HOUSE OF LORDS

Revised transcript of evidence taken before

The Select Committee on the European Union

Internal Market Sub-Committee

Inquiry on

ONLINE PLATFORMS AND THE EU DIGITAL SINGLE MARKET

Evidence Session No. 6 *Heard in Public* *Questions 52 - 60*

MONDAY 9 NOVEMBER 2015

1.30 pm

Witness: Giovanni Buttarelli

USE OF THE TRANSCRIPT

This is a corrected transcript of evidence taken in public and webcast on www.parliamentlive.tv.

Members present

Lord Whitty (Chairman)
Lord Aberdare
Baroness Donaghy
Lord Freeman
Lord Green of Hurstpierpoint
Lord Mawson

_____

Examination of Witness

Giovanni Buttarelli, European Data Protection Supervisor (EDPS)

Q52 The Chairman: Welcome. We are very pleased that you can find the time to see us. We are embarking on an inquiry into platforms as part of the digital single market—we were intrigued that the Commission regarded this as a particularly important area—and the various dimensions of it, from competition through to data protection and so on. Could you kick off by telling us what your role is in terms of the EDPS, how it works and its relationship with the Commission and the industry, and whether certain types of platform processing of personal data, which is obviously highly intensive, are a problem or a benefit? Do you think there are individual platforms on which we should perhaps focus that either create problems or deal with data in an exemplary manner?

Giovanni Buttarelli: My Lord Chairman, thank you very much for the opportunity you have given me to make a contribution to such a distinguished group of people. I am very honoured to have this chance.

I represent an independent institution, one of the smallest entities in the EU bubble, although we are becoming more influential—perhaps we already are. In addition to the supervisory role we exercise over 65 small, medium and large institutions and bodies, offices and agencies located in Brussels and in each country, we exercise our advisory role on every kind of soft and hard legislation, from communications to strategic papers and primary and secondary law at different stages, in co-operation with the three main institutions involved: the Council, the Commission and the Parliament. That is what we do, formally and informally, before documents are adopted on the basis of memoranda of understanding, and formally in public opinions and statements that we regularly publish on our website. In addition, we take part in hearings before the corresponding committees, particularly the

legal committees of the European Parliament. Finally, we exercise many roles in co-operation with national data protection authorities such as the ICO[1], not only at European level but also in terms of global partnerships. We are part of GPEN[2], which includes not only data protection and privacy commissions but other entities around the world with enforcement powers in this area. We are part of the International Conference of Privacy and Data Protection Commissioners. In addition, I speak from 23 years of largely full-time experience in this area.

I am still a member of the judiciary, detached to EU institutions. I have had the privilege to be part of different generations of data protection rules. On the basis of that experience, earlier this year, 88 days after my appointment, I adopted a strategic document with a five-year mandate to be not only accountable and transparent but predictable, focusing on what I called the need for a new deal on data protection, to open an entirely new chapter in this area, where we focus much more on effective safeguards and refrain from insisting on useless bureaucratic requirements.

We would like to discuss with you today, particularly with regard to online platforms, how we see a window of opportunity to make existing and new principles more effective in practice, to identify a way of not slowing down innovation, and to look at how technologies will evolve and consumer and data protection law can better interact, and to what extent reflections on ethics may be relevant—I will come back to that point.

The Chairman: Do you consider that there are certain types of platform that present problems and others we would wish to emulate, or do you not subdivide the area? There are very different sorts of platforms, as we have found, and they are in very different market positions.

Giovanni Buttarelli: There is no need to remind you how in the recent document by DG Connect the European Commission defines online platforms; it provides typical examples of different platforms, from search engines to online marketplaces, from video-sharing platforms to social networks.

As an independent institution in charge of data protection, identifying the experiences and difficulties encountered by users and businesses when they access or provide information, or shop and sell across borders in the EU, is not my primary responsibility. The definition of

