Information Polity 23 (2018) 239–246
DOI 10.3233/IP-180002
IOS Press

Policy Review

The European General Data Protection Regulation: An instrument for the globalization of privacy standards?

Colin J. Bennett
Department of Political Science, University of Victoria, Victoria, BC, V8W 3P5, Canada
E-mail: Cjb@Uvic.ca

1. Introduction: The global diffusion of data protection

The recent revelations about Cambridge Analytica and the breach that allowed the harvesting of the personal information of some 87 million Facebook users (at latest count) has pushed privacy protection to the front pages, and focussed attention on "surveillance capitalism" (Zuboff, 2017) and on the capture of personal data as the central resource for the "platform economy". As Facebook reels from the scandal, and rushes to rebuild consumer confidence, it has also pledged to apply the standards contained in the European Union's General Data Protection Regulation (GDPR) to its global operations, if not all of them and if not immediately (Constine, 2018). At no time in the past 40 years, has the protection of privacy been so prominently, globally and intensively debated. How did it get to this point?

Information privacy as a public policy question is quite modern. It arose in the 1960s and 1970s at about the same time that "data protection" (derived from the German, *datenschutz*) entered the vocabulary of European experts. The issue was inextricably connected to the information processing capabilities of computers, and to the need to build protective safeguards at a time when large national data integration projects were being contemplated by governments (Flaherty, 1989), raising fears of an omniscient "Big Brother" state with unprecedented surveillance power. Study commissions were established in different countries, and a closely-knit group of experts coalesced, shared ideas and forged a broad consensus on how best to resolve the privacy problem as a matter of public policy (Bennett, 1992). "Data protection" or "information privacy" statutes, based on a strikingly similar set of principles, then spread around the world in a number of stages (Swire, 2013). These core principles operate as both fully fledged legal rules, as well as guiding standards for the balancing of privacy rights with legitimate organizational interests (Bygrave, 2002, p. 57).

During these early debates, it was also commonly recognized that information privacy could not simply be regarded as a domestic problem. The increasing ease with which personal data might be transmitted across borders produced two international agreements in the 1980s to regulate the cross-border

flow of personal data: the 1981 *Guidelines from the Organization for Economic Cooperation and Development* (OECD, 1981), and the 1981 *Convention* from the Council of Europe (1981). In the 1990s, harmonization was extended through the 1995 EU Data Protection Directive (EU, 1995), Articles 25 and 26 of which stipulated that personal data on Europeans should only flow outside the boundaries of the Union to countries that can guarantee an "adequate level of protection". Through the Data Protection Directive, the harmonization of data protection then extended geographically and deepened in meaning and content (Bennett, 1997). Progressively, these harmonization efforts standardized what it meant for a country to pursue adequate data protection, and for organizations to process personal data responsibly. As more countries joined the data protection "club" so there was increasing pressure on those outside the club to pass equivalent laws. There has been a process of policy convergence (Bennett, 1992), an intensification and broadening of transnational policy networks (Newman, 2008; Raab, 2011), and a general trading up of standards (Vogel, 1992; Bennett & Raab, 2006).

By the end of the first decade of the 21st century, however, the EU Data protection Directive was coming under different technological, legal and organizational pressures. Multi-national businesses were irritated by diverging interpretations of data protection principles across Europe, and by the lack of interoperability of basic provisions. The "adequacy regime" had not yielded a significant number of countries to which European organizations could legally transfer personal data. Alternative approaches to legal transfer, based on principles of organizational "accountability" (Guagnin et al., 2012) emerged and became enshrined within a system of Cross Border Privacy Rules (CBPR) legitimated through the Asia Pacific Economic Cooperation (APEC, 2005). There was also a urgent desire to "modernize" European data protection to make it relevant for the global networked digital economy, in which social networking services were generating massive volumes of user-generated content, and cloud computing services were rendering geographic borders increasingly irrelevant.

