

Mr. Wayne Long: That's good. It's good that it goes both ways.

I want to speak to you about the GDPR with respect to children—children's rights and the protection of children. We've had lots of witnesses come before us over the last several months to talk to us about the lack of provisions in PIPEDA to protect children. We look at the United States with the COPPA and the provisions that it has.

I wanted to learn from you and understand the GDPR with respect to children's rights, consent, age limits, that kind of thing. If you could give us a bit of information from what you see, it would be greatly appreciated.

Mr. Giovanni Buttarelli: We've said in more than one “EDPS Opinion” that this is an area where we are partly disappointed. The GDPR is not in the form of my dreams, but it's the best we can achieve today. If we started today with a new process, I doubt we could get something better.

On children, the legislator has been less ambitious than expected. We have just one article in the GDPR. We are expecting a new provision with regard to online services in the e-privacy directive.

First of all, there is a fragmented approach in the EU with regard to the age of maturity, and the compromise was that the processing of personal data of a child shall be lawful where the child is at least 16 years old.

Mr. Wayne Long: Should it be tiered? For example, 12-14-year-olds would require parental consent; maybe kids of 14 to 16 would require something a little less. Do you just go with the age of 16?

Mr. Giovanni Buttarelli: The approach is that the child be at least 16 years old. Below the age of 16, the processing is lawful only if and to the extent that consent is given or authorized by the responsible parent of the child.

The compromise was in the final sentence of paragraph 1 of article 8, which said that member states may authorize a lower age, provided that the lower age is not below 13 years.

Mr. Wayne Long: Okay.

Mr. Giovanni Buttarelli: The question is, how are you sure there's control to make a reasonable effort to verify that consent is given or authorized by the holder of parental responsibility? Also, how can you take into consideration available technologies? Here we suffer from the relationship between data collection and the rest of the legal system. Within the member states, apart from differences in considering whether a child is an adult or not, we have divergent approaches to contract law. This is why the GDPR says that the paragraph I mentioned shall not affect the contract law of those member states concerning the validity or the effect of a contract in relation to a child. So in the workplace you may have a different approach to the validity of the relevant contract for employment and the rules on data protection. This is part of our contradictions.

● (1310)

Mr. Wayne Long: I was surprised, actually, when you said you were disappointed with the provisions that have been made for children. Is that somewhat unanimous across the EU? What happened that makes you express that disappointment? Where did it go wrong?

Mr. Giovanni Buttarelli: We said that in two formal “Opinions”, so I'm not now reinventing the wheel. We are here because of the difficulties in regulating, from a data protection viewpoint, an issue that is much bigger, and to speed up the process, perhaps. The approach of the legislator was to count more on the guidance by data protection authorities. So, I'm afraid we will continue working with a flexible approach. Perhaps it will be up to data collection authorities to identify reliable methods that stop content from being freely given, and to identify the relevant safeguards and suitable methods for age and verification.

Mr. Wayne Long: Thank you very much.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thanks very much.

Our final round goes to Mr. Blaikie for three minutes.

Mr. Daniel Blaikie: I am just seeking information about the GDPR with regard to algorithmic decision-making and the extent to which, if at all, the GDPR speaks about transparency in cases where decision-making processes are handed off to algorithms. Does the GDPR contain or foresee any rights for people to have a sense of how those algorithms work and how those decisions are made once it goes inside the black box, so to speak?

Mr. Giovanni Buttarelli: There are two approaches in the GDPR. The first one, which I already mentioned, relates to the right not to be subject to certain decisions unless there are safeguards. The second approach relates to transparency, and here we have a lot of novelties. This is an area where data options....will be equipped with more transparent, intelligible, concise, and easily accessible information and forms. There is a clear need to use plain language. Here we have another area where children are considered in terms of transparency —I forgot to mention this earlier.

These articles on transparency do not relate specifically to processing modalities, but by reading them in a global approach, you will understand that in the case of certain processing modalities that you mentioned, transparency should be reinforced and be effective in practice. This is largely for guidance by DP. There are some provisions concerning machine-readable icons and standardized icons, but I doubt they relate to the case you mentioned.

Mr. Daniel Blaikie: Thank you very much.

The Chair: Thank you, Mr. Blaikie.

Now we just have a few minutes of open time for members who haven't had a chance yet.

Monsieur Dubourg, if you would like to ask your questions, the floor is yours, sir.

Mr. Emmanuel Dubourg (Bourassa, Lib.): Thank you, Mr. Chair.

Buon pomeriggio, mister Buttarelli.

[*Translation*]

I heard you right at the start. I know that you speak French. I just wanted to ask you a question or two about the general regulations on data protection.

Is that okay with you? Can I continue?

● (1315)

[*English*]

Mr. Giovanni Buttarelli: Yes, please.

[*Translation*]

Mr. Emmanuel Dubourg: Okay.

Thank you.

I would like to ask you some questions about the powers. Here, as you are well aware—through your discussions with Mr. Therrien, among others—academia and the general public agree with giving more powers to the Privacy Commissioner, whereas businesses talk more about collaboration.

We know that, over there, you have those powers, even the power to impose fines. We saw that, in Italy, your native country, WhatsApp was fined $4.5 million.