[1] Information Commissioner's Office
[2] Global Privacy Enforcement Network

online platforms, and the fact that, for instance, internet access providers may fall outside the scope of the digital single market strategy, cannot be used to escape their responsibilities. Therefore, at a later stage we contributed to the digital single market document by focusing on what we considered was key—the coming data protection reform, where the definition of platforms does not play a role at this stage. Instead, there is a horizontal approach and we focus essentially on European soil. Emphasis on the kind of platforms is postponed to another stage, when we review the e-privacy Directive[3]—I can come back to this point—since we are currently focusing more on standard telecom providers and electronic communication services. Independent regulators today are suffering a lot in applying the principles of the e-privacy Directive to the rest of the platforms. We already engage in discussions with the European Commission, because as you know, review of the e-privacy Directive is considered one of the priorities of the Commission, after the adoption of the GDPR[4]. The GDPR is likely to be passed, in terms of political agreement, by the end of the year, or at the latest by Data Protection Day at the end of January. On the basis of a consultation next year, we expect to identify the right place for a future piece of legislation to replace the e-privacy Directive, which in my view should be in the same Regulation as the General Data Protection Regulation and not in a separate Directive.

The Chairman: The form of the Regulation will be universal, in the sense that it will not be specified in terms of type of organisation. All platforms would be covered, as well as more traditional forms of industry and third parties using the data that major platforms have available.

Giovanni Buttarelli: Correct. The idea is to harmonise further the existing rules and refrain from having specific sector-related provisions, unless it is fully justified, as is the case for some providers, but that will be postponed to another stage. The GDPR will contain only a few chapters concerning specific sectors where increased harmonisation today will be more difficult: health, scientific research, media and historical archives. Perhaps some of the platforms you are discussing can be considered with an increased margin of manoeuvre by Member States within the chapter on media. The rest will be horizontal. The GDPR will be applicable to everybody in the world offering goods and services to individuals—not

[3] Directive 2002/58/EC
[4] General Data Protection Regulation

necessarily residents or citizens of the EU—or monitoring their activities and behaviour, regardless of the location of the servers and location of establishment - the place where decisions are taken.

In cases where the main decisions on the purposes to be achieved and the main activities are outside the EU, the so-called data controller should appoint a representative acting on behalf of that controller. This has an impact worldwide, as attested to by two missions I carried out this year to the United States. There is a lot of concern outside the EU about an alleged dictatorial approach in the European viewpoint. We are accused by some players in the world of taking a protectionist approach yet, to be frank, 109 countries are now looking at data protection. They are modernising their rules or passing new data protection Acts. From the numerical point of view Europe is currently in the minority, but Europe has a big chance to lead by example, since what we are introducing is at the top of analysis around the world. Even though 18 out of 20 of the big data players are established outside the EU—I am speaking about the top search engines, such as Google, Yahoo, Amazon, Facebook, Microsoft and other well-known giants—their activities will be entirely subject to our provisions. Why? Because they process what we call personal data.

It would be interesting to share with you current trends in the debate on the GDPR—how the provisions could be scalable, focusing on pseudonomised information and when information starts to be anonymous, or, more specifically, when individuals can be re-identified using reasonable means. To what extent are we entitled to identify different tracks, depending on the purpose, and lighter regimes when the data controller has no intention of identifying an individual? That is a challenge I see around the various platforms.

Some data controllers or data processors, particularly intermediaries, are not interested in identifying individuals by name. They are pushing for a lighter regime, saying, “We accept the European viewpoint that these are personal data concerning identifiable individuals, but because of our commitment not to introduce adverse effects on them we would like to keep a lighter regime”. That is the basic expectation from this part of the world.

Q53 Baroness Donaghy: We are told that in practice these platforms harvest as much data as they can because that is the currency on which they rely for their income, and that we as consumers are slightly inconsistent, because we are fearful for our privacy but, on the other hand, rather careless in communicating data to companies we sign up for. How effective do you think the current Regulation has been in generating the enhancement of privacy?

Giovanni Buttarelli: Focusing first on current reality, very little use is made of privacy policy as a competitive advantage, because of the business model but also because of excessive emphasis on the formalities. Many end users, therefore, have difficulty in investing the time to evaluate a privacy policy, and there are difficulties in introducing changes and moving to a more buyer-friendly platform. For the time being, notwithstanding the achievements, we do not see privacy use as a barometer of product quality. As a consequence, businesses that are not privacy-compliant may easily compete more aggressively by using personal data.

The takeaway from my Silicon Valley mission in September is twofold. First, they are scared about potential changes coming from the reform. The reform is likely to be published in the *Official Journal* by late spring next year, and after a transitional period of two years it is likely to enter into force by 1 July 2018, but its implementation will require a lot of time since the emphasis will be on accountability—an essential point to discuss with you.