Thus, the General Data Protection Regulation (GDPR) was born. It was first proposed in 2012 to establish a uniform set of rules that would provide enhanced protection for citizens, foster innovation in the European Single Market and make the EU, according to Commissioner Jourova, "fit for the digital age" (European Commission, 2015). After a lengthy and tortuous journey through the EU-policy-making system, involving intensive lobbying mainly from multinational business interests, the GDPR was approved by the European Parliament in April 2016, and came into force across the entire EU on May 25th, 2018. It is the most ambitious and comprehensive data protection regulation in the world. What does it require, in brief? And can we then expect it to continue the global process of policy convergence?

2. The General Data Protection Regulation: The scope and principles

The GDPR is a complex and lengthy instrument, and has generated volumes of interpretive material by law firms, consultants, legal scholars and data protection authorities themselves. Like the Data Protection Directive, it enshrines a series of fundamental rights for the individual (the data subject) and imposes significant obligations on public and private organizations (data controllers), and on those with whom they contract (data processors). The essential information privacy principles under the GDPR are broadly similar to those in the Directive: lawfulness, fairness and transparency of processing; purpose limitations; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability. But they have been reinforced and broadened in a number of ways.

In terms of territorial scope (Art. 3), the GDPR applies to any EU based "establishment" where personal data are processed "in the context of its activities". Where no EU presence exists, the GDPR still applies when an EU resident's personal data is processed in connection with goods or services offered,

or where the behavior of individuals within the EU is "monitored". Monitoring expressly includes the tracking of individuals online to create profiles, including the analysis and prediction of personal preferences and attitudes.

The GDPR also extends the definitions of personal data and sensitive data. It applies to data from which a living individual is identified or identifiable, whether directly or indirectly. The GDPR's recitals also stress that certain categories of online identifiers (cookies, IP addresses, device identifiers) may fall within the scope if they can be "singled out" for the purpose of tracking user behavior (Recital 30). The processing of special categories of data on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation is only permissible under defined conditions. The GDPR also adds genetic data and biometric data to this list (Art. 9). The GDPR also encourages the use of "pseudonymisation"; pseudonymised data is personal data that can no longer be attributed to a specific data subject without the addition of other information, and may be processed subject to technical and organizational measures to ensure non-attribution (Art. 4).

There are certain conditions that need to be satisfied for the processing of personal data to be lawful (Art. 16): the consent of the data subject; necessary for the performance of a contract with the data subject; necessary for compliance with a legal obligation; necessary to protect the vital interests of the data subject; necessary for the performance of a task carried out in the public interests; or necessary for the purposes of legitimate interests. This last grounds for processing is new, and has been controversial. Various recitals provide relevant illustrations, and if an organization relies on these grounds, the reasons must be fully documented and communicated to data subjects through information notices. If the organization relies on consent, it must ensure that it is a "freely given, specific, informed and an unambiguous indication of the data subject's wishes" and not "bundled" with other agreements. Silence, pre-ticked boxes or inactivity does not constitute consent (Recital 32). Consent should also be revocable easily, and at any time. Where consent is relied upon for the processing of data on children, it must be given or authorized by a person with parental responsibility.

Rights of subject access and rectification are broadly similar to those in the existing Data Protection Directive, but the GDPR also includes a right to "data portability" requiring the controller to provide information in a structured, commonly used and machine readable form (Art. 20). The controller can also be required to transmit those data directly to another controller, thus encouraging interoperable formats and systems. This provision is particularly directed towards social media platforms, and suggests that individuals should have the right to transmit user-generated data from one to another in a seamless fashion. The rights of the data subject also embrace the controversial 'right to be forgotten' as enshrined in European law by the European Court of Justice in the renowned case involving Google Spain (Art. 17) (ECJ, 2014).

There are also restrictions on profiling and automated decision-making. Individuals have a right not to be subject to such decisions if they would have a significant effect on the data subject. Examples would be online credit decisions or e-recruiting (Recital 71). Exemptions apply if the processing is necessary for contractual reasons, if authorised by law, or if based on the individual's explicit consent. Special restrictions apply if the automated decision-making relates to sensitive data or to children.

