2019

If the Legislature Had Been Serious About Data Privacy...

Fred H. Cate
Indiana University Maurer School of Law, fcate@indiana.edu

Christopher Kuner
Vrije Universiteit Brussel

Orla Lynskey
London School of Economics

Christopher Millard
Queen Mary University

Nora Ni Loideain
University of London

See next page for additional authors

Authors
Fred H. Cate, Christopher Kuner, Orla Lynskey, Christopher Millard, Nora Ni Loideain, and Dan Jerker B. Svantesson

Editorial

If the legislature had been serious about data privacy . . .

Christopher Kuner*, Fred H. Cate**, Orla Lynskey**, Christopher Millard**, Nora Ni Loideain** and Dan Jerker B. Svantesson**

It is approximately a year since the European Union's (EU) General Data Protection Regulation (GDPR) came into force, sparking an unprecedented data privacy frenzy. It has been celebrated, and it has been feared. It has been seen as going too far, and it has been seen as not going far enough.[1] Perhaps it is a rather safe bet to predict that the true impact—which still remains to become crystallized—will fall somewhere in between these extremes. But one thing we already know with great certainty is that the GDPR's impact will be felt, indeed is being felt, far beyond the borders of Europe.

Furthermore, law makers around the globe—from Argentina to New Zealand, and from Kenya to Thailand—are now busying themselves with legislative initiatives replicating the GDPR. Consequently, this may seem a strange time to question the sincerity of the general will to tackle the data privacy concerns.

However, at the same time as countries around the world engage in a data privacy law arms race with the pursuit of higher fines, 'rep localisation' requirements,[2] and excessive unnuanced jurisdictional claims, our world continues to be data-driven. It is typically data we contribute when we get online services for 'free', and in relation to most of those apps and other online services we use for free, we—the users—are the product, as the saying goes. This is well-known and despite provisions aimed at minimizing data collection,[3] we have all become used to the idea that our data are constantly collected, frequently shared, monetized, and regularly lost or otherwise misused. There is nothing in the GDPR, or in any other data privacy laws, that will change the centrality of the role that data play in society, and our data privacy laws make no attempt at breaking the advertisement-driven business models that largely are responsible for creating an insatiable appetite for data.

There are many reasons why data privacy laws fail to protect us. There are some deeply troubling practices, such as Cambridge Analytica's apparently invasive use of data analytics for political purposes.[4] Moreover, this may be just the tip of a social media iceberg that includes structural issues that will in due course be addressed via competition and consumer law.[5] There are also 'accidental' data losses; some of them caused by negligence, some of them not, but many of them harmful. Then there is the fact that data privacy laws often are difficult to understand making it difficult for those subject to the laws to ensure compliance.[6]

To address the current situation, data privacy laws are often interpreted as frameworks that merely seek to manage the pervasive collection and use of data. But, as approached in the past and as now required under the GDPR, it would of course be possible to go much further towards actually minimizing data usage. Yet, since the business model of many companies that provide popular 'free' services depends on monetizing our

* EIC.

** Editor.

1 See eg the interesting discussion by leading scholars in the Symposium on EU Data Protection Reform we published in vol 4, Issue 4, November 2014.

2 See eg GDPR art 27 mandating that a foreign controller or processor have a designated representative in the EU. Similar, and seemingly even more stringent, requirements can be found elsewhere; for example, in s 36(5) of Thailand's *Draft Personal Data Protection Act* of the September 2018 version.

3 See eg GDPR art 5(1).

4 <https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf> accessed 21 April 2019.

5 See eg commentaries on the intersection of these laws with data privacy by leading scholars in the Symposium on EU Data Protection and Competition Law we recently published in vol 8, Issue 3, August 2018.

6 Christopher Kuner and others, 'The Language of Data Privacy Law (and How It Differs from Reality)' (2016) 6(4) *International Data Privacy Law* 259.

data, we cannot realistically expect to receive all the services we value in the absence of any data collection. Thus, aside from discussions about inadequate transparency and whether the 'price' we pay in data is too high for what we get in return, one option that surfaces occasionally is for people to be able to choose to pay for the services they desire with money instead of in data.

Clearly, such an option cannot be aimed at eliminating the collection and use of data. After all, many services are attractive precisely because of a high degree of personalization; something which many users appear to value and which cannot be delivered without data analytics. Rather what would be eliminated under a 'pay-with-money-not-data' option is the monetizing of the data—data would be used for the service only, not for profit. Drawing a sharp distinction between data being used for the service only, and data being used for profit will not always be easy. However, this is by no means a problem unique to this distinction and the law is used to working with difficult distinctions.