In answer to your first question, we expect to change from a basic system articulated on a to-do list, where I check what I should do in terms of privacy—as often as not, it is a choice—and I will be asked as data controller to do much more: to translate into practice existing principles, to allocate responsibilities, to better define roles and to document and demonstrate that I am proactive on the data protection policy. In return, the data protection authorities will have to be more effective and selective as regulators.

The two takeaways from my mission are, first, as I said, that they are scared about the potential changes and, secondly, that they continue to believe that we will fail and that we will proudly insist on the preservation of our fundamental rights. They do not care about Article 16 of the Treaty or about the Charter[5]; they say that the business model will prevail. As far as I know, a message has not been passed to designers and developers—those who are planning the future we will inhabit until 2025—that "privacy by design" and "privacy by default" are not simply recommendations but legal requirements. Therefore, they are postponing implementation to another stage. They still believe, as was the case in 1995, that there is a space for last-minute changes to water down the existing safeguards.

We are not focusing only on data protection law. We launched last year, with a preliminary opinion and a couple of workshops, a wider debate, together with the competent authorities, on competition and consumer law. We think that some of the barriers you are considering around online platforms are also relevant to us. I can give you six examples

[5] Charter Fundamental of Rights

where we are deeply concerned today: any time there is unjustified or non-transparent profiling by some of the intermediaries; any time there is unlawful discrimination based on residence or nationality; and any time there is unlawful use for incompatible purposes. Many of the activities described in the digital single market document are based on covert monitoring or unlawful access to traffic data—peer-to-peer is an example that could be used—not to mention the protection of minors online. Other barriers can be addressed mainly by the competition authorities—for instance, the abuse of a dominant position—or by consumer law authorities, as is the case in the US by the Federal Trade Commission in cases of unfair terms and conditions.

It is time for us to work less in silos and to understand better what we should do. Let me give an example as a member of the judiciary. Many court cases based on consumer law start from the assumption that you can easily apply, for instance, provisions on e-commerce, but then they ignore complainants, even consumer associations. A caveat appears at the end in an obscure corner: "This is without prejudice to data protection provisions". It is quite normal that by offering goods and services you also process personal data. Any time you have a concern about data protection and you point to the rules, they are entirely different in terms of the jurisdiction and the substantive provisions to be respected, and court cases have to be reconsidered in an entirely different way. In my experience, there is a lack of sufficient interaction and effort, which is why we are working a lot on that aspect.

Q54 Lord Aberdare: Can I ask you about transparency? One of the areas of concern among consumers and, I suppose, those who represent them is transparency about what data are being collected and how they are being used. That is the price you pay; the services look free, but you are paying by handing over your data. Do you believe from a data protection point of view that something could or should be done to enhance transparency and ensure that consumers are more aware of what data they are handing over, and how it is being used?

Giovanni Buttarelli: Thank you for that question. This is an area where I see big opportunities for success. In exchange for a reduced private sphere, we have introduced in the EU the new fundamental right to the protection of personal data, which is separate from privacy, as you know. It means that the way in which others process information relating to me—who is doing what for which purposes and where and when—is part of a fundamental right, regardless of the impact on my private sphere. Therefore, transparency is more than

key. Today, we suffer from bureaucratic notices based on legalese. One of the most successful innovations in the reform is to force controllers to use shorter, plain language to communicate; to use dynamic technologies and invest their energy in privacy by design; and even in terms of settings, to allow the individual to go for a more invasive solution—imagine the internet of things—but based on proper information. It does not mean that you should have all the relevant information in one shot, so references to pop-up windows and need-to-know boxes with a reminder about privacy policy pages based on different languages can also be used. In a nutshell, it is user control, which means that I should be able to understand more easily what use is made of my information. It is also that I have the right to object, because if in the end information simply means take it or leave it, that makes no sense.

Lord Aberdare: You raised the very important point earlier that when data become anonymised lighter Regulations and controls may be appropriate. Is there a clear definition of when they become anonymous? We had an issue in the UK, as you may know, with the idea of using large quantities of patient data in an anonymised form to provide enormously valuable input to health research and so forth. Because it was not very well sold to us it caused a huge reaction from people who thought their data might be at risk. Clearly, there was a communication problem, but it raises the issue: when are data reliably anonymous in a way people will trust so that they say, "I do not want you to do this with my personal data, but if you convince me that it is not traceable to me I am happy for it to be shared"?