3. The General Data Protection Regulation: A blend of global policy instruments

At the time of the passage of the Data Protection Directive, the entire panoply of policy instruments associated with the protection of personal data were neither globally understood nor deployed. Rather, particular self-regulatory, regulatory and technical instruments were closely associated with different

national administrative and regulatory traditions (Bennett & Raab, 2006). The GDPR not only revises the 1995 Data Protection Directive to produce a single harmonized regulation for the entire EU, it is also a more multi-faceted instrument, embracing and combining policy instruments that have tended to originate in non-European jurisdictions. The GDPR is therefore a manifestation of an intense international the renewed approach to supervisory data protection authorities (DPAs), which must monitor the application of the GDPR in their respective jurisdictions, and cooperate with one another to effect the consistent application of the regulation across the EU (Arts. 51–59). DPAs must act with complete independence, have sole authority over choice of staff, and may not be appointed for less than four years. Member states are also required to provide the necessary human, technical, financial and other resources necessary for them to perform their duties effectively. Considerable attention has been paid to the proposal for a "one-stop-shop" approach in cases of cross-border processing of personal data. There is a lead authority in the jurisdiction where the company has its main establishment, which must take into consideration the views of other concerned authorities, seeking mutual assistance and conducting joint investigations where appropriate. The procedures are designed to prevent "forum-shopping". A new European Data Protection Board (EPDB), the successor to the Article 29 Working Party, is comprised of the heads of the DPAs (Art. 68). It has an enhanced status with its own legal authority to conciliate disputes between DPAs, as well as to issue guidance and recommendations of best practice.

DPAs have a range of other tools available to them. Data Protection Impact Assessments (DPIAs) are required for any "high risk" processing activity, for example involving sensitive data or profiling. The DPIA must include a description of the processing, an assessment of the risks and the measures taken to mitigate risk (Art. 35). Data protection by design and by default, approaches that originated largely in Canada (Cavoukian, 2011) require organizations to implement technical and organizational measures to ensure, by default, that only necessary personal data are processed. Controllers and processors are subject to a broad data breach notification regime, whereby breaches must be reported to the supervisory authority without delay, and in serious cases must also be reported to data subjects (Art. 33). The GDPR also strengthens the process for the development and approval of codes of conduct (Art. 40). Member states and DPAs are encouraged to establish the criteria for certification mechanisms, such as privacy seals and marks (Art. 42). Finally, public authorities and any organizations whose "core activities" are the processing of personal data, or which are "large scale" are required to appoint Data Protection Officers (DPOs).

These are instruments designed to promote organizational *accountability*, which have emerged over the last twenty years mainly in countries outside Europe. In the GDPR, they do not just supplement the law; they form an integral part of the entire regulatory scheme and need to be deployed creatively by every supervisory authority (Bennett & Raab, 2017). The GDPR reflects a persistent reality that the governance of privacy is inherently based on a co-regulatory model in which regulators give organizations, advice and guidance about how and when to deploy tools, and stand in the background ready to enforce and sanction, if necessary (Bennett & Raab, 2006). Organizations, for their part, are expected to demonstrate a capacity to comply with law, so that if they are investigated they can point to a DPIA, code of practice, the care and attention of company management, anonymization mechanisms, and perhaps external certification, as evidence of due diligence.

The ultimate sanctions in the GDPR, however, are onerous. DPAs are empowered to impose significant administrative fines on data controllers and processors. The fining structure is tiered. In some circumstances, organizations might be subject to fines of up to 20 million euros, or 4% of global turnover, whichever is the higher. Data protection laws are now a lot more costly to ignore.

4. The General Data Protection Regulation: Its extra-territorial impact

The mechanisms to control the transfers of personal data to "third countries" outside the EU are broadly similar to those established under the Data Protection Directive (Arts. 44–50). The Commission has the power to determine whether certain countries, territories, sectors or even international organizations offer an "adequate level of protection" for the data transferred. Those few countries that had been approved as adequate by the Commission will continue to enjoy that status, at least for four years when their status will be reviewed. Other methods for effecting transfers continue to be recognized, including approved standard contractual clauses, binding corporate rules (BCRs) and codes of conduct. The GDPR combines, therefore, the "jurisdiction-to-jurisdiction" approach with the "organization-to-organization" approach to international data transfers.

