Statement of Helen Dixon, Commissioner, Data Protection Commission of Ireland

Before the

U.S. Senate Committee on Commerce, Science, and Transportation

Hearing on

"Consumer Perspectives: Policy Principles for a Federal Data Privacy Framework"

Wednesday, May 1, 2019

Introduction

Chairman Wicker, Ranking Member Cantwell and Members of the Committee, thank you for inviting me to be here today.

I am pleased to have the opportunity to share with the Committee the experience of the Irish Data Protection Commission in dealing with complaints from consumers under the General Data Protection Regulation or GDPR, applicable since 25th May 2018. Clearly, in a global context, the GDPR represents one significant form of regulation of the collection and processing of personal data and the Irish Data Protection Commission's approach to monitoring and enforcing its application provides an early insight into the types of issues raised by consumers in complaints about how their personal data is handled.

It's useful for me to take a few minutes to set in context for you the circumstances in which complaints from consumers are lodged with the Data Protection Commission.

The right to have one's personal data protected exists as an explicit fundamental right of EU persons under the EU Charter of Fundamental Rights that came into legal force in 2009 and the right is called out specifically in Article 16 of the Treaty on the Functioning of the European Union – the "Lisbon Treaty". It is of course not an absolute or unlimited right. It may be and often is subject to conditions or limitations under EU and member state law but those conditions cannot render it impossible for individuals to exercise core elements of the right to data protection. The aim equally of a consistent and harmonised data protection law across the EU is to ensure a level-playing field for all businesses and a consistent digital market in which consumers can have trust. While many may argue that data privacy is now "dead" given the ubiquitous nature of data collection in online environments, the Data Protection Commission can nonetheless identify the clear benefits to consumers of having exercisable and enforceable rights. (Dorraji, 2014)

The committee is well aware of the basic structure of the GDPR which sets out a) obligations on organisations, b) rights for individuals, and c) enforcement provisions. As an EU regulation, it has direct effect in every EU member state but also has extra-territorial reach in that it applies to any overseas company targeting goods or services at European consumers.

Obligations

Under the GDPR, a series of obligations apply to *any* organisation collecting and processing information that relates to an identified or identifiable person. A broad definition of personal data is in play with the GDPR specifying that identification numbers, location data and online identifiers will be sufficient to bring data in scope. The obligations on organisations are set down in a series of high-level, technology neutral principles : lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality and accountability.

Rights

In turn, the individuals whose personal data are processed have a series of enumerated rights under the GDPR. Incidentally, individuals under the GDPR are referenced as "data subjects" which is a concept far broader than consumers given that the GDPR concerns itself with any personal data processing and not merely that which occurs in commercial contexts. However, I understand for the purposes of this committee, that it is the subset of data subjects that are consumers and service users that is of particular interest. The rights of consumers under the GDPR are set out in Chapter 3 and cover the right to transparent information, the right of access to a copy of their personal data, the right to rectification, the right to erasure, the right to restriction of data processing, to object to certain processing and the right to data portability with varying conditions pertaining to the circumstances in which those rights can be exercised. And I will revert to these rights shortly when I outline for the committee a profile of the complaints from consumers the Data Protection Commission is handling where consumers allege those rights are not being delivered on by companies.

Enforcement Provisions

Finally, the GDPR provides for independent and adequately resourced data protection authorities in each EU Member State to monitor the application of the GDPR and to enforce it (these authorities are separate and distinct from the consumer protection and anti-trust authorities in the Member States). In this context, data protection authorities have a very broad range of tasks from promoting awareness, to encouraging industry codes of conduct to receiving notifications of the appointment of Data Protection Officers in companies to handling complaints from consumers and investigating potential infringements of the GDPR.

In general terms, the individual EU member state data protection authorities are obliged to handle *every* valid complaint from any individual in their member state and to supervise establishments in their territory. However, because of a new "one-stop-shop" innovation in the GDPR, multinational organisations operating across

the EU can be supervised by one lead supervisory authority in the EU member state where that multinational has its "main-establishment". Equally, any individual across the EU may lodge a complaint with the data protection authority in the member state of the main establishment of the company concerned. As a result, the Irish Data Protection Commission is the lead supervisory authority in the EU for the vast majority of US global internet companies such as Facebook, Twitter, WhatsApp, Google, AirBnB, Microsoft and Oath as they have their main establishments in Ireland. Equally, complaints are lodged with the Irish Commission from complainants across the EU either directly or via the supervisory authority in their own member state.