Giovanni Buttarelli: I will answer with a two-minute anecdote that relates to 1981. Professor Jon Bing, a distinguished member of the Norwegian academy, wanted to demonstrate how easy it was to re-identify people. He got funds to perform his research in a small community of 26,000 people in Norway. The exercise was on data collected from a regional census. He demonstrated that by building on truly anonymised information he could properly re-identify at that time—30 years ago, perhaps more—86per cent of the people. Can you imagine that situation today with the new technologies? That is the anecdote. The provocative conclusion is that the notion of the data subject or the notion of personal data has already disappeared. I cannot say that formally in public, but technologies will continue to improve to allow data controllers to more easily to identify individuals. This is why the European Union is likely to keep the current definition of personal data and include an additional reference to targeting and, more specifically, a case where the individual is singled

out. We do not care about his identity. What is important is that in the universe of information you can easily aggregate information concerning an IP address because of location, online searches and the use of social networks, although you are not interested in identifying the individual; you are not offering personalised services, as was the case with anti-spam legislation years ago.

In the big data trend, the business will be in amassing information from the use of aggregate data. As was said, the winner will be the one with much more information to create more and more interrelations. Of course, it does not mean that data brokers offering lists of profiled people are disappearing, but in principle the business will be in doing something else.

Your question related to what we do about it. My manifesto on data protection is that big data should imply big data protection, but it would also be a driver for benefits in terms of prosperity and well-being. The data protection community should identify the right balance. I would be the first to allow data controllers to do that in a completely transparent process where we understand who is using the data. Even the notion of a controller will disappear now that we have different players. They sell information; there are intermediaries, but one day, because of big data, the information will be much more concentrated in a few hands. Even the distinction we find in the document from the Commission is likely to have much less relevance, because the information will be increasingly concentrated in the hands of a few and the business will be in processing an unbelievable amount of information with an entirely new generation of software in a way that is not possible today. We have to consider what would be beneficial for health, scientific research, urban planning and even for security. Big data is a challenge for data protection, but it is not a good reason for departing from our principles.

To come back to my preliminary statement, what is needed is innovative thinking. I cannot say that all data protection regulators are future-oriented enough to be easily on board, but my mission is exactly to encourage them to have rules that last for at least 20 years. Today, we are discussing the 1995 provisions. They were successful in first-round harmonisation, although 20 years later the way Member States are implementing those principles is no longer sustainable. Imagine these rules coming into force in 2018 with a few delegated implementing Acts and guidance from data protection authorities. It means that the full package will be ready, even for the digital single market, by 2020, and no one will start

talking about potential changes, apart from the e-privacy Directive, before 2025. When a change is discussed for years it requires time for implementation, so what we are discussing today, and what we would like to have under the Christmas tree, will last for at least 20 years, which is more than a century[6]. That is the challenge. Some colleagues are not entirely aware of what technological neutrality and net neutrality mean. They want to fix everything at the level of primary law and they do not care about guidance from regulators. It is not that easy.

Q55 Lord Green of Hurstpierpoint: The fundamental problem we have been wrestling with, and which lies behind Lord Aberdare's question, is that the consumer gets something for free in return for parting with his or her data. That may not be a cost, but it is certainly an opportunity cost in terms of value, because those data have a value from which the consumer will not benefit. There are various possible approaches, one of which is to make what is happening more transparent so the consumer understands what value they are giving up in return for this free service. Another one, if you look at parallels in other industries where a free service is provided, or something is provided at low cost and other things are packaged on top of it—for example, famously Microsoft but also famously the banking industry—is to force an unbundling where the consumer may pay for the basic internet platform service but gets value for the data he or she parts with. Furthermore, you could make that more portable so they can sell their data to another internet platform instead of to the particular one whose services they are using in return for a cost. Is that completely unrealistic, or is it a way forward in terms of opening up the market and simultaneously making more transparent to the consumer what is going on?

Giovanni Buttarelli: As you can see from the beautiful app we posted on the AppStore, we commented provision by provision on the GDPR. It is an app named EDPS, which you can download free of charge on smartphones and tablets and you will find six pages going through the text provision by provision. I am advertising the app, because if you go to Articles 17 and 18 of the proposed GDPR you will see how difficult it is to invest energy in the so-called right to portability in a way that makes sense. The right to portability was included by the Commission. We support the idea, but we also see the difficulty in making that right realistic.

