Society | DOI:10.1145/3276744 Samuel Greengard

Weighing the Impact of GDPR

The EU data regulation will affect computer, Internet, and technology usage within and outside the EU; how it will play out remains to be seen.

When the European Union (EU) General Data Protection Regulation (GDPR) went into effect on May 25, 2018, it represented the most sweeping effort yet to oversee the way businesses collect and manage consumer data. The law, established to create consistent data standards and protect EU citizens from potential privacy abuses, sent ripples—if not tidal waves—across the world.

GDPR gives European citizens greater control of their data while establishing strong penalties for businesses that do not comply. What is more, any data that involves EU citizens or touches EU companies is covered by GDPR. The initiative replaces an older data privacy initiative called the Data Protection Directive 95/46/EC, which was introduced in 1995.

The implications and ramifications are enormous—and the initiative's reach is global. GDPR will change everything from the way data collection takes place to the way corporate databases are designed and used. It also will potentially change the way research and development takes place, and will impact cybersecurity practices, as well as introducing a practical array of challenges revolving around sites and repositories where groups share comments, information, and other data.

"It's a groundbreaking initiative," says Brett M. Frischmann, Charles Widger Endowed University Professor in Law, Business, and Economics at Villanova University, and Affiliate Scholar of the Center for Internet and Society at Stanford Law School. "Europe has flipped a switch and prompted reconsideration of how data can be collected, managed, and used." The EU takes the position that a person owns his or her data, and their privacy is a fundamental right that is "basic to the integrity of a human being," Frischmann adds.

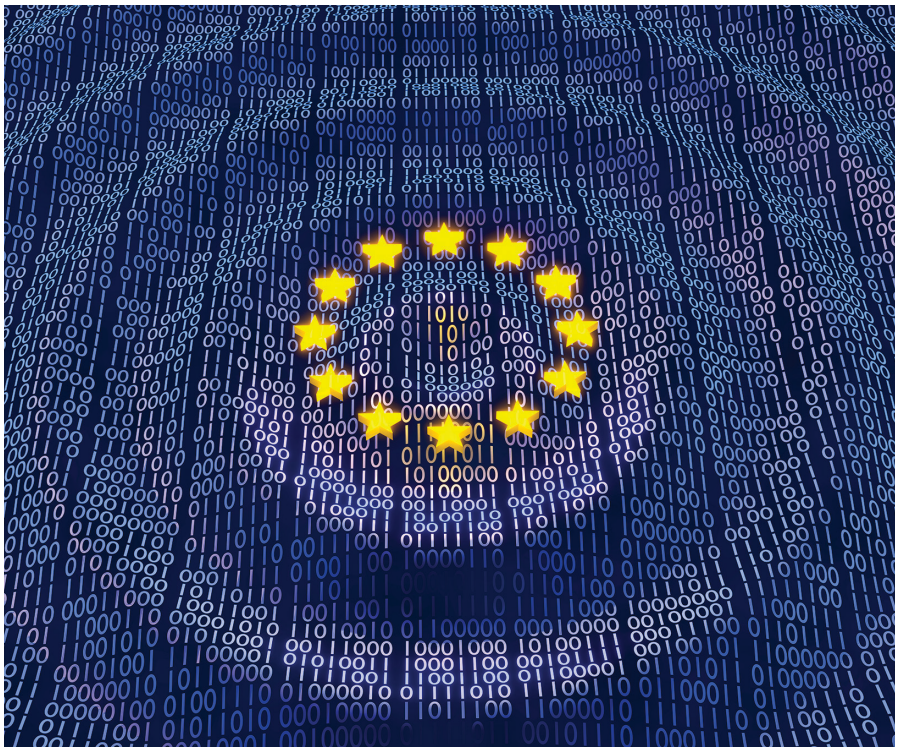

IMAGE BY MIXMAGIC

Data Wars

Digital technology has inexorably changed the face of privacy. Today, there is a perception—and plenty of evidence to support it—that personally identifiable information (PII) is under assault as never before. A Pew Research Center survey found that in the U.S., 93% of adults say being in control of who can get information about them is important; 90% say controlling what information is collected is important. The figures in Europe and other parts of the world are the same.

In a 2016 interview in *Recode*, Europe's Competition Commissioner Margrethe Vestager said, "There is no such thing as a free lunch. You pay with one currency or another—either cents, or you pay with your data, or you pay with the advertisements that you accept. And I think people are becoming more and more aware of the fact that their personal data do have a value."

Says Alison Cool, assistant professor of anthropology at the University of Colorado, Boulder, "There are a lot of questions and ambiguities that must be addressed, but it's clear that GDPR will significantly change the data landscape."

While the U.S. and a number of other countries have adopted an opt-out approach to data collection—essentially, a consumer must instruct a company if he or she doesn't want his or her data used or shared in certain ways—Europe has implemented a more restrictive opt-in approach. However, GDPR takes this concept to a new and previously untested level. Besides giving consumers near-total control of their data, they can have

their data removed from a database or online source at any time and, for those who believe they have been wronged, seek an investigation and join a class-action lawsuit.