Tell us how those powers are a deterrent in a situation of this kind. Or do you think that we should keep collaborating with companies instead of imposing penalties?

[*English*]

Mr. Giovanni Buttarelli: The two approaches are not opposite. Accountability is the right approach we request, and it doesn't mean that you should simply respect the law. We are asking now more, and let me speak for a second as a member of the judiciary, as I am.

Being in front of a court case where we may discuss to what extent the controller has been proactive, I would consider in a better way the case where he made mistakes but has been very operational. The question is not to have an emphasis on every kind of even minor mistake. I would like to see the big picture, but I would welcome the approach they recommended to you. We need a dissuasive approach.

Let me say that we are now bombarded from everywhere in the world, and if I am in Silicon Valley or in Africa or in South America, the first question is the same everywhere. What about fines?

We know that they are very serious.

I would now advise the legislators to clarify the interlink between administrative fines and penal law. This is another area. We have to clarify the so-called *non bis in idem* principle, so are we going to apply fines in all countries with regard to the same controller? In adopting the criteria to decide if a fine is to be applied, we have to consider the remedies considered by the subject, which is then he has been fair and dynamic in approaching a security breach, informing people after a violation, reducing the kinds of damages. All in all, data protection costs a lot, and every effort is to be considered when taking a decision.

So this is why I talk and I would defend this approach, a system where fines are to be applied where necessary, but not necessarily in every case. I'm not a lover of the Spanish approach. We call it *tot capita, tot sententiae*. If there is even a minor breach, there is no appeal, and unavoidably, the sanction is to be applied.

Let's look to the picture because otherwise we risk having fines considered as a budget line, and this leads also to an amount of fines because we need to graduate, we need to consider the position of small and medium enterprises, and we need to carefully consider the criteria in terms of the seriousness of the breach, the implications of a larger-scale approach. We cannot treat every breach in a single way. So we need a very dynamic approach where we use the carrot and the stick.

● (1320)

[*Translation*]

Mr. Emmanuel Dubourg: I would like to ask you one final question.

You talked about the big picture. However, what has to be done to assess the situation in terms of imposing those penalties? For example, do we have to start by establishing negligence, or do we go extremes and prove that something was illegal? How do we resolve that situation?

[*English*]

Mr. Giovanni Buttarelli: If you'll give me 20 seconds to open article 83, I think this is one of the lucky provisions where we have no excuse because we have all the opportunities to consider. I'm quoting now the relevant paragraphs:

> (a) the nature, gravity and duration of the infringement taking into account the natural scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;
>
> (b) the intentional or negligent character of the infringement;
>
> (c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;
>
> (d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
>
> (e) any relevant previous infringements by the controller or processor;

Another important point relates to the degree of co-operation with the supervisory authority to mitigate the possible nefarious effect. How many data subjects have been involved? What about the categories of personal data or data subjects involved? How has a data controller been proactive in approaching the supervisory authority to confess the breach? How do they notify them of the infringement? Are they following codes of conduct? Do they consider other circumstances, for instance financial benefits they got from the infringement?

All these criteria can be applied to four categories of breaches. We cannot treat every breach in a single way. In addition to the criteria I've just mentioned, we should also consider the seriousness of different violations so we are reasonable, we are credible. Otherwise, people would not understand.

We need to avoid a system whereby the fines are simply a budget line item for a big corporation. We need to increase the amount of fines where and when dispensable, but in the end we need to consider the amount of money and the energy that the controller, in the process, has spent on the case.

[*Translation*]

Mr. Emmanuel Dubourg: *Grazie tanto, mister Buttarelli.*

[*English*]

Mr. Giovanni Buttarelli: Oh. Your Italian is better than my French.

[*Translation*]

Mr. Emmanuel Dubourg: *No, no, è una parola al giorno.*

[*English*]

The Chair: Thank you very much, colleagues.

That pretty much exhausts the questions we have for you, Mr. Buttarelli. We want to extend our sincere appreciation for your making the time and effort to discuss this with us. As a committee we want to make sure that we get our recommendations to the government right when it comes to changing our laws here and making sure that we comply with any agreements that we need to honour as well. Your help has been indispensable. We thank you very much for your time. We trust that you'll remain available should we have any further questions.

Mr. Giovanni Buttarelli: Yes, we will. As I said, I'm very honoured. Tomorrow we'll appear before the Senate of this country. I hope to have the same kind of qualified audience as I noted today.

Needless to say, my office and I remain available for any specification in this case to provide accompanying documents and to satisfy any kind of curiosity as much as possible.

Thank you very much for your attention. Let me stress the high level of awareness and competence. I have long-term experience with politicians. This is not the case, so *Chapeau!*

The Chair: You're very kind. We appreciate that feedback, and we thank you again for your time. Hopefully, we'll keep our channels of communication open as we move forward.

● (1325)

Mr. Giovanni Buttarelli: Thank you. Have a good day.

The Chair: You as well.

Colleagues, we're going to suspend the meeting for a few minutes. There are some in camera items that we need to discuss with regard to some committee business.

For those people in the room who can be here, please stay; for those who can't, please exit as quickly as possible. Thank you.

[*Proceedings continue in camera*]