[6] The witness clarified this mean in terms of technological development.

Regarding free-of-charge services, in the data value chain nothing is free of charge. It is quite evident that data are increasingly the currency of a data-driven economy, but because of the Lisbon Treaty we have a curious outcome. We are talking about personal rights, where an individual can even refrain from exercising his or her rights, but a kind of authoritative discipline intervenes in the interests of all, regardless of the choice of the individual. For instance, the principle of proportionality and necessity, which means compatibility with purposes originally achieved for commercial ends and other purposes to be achieved by the same data controller or others, is of a mandatory nature: we do not care about the potential for choice. Choice will be confined by the reform to a minor corner where genuine will can be revoked without any counterproductive effect. In parallel, we will focus on the concentration of information in a few hands.

We have started an exercise with Commissioner Vestager to see how the proportional impact of data protection can be evaluated by the competition authority. What does it mean to concentrate data in the hands of a few? When WhatsApp is merged with Facebook there are also data protection implications to be evaluated. We basically do not care about the free-of-charge approach. On the contrary, this is a signal saying that much more attention is needed to see what the trick is.

Lord Green of Hurstpierpoint: I am not sure I entirely understand what you are saying. Are you saying that an unbundling approach is just technically infeasible, or merely that nobody is discussing it because you are coming at it from a higher notion of privacy and not from the perspective of making a market work better, at least in principle?

Giovanni Buttarelli: The right to portability may have sense but it is not the unique solution or the only winning solution; others have to be considered. In a recent opinion we adopted on ethics, we also recommended further exploration of the idea of privacy vaults or areas where you may apply the principle of data in one hand—a secure place in closed computing where an individual can preserve their data and give access to the relevant players' or intermediaries' platforms, depending on his or her choice, without the need to apply the principle of transfer of portability, because the data will remain in one place or will only be accessible in that way.

Lord Green of Hurstpierpoint: I do not want to press this too far, but if you go down the route of unbundling, assuming it is technically feasible—I cannot believe it is not—you enable the consumer to capture more of the value of the data they have given up to the

platform than they do at present, more so than simply making it transparent by the way, because they can say, "I accept that I am going to pay for the cost of the platform, which at the moment I get for free, in return for which I am going to get a reward if I agree to my data being used for other purposes". That is a normal unbundling process, and it is exactly what the Commission forced in the case of Microsoft, for instance.

Giovanni Buttarelli: The purpose indication principle is a problem. It has to be respected in any event, regardless of agreement between the data subject and the controller. You have to identify to what extent the original purpose is fully compatible with the other one. We adopted, with the Article 29 working party, a document to help businesses realise in advance the kind of compatibility and a checklist to assess it. In other words, this is not an area where a contractual approach is delivered.

Lord Green of Hurstpierpoint: I do not see why not, but we will let that pass for the moment. Take the simple example of Facebook using my data for marketing purposes. I could make them pay me for that in return for accepting that I have to pay to use the Facebook platform, which at the moment I do not. Then I could decide whether I want the money or not.

Giovanni Buttarelli: Are you saying that Facebook is using your data for another platform?

Lord Green of Hurstpierpoint: No; they are using their own marketing, or their own discussions with the advertisers who pay them.

Giovanni Buttarelli: I have to insist on this point. Even in the case of data coming from another provider, or data already in the hands of Facebook used for other purposes within Facebook, a compatibility assessment has to be made. If you do not succeed on that test the agreement, free of charge or not, is not playing a role. Recent statements from the Article 29 working party are self-evident in this perspective. Assessment is made of the extent, when you start to process information for one purpose, you have in mind—

Lord Green of Hurstpierpoint: I entirely accept that, if you take a bunch of data under an agreement to use it for purpose A and end up using it for purpose B, that is a breach of contract.

Giovanni Buttarelli: Not necessarily a breach of contract.

Baroness Donaghy: If you know about it.

Lord Green of Hurstpierpoint: It is a breach of contract whether or not you know about it. You make it worse because it is difficult to tell what is happening.

Giovanni Buttarelli: We accept succession between different models. The question is that, if you merge WhatsApp and Facebook, you have to see what the Americans call the context. In the recent Bill of Rights submitted by Obama's Administration to Congress, what we call "purpose limitation" is defined as "respect for the context"—what you can reasonably expect in the short and medium term with regard to use of the data. There is a limit. Therefore, there is also a discretionary evaluation with a little flexibility, but then there are objective limits. I am happy to give further details.