This may seem like a difficult computation given that there are potentially up to half a billion consumers in the EU. How can a data protection authority with currently 135 staff deal with complaints from across the EU and supervise so many large companies? Part of the answer lies in the orientation of the GDPR itself which places accountability to consumers directly on the shoulders of companies themselves. Companies must in many cases appoint Data Protection Officers; they must publish contact details for those officers and they must administer systems to allow them effectively handle requests from consumers to exercise their data protection rights. It's therefore now the case that many issues arising for consumers are being resolved directly through the intervention of the mandatorily appointed Data Protection Officer in the company before there's a need to file a complaint with the data protection authority. Many companies we supervise report to us that that have had a steep rise in consumer requests to exercise rights since the application of the GDPR in May 2018. Equally, EU data protection authorities can conduct joint operations where an authority like the Irish Commission can leverage specific expertise in another EU data protection authority in conducting an investigation. Further, multiple consumers may often raise the same issue as one another which may lead the Data Protection Commission to open an investigation of its "own volition" in order to resolve what may be a systemic matter. Finally, the threat of very significant administrative fines hangs over companies that fail to implement the principles of GDPR and/or deliver on consumer rights under the law with 4% of global turnover representing the outer but significant limit of fine that may be imposed.

Clearer Standards

Much of the success over the coming years of the GDPR will derive from the evolution of clearer, objective standards to which organisations must adhere. These standards will evolve in a number of ways :

- Through the embedding of new features of the GDPR such as Codes of Conduct, Certification and Seals that will drive up specific standards in certain sectors. Typically, codes of conduct that industry sectors prepare for the approval of EU data protection authorities will have an independent body appointed by the industry sector to monitor compliance with the code thereby driving up standards of protection and means by which consumers can exercise their rights.

- Through enforcement actions by the Data Protection Commission where the outcome, while specific to the facts of the case examined, will be of precedential value for other organisations. The Data Protection Commission currently has 50 large scale investigations running which, as they conclude in the coming months, will serve to set the mark for what is expected of organisations under the principles of transparency, fairness, security and accountability
- Through case law in the national and EU courts, where data protection authority decisions are appealed or in circumstances where individuals use their right of action under the GDPR to claim compensation for any material or non-material damage they have suffered arising from an infringement of the GDPR.
- Through the provision of further guidance to organisations on specific data processing scenarios particularly through published case studies of individual complaints the Data Protection Commission has handled. Equally, guidance will be published off the back of consultations with all stakeholders on how to implement principles in complex scenarios such as those involving children where specific protections and consideration of the evolving capacities of the child need to be factored in.

Consumer Complaints

In the 11 months since GDPR came into application, the Data Protection Commission has received 5839 complaints from individuals. It is frequently a feature of complaints we handle from consumers that their interest in their personal data is as a means of pursuing further litigation or action. For example, former employees of organisations often seek access to their personal data as part of the pursuit of an unfair dismissals case; consumers seek access to CCTV images in different scenarios to pursue personal injuries cases and so on.

Overall, the most complained against sectors in a commercial context are retail banks, telecommunications companies and internet platforms.

In the cases of the retail banks and telecommunications providers, the main issues arising relate to consumer accounts, over-charging, failure to keep personal data accurate and up-to-date resulting in mis-directing of bank or account statements, processing of financial information for the purposes of charging after the consumer has exercised their right to opt-out during the cooling-off period. While you might argue that these are clearly predominantly customer service and general consumer issues, it is the processing of their personal data and in particular deductions from their bank accounts that bring consumers to the door of the Data Protection Commission.

In terms of the internet platforms, individuals, as well as Not-for-profit organisations on their behalf that specialise in data protection, raise complaints about the validity of consent collected for processing on sign-up to an app or service, the transparency and adequacy of the information provided and

frequently about non-responses from the platforms when they seek to exercise their rights or raise a concern. Further, the Data Protection Commission has received several complaints about the inability of individuals to procure a full copy of their personal data when they request it from a platform. This can arise in scenarios where platforms have instituted automated tools to allow users by self-service to download their personal data but elements of data are not available through the tool. In one such complaint we are handling, the user complains that significant personal data is held in a data warehouse by a platform and used to enrich the user's profile. The platform argues that access to the data is not possible because it's stored by date and not individual identifier and further that the data would be unintelligible to a consumer because of the way it's stored. The Data Protection Commission must resolve whether this is personal data to which a right of access applies.