The standards for assessing adequacy have, however, changed since the decision by the ECJ in the famous Schrems case, that invalidated the EU-US Safe Harbor Agreement (ECJ, 2015). The CJEU noted that the "term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter". The point, according to the Article 29 Committee's analysis, is not to "mirror point by point the European legislation, but to establish the essential, core requirements of that legislation". It is also clear that "any meaningful analysis of adequate protection must comprise the two basic elements: the content of the rules and the means for ensuring their effective implementation" (EU, Article 29, 2017). Attention should also be given to the overall legal framework for access by public authorities to personal data, the issue that precipitated the ECJ ruling and the invalidation of the Safe Harbor agreement in the first place.

The test of adequacy makes a distinction between the "core" privacy principles, additional content principles that might be necessary in regards to particular forms of processing, and procedural and enforcement mechanisms. The latter includes the following elements: a competent and independent supervisory authority (though not necessarily a data protection authority); the assurance of a good level of compliance; measures to ensure accountability; and a system to provide help and support for data subjects and appropriate redress mechanisms. Symbolic data protection statutes, therefore, are not adequate, and they must be embedded within a system that respects the rule of law.

A determination of adequacy, thus establishing a safe harbor for personal data transmitted from the EU, can benefit domestic and multinational companies, and relieve them of having to develop complex case-by-case contractual mechanisms, or BCRs. There are several countries, including Japan and Korea, which are actively promoting their cases for an adequacy determination (Privacy Laws and Business, 2017). And those countries which have this status, including Canada, are trying to determine whether their existing regimes will pass muster, and if not, what reforms would be considered necessary given the higher threshold, and the continuing ambiguity about what are "core" principles, and how the overall effectiveness of the system is to be measured (Bennett, 2016). The EU has continued to establish the global standard for the international transmission of personally identifiable data. In playing that role, it opens itself to all kinds of challenges for acting as judge and jury and jury over the privacy regimes of non-EU countries (Stoddart et al., 2016).

5. Conclusion: A continuing convergence and raising of privacy standards

Transnational instruments for data protection have played three overlapping functions over time. They have acted as *instruments of harmonization*, as templates that any state, or organization, might use in

order to fashion its own data protection policy. They have acted as *exemplars*, producing a progressive and inexorable desire to be within the community of nations that has adopted data protection legislation; the more states that adopt, the higher the pressure on the non-adopters. More recently, they have acted as *a coercive force*, with significant economic consequences for those businesses that rely upon the unimpeded international flow of personal information, and on those governments that wish to protect their domestic industries from the possible consequences of non-compliance. These instruments have built upon each other. They represent a logical progression reflecting the increasing policy interdependence of different countries. The Directive was only possible because of prior agreement on data protection principles within the OECD and the Council of Europe (Bennett & Raab, 2006). By the same token, the GDPR was only possible because of twenty years of experience through the Directive

The GDPR is clearly a significant extension of the global process of policy convergence and trading-up the of international privacy standards. The criteria for convergence are deepening. Policy instruments that were once considered optional methods of implementation and enforcement, and now central to the privacy protection regime and robust tests of international adequacy. There is an increasingly global understanding about what it means for the responsible organization to process personal information in an accountable manner. Adherence to privacy standards is now regarded as a necessary condition for participation in the international, networked economy.

As of 2018, and before the GDPR was implemented, around 120 countries in the world have passed data protection statutes which meet at least minimum standards of formal international agreements (Greenleaf, 2017). It would seem that there are certainly no geographical barriers to diffusion. Privacy protection laws now appear in Latin America, East Asia, Africa, former Soviet-bloc countries, as well as in Western Europe, North America and Australasia. Nor does it appear that privacy protection policy is associated with particular types of democratic governance; parliamentary and presidential regimes, federal and unitary systems have all adopted such legislation. Moreover, some of these countries have experienced quite recent histories of authoritarian rule.