Lord Green of Hurstpierpoint: I might take you up on that.

Q56 Lord Mawson: To what extent do consumers have control over the personal data they share? What steps could be taken to improve consumer control over their personal data? To give a little illustration, we have all come here today as parliamentarians. We have lots of technology that is meant to protect us. We have just walked into this building and passed two men with large guns. We were not asked who we were. We went to a desk and gave them our passports. We got a pass. We do not know who the person on the desk is. We do not know what they are doing with our passports at the moment. That is an illustration of the craziness of the world we are in. You would think that, if we could put a technology innovator into that space, they would come up with a little system that would be far simpler and make me feel more in control. It seems to me that part of the question about data is how much control I have not only over my passport but over my data. What work have you done to look at who is out there in terms of modern entrepreneurial technology companies—and can we meet them—looking at the whole question of protection of my data? It is almost as if I need a key that I can put in a door to control my data. Maybe that is simplistic, but who is doing the work out there to find technological solutions to these things?

Giovanni Buttarelli: That is simply music to me; you are saying what I have repeated since the moment of my appointment. The new legal framework should be much more user-friendly and it should build on the basis of recent surveys. I am sure you heard about the Eurobarometer survey this year. I give just three quotes: six in 10 citizens do not trust online businesses; two-thirds are concerned about not having complete control over the information they provide online; and seven in 10 are concerned about their information being used for a purpose different from the one it was collected for.

The reform builds on the need to strengthen data subjects' rights, and it is largely based on more dynamic requirements. It builds in a notion of control, which is not only about choice but the ability for an average user better to understand the context and, therefore, the relevant consequences—easy access to competent regulators and the courts, with class actions where needed, or, more specifically, the ability of competent associations to act based on the principle of representative majority.

Lord Mawson: But there must be some people out there—maybe I am wrong—who are worried about a technological solution to some of the questions that worry so many of us. This whole market is about innovation—we are only 20 years in. There must be companies and people out there worrying about it, because if you found that key you would be in a very wealthy business.

Giovanni Buttarelli: As part of our exercise, we launched a new network called IPEN—the Internet Privacy Engineering Network—where we demonstrate that "privacy by design" and "privacy by default" are not simply formal principles. They have to be used not only for the design of computers and software but to identify solutions to understand more easily from the consumer viewpoint an act in terms of control. If as a data controller you de-bureaucratise, I am sure that you will focus more on what is essential in terms of notice by refraining from bombarding people with every detail where it is less relevant. The quality of notices in the new framework will be verifiable by regulators to say that you are below the threshold, "This is not dynamic communicative language", or, "You did not use in this area the privacy by design principle, which is not a recommendation but a mandatory principle".

Q57 Lord Freeman: My question is about compliance by online platforms with existing protection laws. There are three specific points which I will ask you to comment on. First, how compliant are they at present in your judgment? That is obviously a generalisation. Secondly, how do we know when they are not being compliant? Thirdly and most importantly, what is your advice as to whether and to what extent protection agencies need more powers?

Giovanni Buttarelli: How much do they comply? Not at the level required. It depends; it is country by country and it happens much more in the EU and much less outside it. Three recent court cases before the Court of Justice can now be considered as landmark judgments: for example, the right to be forgotten and the recent decision in Schrems concerning safe harbour, where the emphasis was not on bilateral agreements with the US

but on a higher level of data protection. My analysis is that this is not a disaster, but it is not satisfactory. That is why the second pillar of the reform is to strengthen data controllers' accountability.

How do we know? We know from complaints, audits, investigations by independent DPAs[7] and a limited number of court cases; and from co-ordinated actions by data protection authorities. There is a lot of work to be done. That leads to the third question: what do we do with what you call protection agencies and we call data protection regulators? Perhaps one of the most encouraging signals in the reform is to have much more transparent and accountable institutions that are more powerful because they can apply sanctions. They have not only remedial powers but pecuniary sanctions—scalable, depending on the gravity. They have much more power in terms of logistics and human resources; they are independent of the market and Governments; they have accountability in terms of being predictable and transparent; they have accessibility; there is co-operation in cross-border cases, which are increasing, and co-ordination of relevant approaches.