Some will no doubt characterize this as a 'pay-for-privacy' option and express outrage at the very notion of paying to protect their data privacy, not least given that data privacy is a fundamental human right. However, the 'pay-for-privacy' slogan is clearly misleading. Indeed, this type of concern may be countered by reference to the fact that the model discussed here is actually reflecting long-standing common commercial practices—after all, it is paying with data that is a new phenomenon and paying for a service with money that is the traditional approach. If you do not want your data to be used for profit when you use a private entity's email service, search engine or social media network, what you would be paying for is not the protection of your privacy, you would be paying to utilize the service in question without consenting to the types of for-profit data processing that are commonplace today. Thus, the 'pay-with-money-not-data' option shares similarities with, or arguable is a type of, the paid-for premium services provided by many online businesses, for example, eliminating advertisement.

We hasten to stress that the 'pay-with-money-not-data' option discussed here must never be an alternative to the conditions that data privacy laws place on the processing of personal data. Even if a 'pay-with-money-not-data' option was introduced, there would obviously still be a need for traditional data privacy laws.

Another concern that may be expressed is that some of the key companies in question will never agree to adopt a 'pay-with-money-not-data' option. Such a concern is obviously well founded. However, where such an option does not evolve through market pressure, the legislator may need to step in. In fact, it may be said that any data privacy law that is truly serious about addressing the current situation, characterized by over-collection and misuse of data, must include rules mandating the availability of a pay-with-money-not-data option, exactly because such an option is unlikely to emerge widely enough by market forces alone.

Numerous further questions would need to be confronted if a scheme like this was to be pursued. For example, we may ask how much would people be willing to pay to access the relevant services while maintaining their data privacy? And how should the price be determined? Perhaps the price businesses would be allowed to charge should be in line with the profit they actually make from our data? This may not be easy to calculate, but it should not be impossible to make an estimate that is good enough.[7]

Where we do not have a pay-with-money-not-data option, we, the users, are presented with a binary choice of either embracing the benefits offered by the service in question and thereby accepting the monetizing of our data or missing out on those benefits. That is not a choice we should have to make, and often it is not a real choice as society is structured in manner that demands us accessing and using certain data intensive services that currently are monetizing our data. With a pay-with-money-not-data option, we would not have to make such a choice.

Some will no doubt see a mandatory pay-with-money-not-data option as an expression of a draconian 'nanny state' gone mad. And there are legitimate

7 Many popular online services (eg YouTube and Spotify) are available in 'free' (with ads) and 'premium' (without ads) versions. It is likely that the monthly charge is designed primarily to offset the 'lost' advertising revenue from a typical user. There are, however, usually other differences between such free and premium services, for example, streaming quality, amount of content available, etc, the costs of which are difficult to estimate. The picture is complicated further by the fact that premium services may still make extensive use of personal data for enhanced personalization purposes which, indeed, is a feature that many users may value. All of this, however, is relatively simple compared to the cost/value analysis for a social network, such as Facebook. Attempts have been made to estimate the opportunity cost of eliminating Facebook ads on a hypothetical per-user basis, but the monetisation value may vary substantially between users. Moreover, offering a paid-for version of a service like Facebook may have undesirable collateral consequences, such as amplifying political and cultural polarisation 'by effectively offering different media models for the haves and have-nots'. See David Cohen, 'Could an Ad-Free, Subscription Version of Facebook Be a Viable Option?' *AdWeek* (New York, 7 May 2018) <https://www.adweek.com/digital/could-an-ad-free-subscription-version-of-facebook-be-a-viable-option/> accessed 21 April 2019. See also Callum Borchers, 'Would You Pay $18.75 for Ad-free Facebook?, *The Washington Post* (14 April 2018) <https://www.washingtonpost.com/news/the-fix/wp/2018/04/14/would-you-pay-18-75-for-ad-free-facebook/?utm_term=.e54442ae2d05> accessed 21 April 2019.

reasons to question the viability of such a structure. However, as several of the articles published in *IDPL* have highlighted, and as many of our editorials have sought to emphasize,[8] the data (privacy) ecosystem is undergoing tremendous change, and all options need to be on the table.

doi:10.1093/idpl/ipz006

8 See most recently: Christopher Kuner and others, 'Expanding the Artificial Intelligence-data Protection Debate' (2018) 8(4) *International Data Privacy Law* 289.