Other cases dealt with this year by the office relate to financial lenders required to notify details to the Irish Central Bank of credit given to individual consumers. Certain lenders notified the details twice resulting in adverse credit ratings for the individuals as they appeared to have 2 or 3 times the number of loans as compared to what they actually had. In another case, a multinational agent dealing by web chat with a service user about a customer service complaint took note, according to the complaint received by the office, of the consumer's personal details including mobile 'phone number she used to verify her account and contacted the user asking her on a date. That didn't turn out to be a happily-ever-after story when independently of the investigation of my office, the agent was removed from his job!

A further complaint dealt with was lodged by an individual who had suffered a family bereavement. A tombstone company issued immediate correspondence to her family advertising cheap headstones in respect of the dead relative. The tombstone company had taken data from an online death notice website and recreated the full address from multiple other sources. The actions of the company were not only distasteful but in breach of the purpose limitation requirements of data protection law.

A particularly concerning case was reported to the office six months ago concerning a mobile 'phone user whose ex-partner had managed to verify identity with her mobile telephone provider by masquerading as the individual herself and gained control of her telephone number. He did this by contacting the telco via web chat and when asked to identify himself, he provided her name and mobile 'phone number. He then told the customer service agent at the telco that he (masquerading as her) had lost his mobile 'phone, had now purchased a new SIM card and requested that the 'phone number be ported over to the new SIM he had bought. The agent asked the imposter the following verification questions :

- What is your full address? **Answered correctly**
- What are 3 frequently dialled numbers? **Could not answer**
- Can you tell me your last top-up date? **Could not answer**
- Can you tell me your last top-up amount? **Answered correctly**

Despite the imposter not answering all of the questions, the agent accepted this as valid authentication, and ported the complainant's number onto the imposter's newly bought SIM card. This gave access to any future texts and calls coming to the complainant's phone number. This would allow for example the imposter to bypass the 'phone number factor for authentication with her online banking account. In this case, the telco had failed to adhere to its own standards for verification of identity with very unfortunate consequences.

Parallel but overlapping laws to the GDPR specific to E-Privacy are equally enforced by the Data Protection Commission and annually the office prosecutes a range of companies for multiple offences. In the majority of cases, these relate to targeting of mobile 'phone users with marketing SMS messages without their consent and/or without providing the user with an OPT OUT from the marketing messages. Equally, a number of companies are prosecuted annually where they offer an OPT OUT but fail to apply it on their database resulting in the user continuing to receive SMS messages without their consent. As a result of several years of consistent high-profile prosecutions in this area, the Data Protection Commission considers the rate of compliance appears to be improving.

Considerable resources of the office have been applied in recent years to a series of investigations into the "Private Investigator" sector. The Data Protection Commission received complaints from individuals who had lodged claims with their insurance providers and later became concerned about how their insurance company had sourced particular information about them and used it to deny their claims. The Data Protection Commission uncovered a broad-ranging national "scam" involving a considerable number of private investigator or tracing companies that had been either bribing or blagging government officials and utility company staff in some cases to procure a range of pieces of personal information about the claimants. 5 companies and 4 company directors were successfully prosecuted by the Data Protection Commission for these data protection offences over the last 4 to 5 years.

The final case I'll mention in a commercial context is the case of an individual who suffered an accident giving rise to a leg injury. When her claim to her insurance company was denied, she sought access to a copy of her personal data that had been used by the company to deny her claim as she was surprised at the reasons given. She discovered on receipt of her personal data, that her family doctor had, instead of sending a report detailing information about the nature of her leg injury suffered in the recent accident, sent the entire file of 30 plus years of consultations between him and the patient to the insurance company. The company used very sensitive information about another condition the woman had suffered from years previously to deny the claim. Aside from the denial of the claim, the complainant suffered considerable distress at the thought of a very sensitive and irrelevant set of information about her having been disclosed and then processed in this matter. This office found the family doctor had infringed data protection law in disclosing excessive personal data including sensitive personal data. Ultimately, this complainant pursued a civil claim for compensation in the courts and the case settled on the steps of the court.

Outside of these commercial contexts, a large volume of complaints that come to the Commission relate to, for example, employees complaining about their employers using excessive CCTV to monitor them or unauthorised access and excessive processing of their image if the employer uses CCTV as part of disciplinary proceedings. Each of these cases has to be examined on its specific facts with consideration given to the proportionality of processing in the given circumstances.