Let me come back for a second to the e-privacy Directive. We started by saying that to date it is applicable largely to telecom companies. The conclusion that the e-privacy Directive was also applicable to search engines was at the time controversial. Then last year, we had the Costeja González case. The Court of Justice concluded in May 2014 that search engines are data controllers and are subject to the general Directive—they did not mention the e-privacy Directive. Therefore, data subjects can easily access search engines directly, and not necessarily the first website that publishes the information. This is the novelty. Data protection authorities started co-ordinating their activities by applying de facto what is now called in the reform the one-stop shop consistency mechanism—testing what the future will be.

It has been a challenge to co-ordinate 28 voices to reach a common position to be implemented at national level, depending on different administrative laws, procedures, outcomes and priorities. The reform builds on the duty and obligation to co-operate more and to say less, "This is not my priority", because the priority will be defined at European level. It will invest more on cross-border cases, in terms of joint operations and the exchange of experiences, given that 66per cent of processing under national DPAs is currently global,

[7] Data Protection Authorities

and much less local. Even implementation of these principles against local providers is based on principles established at EU level.

I am not saying that the reform is the panacea for all the relevant problems, but when discussing the future Regulation of online platforms we need to see the global scenario and to work less in silos. It is a challenge for us as well. We do not want to impose the data protection viewpoint horizontally. We want to build. We might not be able to answer difficult questions one by one from the technical perspective, but we offer the chance.

To conclude, my vision is not that data protection is the centre of the world but that it can be a help for an entirely new business model, where we do not want to block innovation and where it is not mission impossible to mention technology in a piece of legislation. At the same time, without good data protection you cannot invest energy in terms of consumer trust and business models. In our view, the technologies are not morally acceptable everywhere. We do not know how they will evolve and how the design will work out, but we think that the message should be to consider individuals less in terms of users, consumers or subscribers and more as persons. We would like to consider what it means for the dignity and respect of users, particularly in the face of "Take it or leave it" approaches.

Q58 Lord Freeman: That is very helpful. Can I follow up directly with a related question, of which I think we have given you notice, about looking at it from the point of view of users. Over the course of our inquiry we have all found evidence of a wide range of possible data protection changes, both regulatory and self-regulatory. However, we have also heard that consumers tend to base their actions on convenience and that more information is not necessarily the answer. What in detail does the EDPR think online platforms need to do to empower users more, and how could that be accomplished?

Giovanni Buttarelli: To understand the context better, they should work less with difficult contractual clauses; use more dynamic language to simplify the message; have scalable approaches; identify new systems in a way that is more compatible with data subjects' rights; and focus on apps for tablets and particularly smartphones, to be used, for instance, in the health area. We demonstrated recently that there is a way to have a successful business model by minimising the impact on data users. Where are the data processed? Who is controlling the information? Where are they located? Are they on a smartphone or server? We realised that in some cases the invasive approach to the data subject did not come from awareness; it was simply the result of an automatic process within the company

and they realised only at a later stage. There is an issue of data protection culture, realising that perhaps being more user-friendly can be of help.

We have examples of companies that have invested energy to stop an overly regulatory approach, for example, opt-in versus opt-out, particularly with regard to online tracking, by investing a lot of money in an opt-out solution. The World Wide Web Consortium is an example. That is based on the famous "Do not track" approach where by default I will collect information about you—your IP address and cookies going beyond the session's cookies—unless you modify the settings. The problem is that this kind of opt-out approach does not work. The US in particular lobbies a lot in Europe, because basically it is an activity that is much more relevant outside the EU. The current EU rules are based on the opt-in under Article 5.3 of the e-privacy Directive, but the big players are outside the EU. They have been lobbying a lot to insert in the GDPR a modification to the current legal framework. To date, they have failed. They offer in exchange this model, which is not working at all. We found that in the US the system is dead in the water—just a manifesto without any substance. I would not be against a system where users had more ability to speed up the process for access to their information. It also depends on the company. Companies such as Apple have less interest in sharing information, while others have an interest in maximising any kind of information as much as possible, because they are thinking of the future and the day when processing billions and billions of pieces of information may be an advantage.

I am not sure that your question has an easy answer, and I will tell you why: because of the business model. The question is how we go beyond the standard protective measures, where we protect or empower the individual more; how we approach the issue of privacy as a competitive advantage, allowing individuals to identify a company because of the privacy policy; and how we can more effectively approach aggressive companies that do not comply. That is a serious problem today because the Americans rightly say that we have solid principles, but we are weak on enforcement, and that is the reality.