Of course, the existence of law does not ensure its effective implementation. And it is obvious that some of these laws are totally symbolic. The EU is cognizant of these limitations, and is rightly sceptical of data protection legislation passed for reasons of international trade, and in countries that do not have a basic respect for the rule of law. Privacy protection policy is grounded on some basic assumptions that have grown out of Western liberal assumptions about the ability of the individual to control the circulation of his or her personal information (Westin, 1967). The assessment of a "good level of compliance" cannot be divorced from broader political, administrative and cultural factors among some highly divergent jurisdictions.

Furthermore, this deep and extending consensus surrounding the privacy protection doctrine has occurred against a backdrop of some profound skepticism as to whether it can actually protect personal privacy and stem the inexorable tide of surveillance. Is this the diffusion of privacy *protection*, or the diffusion of privacy *law*? Scholars who examine the issue from broader sociological perspectives have continuously argued that contemporary information privacy legislation is designed to manage the processing of personal data, rather than to limit it (Rule, 2007, p. 152). Some also contend that the essential problem is the grounding of these policies within the individualistic and liberal notion of "privacy" which overlooked what is at stake in the broader debate over contemporary surveillance (Lyon, 1994, p. 196). Thus, data protection law does not halt surveillance; it manages it. It may produce a fairer and more efficient use and management of personal data, but it cannot effectively control the voracious and inherent appetite of modern organizations for more and more increasingly refined personal information, especially when those data are central to the business models of the platform economy.

This critique, of course, resonates in the context of the broader debate about mass surveillance, motivated in part by the revelations from whistleblower, Edward Snowden. The extraordinary picture resulting from these leaks of massive surveillance programs perpetrated by out-of-control national security agencies in collaboration with large multinational Internet companies contrasts starkly with the picture painted above of a world increasingly embracing the philosophy and policy instruments of privacy protection (Greenwald, 2014; Lyon, 2015). The global debate about the diffusion of privacy protection is now, therefore, influenced by wider concerns about the role of national intelligence agencies, the warrantless surveillance of Internet traffic (and especially metadata), and the appropriate role for multinational business in assisting law enforcement in its efforts to curb international crime and terrorism. This new reality is reflected in the requirement in the GDPR (Art 45.2) that, in assessing adequacy, the Commission must take into account "relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data as well as the implementation of such legislation".

When we try to assess, therefore, the likely impact of the GDPR on the level of privacy protection globally, the picture is always going to be complex and multi-faceted. The "level of protection" is simply not amenable to precise calibration. That is a rhetorical shorthand device that obscures the multidimensional characteristics of these laws, the inherently subjective nature of the assessment process, and the danger of evaluating the 'black letter of the law' in isolation from broader cultural and institutional factors and conditions (Stoddart et al., 2016). The GDPR, like the Data Protection Directive, will continue to offer an important template of principles and provisions for other jurisdictions to emulate if they wish. Whether or not, however, it will establish the enforceable rules of the road for the processing of personal data in the global networked economy remains to be seen.

Acknowledgments

I acknowledge the very helpful assistance of Smith Oduro-Marfo in the preparation of this article.

References

Asia-Pacific Economic Cooperation (APEC). (2005). *APEC Privacy Framework*. Retrieved from https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework.

Bennett, C.J. (1992). *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Ithaca, NY: Cornell University Press.

Bennett, C.J. (1997). Convergence Revisited: Toward a Global Policy for the Protection of Personal Data, In P.E. Agre and M. Rotenberg, *Technology and Privacy: The New Landscape*. MIT Press, Cambridge, Ma., pp. 99-123.

Bennett, C.J. & Raab, C. (2006). *The Governance of Privacy: Policy Instruments in Global Perspective.* Cambridge: MIT Press.