The most frequent category of complaint relates to access requests where an individual considers they have been denied access to a copy of the personal data they requested from an organisation. In the majority of cases, the Data Protection Commission amicably resolves these cases which in an access request scenario means we ensure the individual receives all of the personal data to which they're entitled. This may of course be less than they sought as an organisation may legitimately apply exemptions where it is lawful to do so.

The Committee will be well aware of various academic studies on the so-called "privacy paradox" where discrepancies between our attitudes as online users and our behaviours are apparent. This is a complex area of study but I raise it by way of pointing out that consumer complaints alone may not give us a very complete picture of what concerns consumers or what elements of the controls provided by platforms are useful to them. The platforms don't publish data on user engagement with their privacy control dashboards and the frequency with which users complete "privacy checkup" routines prompted by the platforms but based on data they have shared with the Data Protection Commission, the number of users seeking to engage with and control their settings is significant. Of course, this leads us then to the issues raised by Dr Zeynef Tufecki in the recent New York Times privacy series on whether being "discreet" online protects users and where she concludes that powerful computational inferences make it unlikely discretion is of much assistance. (Tufekci, 2019) Academic Woodrow Hartzog equally argues against idealising a concept of control as a goal of data protection. (Hartzog, 2018)

Large-scale Investigations

This brings me then to the important work of the Data Protection Commission outside of the role in handling complaints from individuals. In many ways, effective implementation of principles of fairness, transparency, data minimisation and privacy by design will negate the need for users and consumers to have the responsibility for ensuring their own protection thrust *entirely* upon them through making decisions about whether to "consent" or not.

The Data Protection Commission has powers to open an investigation of its own volition or may opt to open an investigation into a complaint from an individual that discloses what appears to be a systemic issue that potentially affects hundreds of millions of users.

The Data Protection Commission has currently 51 large-scale investigations underway. 17 relate to the large tech platforms and span the services of Apple, Facebook, LinkedIn, Twitter, WhatsApp and Instagram. Because the GDPR is principles-based and doesn't explicitly prohibit any commercial forms of personal data processing, each case must be proved by tracing the application of the principles in the GDPR to the processing scenario at issue and demonstrating the basis upon which the Commission alleges there is a gap between the standard we say the GDPR anticipates and that which the company has implemented. The first sets of investigations will conclude over the summer of 2019.

Redress

EU data protection authorities resolve complaints of individuals amicably for the most part and where amicable resolution is not possible, the action of the authority is directed against the processing organisation. Authorities do not order redress in the form of payment of damages to individuals whose rights have been infringed.

In order to secure damages, individuals have a right of action under Article 82 GDPR where they or a not-for-profit representing them can bring a case through the courts to seek compensation for material or non-material damage they allege they have suffered as a result of infringements of the GDPR. Such Article 82 actions for compensation by individuals in the Irish courts have not yet been heard but when these are, they will represent further clarifications on how the courts view the GDPR and its application.

No class action system exists in Ireland and in general this is not a feature of the EU landscape. While there are some reports emanating particularly from the UK that representative actions are being lined up by some law firms on a "no win no fee" basis post large-scale breaches being notified, nothing of significance has materialised in this regard. (Osborne Clarke - GDPR one year on: how are EU regulators flexing their muscles and what should you be thinking about now?)

Conclusion

EU data protection law places a strong emphasis on the individual and the exercise of their rights and accordingly mandates the handling of every complaint from an individual by data protection authorities. This means EU data protection authorities play an important dual role – on the one hand, resolving high volumes of issues for individuals and on the other supervising companies to ensure systemic issues of non-compliance are rectified and punished as appropriate. The GDPR is 11 months old and clarity and consistency of standards will evolve in the coming years driving up standards of data protection for consumers in every sector.

References

Dorraji, S. E. (2014). Privacy in Digital Age : Dead or Alive?! Regarding the New EU Data Protection Regulations . *SOCIALINĖS TECHNOLOGIJOS SOCIAL TECHNOLOGIES 2014, 4(2)*, 306-317.

Hartzog, W. (2018, Volume 4 Issue 4). The Case Against Idealising Control . *European Data Protection Law Review* .

(n.d.). *Osborne Clarke - GDPR one year on: how are EU regulators flexing their muscles and what should you be thinking about now?* 2019 Lexology : daily subscriber feed.

Tufekci, Z. (2019, April 21). Think You're Discreet Online? Think Again. *New York Times*.