Q59 Baroness Donaghy: The regulatory inconsistencies between Member States must be one of your biggest challenges. What permanent features can you offer? Like Lord Aberdare, I was interested in anonymity in return for light-touch legislation, but what are the permanent factors you can offer that will make wildly inconsistent Member States, with very different views on this, come together in one consistent policy? I am also thinking of the timeframe. When you mentioned 20 years, some of us thought "Er, what?". This is such a

fast-moving area that data protection is one of those things that perhaps has a slightly more permanent ring to the ear than some of the other aspects.

Giovanni Buttarelli: Mrs Reding in 2012, when introducing the Commission proposal, commented on the change: "For the future, one Europe, one law". That is partly true. It is extremely relevant for anonymisation, big data and a lighter approach, because we have space for guidance by the network of data protection authorities. We are moving from an advisory group, the current Article 29 working party, to the EDPB[8] with power to adopt binding decisions, including the certification of codes of conduct, audits, guidance, recommendations and best practice, and I am sure big data will be part of its priorities.

In parallel, the new Regulation will be directly applicable to all 28 Member States; it will not require implementation[9]. It will automatically replace existing, conflicting and even equal rules in all 28 Member States, but it will not represent the only piece of legislation. This is in my view one of the challenges for a Committee like this one. We counted at least five categories of national laws that will survive even this Regulation. They include provisions building on the Regulation that further specify existing requirements or new requirements, or that perhaps develop the Regulation in further detail, and provisions allowed by the Regulation that will introduce new obligations; for instance, the article about alternative requirements for consent mentions the need to comply with legal obligations in a member state—provisions for businesses to comply with security rules is one example. Another category concerns provisions that entitle you to derogate or depart from the Regulation. Finally, the five areas where Member States will have more margin for manoeuvre are media, scientific research, health, statistics and employment practices. To conclude, there are known data protection provisions, which are not directly affected by the Regulation, including national legal frameworks on online platforms, where perhaps Member States will have marginal manoeuvre, provided full consistency is ensured. Other examples are e-government and intellectual property rights.

How do you ensure full synergy with those seven blocks of legislation? Even in the six areas I mentioned, you cannot exclude some uniform rules at EU level, but it will be mainly a galaxy of different platforms, so interaction between national parliaments and the European Parliament will remain key.

---

[8] European Data Protection Board (to be established under the GDPR).

[9] The witness clarified this to mean transposition into national law.

The Chairman: We are almost out of time, but we have two rather important questions relating to the relationship between the data side and market dominance. If Lord Green and Lord Mawson can put them in sequence perhaps we can have one answer.

Lord Green of Hurstpierpoint: To some extent we may have covered my question in the earlier discussion. Perhaps I should hand the floor to Lord Mawson.

Q60 Lord Mawson: We have heard that data-driven network effects have the potential to entrench dominant positions. On the other hand, we have also learnt that data are non-exclusive and can be replicated by several platforms at the same time. To what extent are data a parameter of competition or market power?

Giovanni Buttarelli: It is. As discussed with Commissioner Vestager, a new scenario can now be identified. I am not party to investigations by competent national data protection authorities under competition law, but we understand that there is much more interest from that side to analyse, for instance, the existence of a dominant position, including apparent free-of-charge services, and to consider to what extent breach of a data protection rule could be automatically or indirectly relevant, say, to an unlawful or unfair approach under competition law. To what extent is unfairness according to the two different areas—competition and data protection law—convergent?

The preliminary opinion we adopted last year has been followed by a successful workshop to which we invited the Federal Trade Commission and other experts from around the world. We hope to have a consolidated opinion in a few weeks from now, in early 2016, to sum up the debate, as the new scenario seems to be the reality. The conclusion of pending investigations before the Commission, particularly on search engines, will be, in my view, very promising.

The Chairman: Thank you very much indeed. You have given us a fair chunk of your time and some very full answers to our questions. Unless there is anything you want to add, we will break shortly.

Giovanni Buttarelli: I simply thank you once again for this chance. Of course, if you want any clarification or footnotes, or if there is anything you would like me to develop further—perhaps where issues have been too clear, very clear or unclear—please contact me.

The Chairman: You are laying yourself open. We will study the transcript carefully. You may well hear from us. Thank you very much indeed.