Bennett, C.J. (2016). *Is Canada still 'Adequate' under the New European General Data Protection Regulation?* Retrieved from http://www.colinbennett.ca/data-protection/is-canada-still-adequate-under-the-newgeneraldata-protection-regulation/.

Bennett, C.J. and Raab, C. (2017). *Revisiting the Governance of Privacy*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972086.

Bygrave, l. (2002). *Data Protection Law: Approaching its Rationale, Logic and Limits.* The Hague: Kluwer Law International.

Cavoukian, A. (2011). *Privacy by Design: The 7 Foundational Principles*. Toronto: Information and Privacy Commission, Ontario. Retrieved from https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.

Constine, J. (2018, April 4). Zuckerberg says Facebook will implement GDPR controls everywhere. *Techchrunch*. Retrieved from https://techcrunch.com/2018/04/04/zuckerberg-gdpr/.

Council of Europe. (1981). *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*. Strasbourg: Council of Europe.

European Commission. (2015). *Data Protection Rules Fit for a digital and globalized age, Press Statement (IP/12/46).* Retrieved from www.europa.eu/rapid/press-release_IP-15-6321_en.htm.

European Court of Justice (ECJ). (2014, May 13). *Google Spain v. Agencia Espanola de Proteccion de Datos (AEPD) 2014, C-131-12*. Retrieved from http://curia.europa.eu/juris/liste.jsf?num=C-131/12.

European Court of Justice. (2015, October 6). *Maximilian Schrems v. Data Protection Commissioner Case C-362/14*. Retrieved from https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A62014CJ0362.

European Union. (1995, October 24). *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data.* Retrieved from http://eur-lex.europa.eu/eli/dir/1995/46/oj.

European Union, Article 29 Working Party. (2017, November 28). *Adequacy Referential* (Updated). Retrieved from http://ec.europa.eu/newsroom/article29/itemdetail.cfm?item_id=614108.

Flaherty, D.H. (1989). *Protecting Privacy in Surveillance Societies*. Chapel Hill: University of North Carolina Press.

Guagnin, D, Hempel L, Ilten C, Kroener I, Neyland D and Postigo H. (2012). *Managing Privacy through Accountability*. London: Palgrave Macmillan.

Greenleaf, G. (2017, January 30). Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey. Privacy Laws & Business International Report, 10-13; UNSW Law Research Paper No. 45. Retrieved from https://ssrn.com/abstract=2993035.

Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA and the U.S. Surveillance State.* New York: Picador.

Lyon, D. (1994). *The Electronic Eye: The Rise of Surveillance Society*. Minneapolis: University of Minnesota Press.

Organization for Economic Cooperation and Development (OECD). (1981). *Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data.* Paris: OECD.

Privacy Laws and Business, (2017). *EU to start adequacy talks with Japan and Korea*. Retrieved from https://www.privacylaws.com/Int_enews_11_1_17.

Raab C. (2011). Networks for Regulation: Privacy Commissioners in a Changing World. *Journal of Comparative Policy Analysis: Research and Practice* 13(2), 195-213.

Rule, J. (2007). *Privacy in Peril: How we are Sacrificing a Fundamental Right in Exchange for Security and Convenience.* Oxford: Oxford University Press.

Stoddart, J. Chan, C. and Joly, Y. (2016). The European Union's Adequacy Approach to Privacy and International Data Sharing in Health Research. *Journal of Law and Medical Ethics,* 44(1), 143-55. Retrieved from http://journals.sagepub.com/doi/abs/10.1177/1073110516644205.

Swire, P. (2013). The Second Wave of Global Privacy Protection: Symposium Introduction, 74. *Ohio State Law Journal 841*. Retrieved from https://ssrn.com/abstract=2404261.

Vogel, D. (1995). *Trading Up: Consumer and Environmental Regulation in a Global Economy.* Cambridge, MA: Harvard University Press.

Westin, A. (1967). *Privacy and Freedom*. New York: Atheneum Zuboff, S. (2015). Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology* 30, 75-89.