Strict rules about how organizations collect, manage, and process data anywhere in the world are only the starting point for GDPR. It allows consumers to file complaints with each nation's national data protection authority, which will investigate the claim. A company that violates GDPR could face a fine of up to 4% of its worldwide annual revenue from the previous fiscal year. The regulation also mandates consumers can remove themselves from a database at any time and take their data elsewhere—to a new bank, a new mobile provider, or a new content service.

Not surprisingly, data scientists, legal experts, and others have radically different perspectives of GDPR. Says Daniel Le Métayer, Senior Research Scientist at Inria (the French Institute for Research in Computer Science and Automation) and a leading authority on data protection and privacy, "GDPR could be a great achievement if properly implemented. It could establish a more concrete framework for data use and protection and help reduce the misuse of personal information."

Adds Cool: "It potentially changes the balance of power. GDPR takes aim at the widely used model of forced consent, which is built on the idea that in exchange for various services, there is an implicit agreement to give up your personal data."

However, there are also plenty of potential pitfalls likely to result from GDPR. Le Métayer says the complexity of GDPR, and the way regulators and courts interpret some of the intentionally vague wording, could create such rigid restrictions that the initiative becomes ineffective over time.

There is also strong opposition in the corporate arena, where the focus is on profiting from data rather than stemming the wave of abuses and breaches. Attorneys such as Tanya Forsheit, partner and chair of the Privacy & Data Practice Group at New York City-based law firm Frankfurt Kurnit Klein & Selz, demonstrate the level of frustration about changes as a result of GDPR. Forsheit describes many GDPR provisions as onerous, and suggests they could be more effectively addressed through self-regulation. "It is simply not possible to be 100% compliant. GDPR forces organizations to devote significant time and expense to comply with standards that are not consistent with the way business is done online," she argues.

GDPR allows consumers to remove themselves from a database or online source at any time; companies violating GDPR face fines of up to 4% of their global annual revenues.

Data Gets Personal

To be sure, the practical challenges of complying with GDPR are significant, especially as digital technology and artificial intelligence (AI) advance.

Personal assistants such as Siri, Alexa, and Cortana add layers of complexity to the issue of PII. Robo-advisors, chatbots, recommendation services, and other automated systems introduce additional compliance challenges. All these systems collect and store data about individuals. In the past, there was no need to determine where a person lived; under GDPR, that could amount to crucial information that would need to be added to each individual data point related to an individual. Even human resources systems, payroll systems, and similar repositories of personal data could be significantly impacted by the regulation; all may require algorithmic auditing processes that revolve around "data protection by design."

Companies already are voicing concerns that GDPR could inhibit innovation by limiting how data is handled in apps, databases, and online services—and how data is used for advertising and other purposes. The issue could impact autonomous vehicles,

Milestones

Håstad Receives Knuth Prize

The 2018 Donald E. Knuth Prize has been awarded to Johan Torkel Håstad of Sweden's KTH Royal Institute of Technology for his sustained record of milestone breakthroughs at the foundations of computer science, with major impact on areas including optimization, cryptography, parallel computing, and complexity theory.

The Knuth Prize is jointly bestowed by the ACM Special Interest Group on Algorithms and Computation Theory (SIGACT) and the IEEE Computer Society Technical Committee on the Mathematical Foundations of Computing (TCMF). The Prize is named for Donald Knuth of Stanford University, the "father of the analysis of algorithms," and is bestowed in recognition of outstanding contributions to the foundations of computer science by individuals for their overall impact in the field over an extended period.

A professor of computer science at the KTH Royal Institute of Technology in Stockholm, Håstad received his bachelor's degree in mathematics from Stockholm University, his master's degree in mathematics from Sweden's Uppsala University, and his doctorate in mathematics from the Massachusetts Institute of Technology.

Håstad's works resolved long-standing problems central to circuit lower bounds, pseudorandom generation, and approximability. He also introduced transformative techniques that have fundamentally influenced much of the subsequent work in these areas.

Previous honors bestowed on Håstad include the ACM Doctoral Dissertation Award (1986), the Gödel Prize for outstanding papers on theoretical computer science (1994 and 2011), and the Göran Gustafsson Prize for outstanding achievement in mathematics.

robotics, and a variety of systems that rely on AI. Organizations may ultimately need to keep two separate databases—one for the EU and one for elsewhere—or find ways to differentiate records in databases.

In addition, GDPR might add a layer of complexity atop an already complex European privacy framework. For example, more than 2.4 million individuals have already submitted "right to be forgotten" requests so they can be expunged from Google searches. Cool says some people believe the law will "hinder innovation by making organizations more risk averse."

Depending on who opts in, who opts out, and what data appears or disappears from a database or other source, the situation could become even more problematic. As Frischmann puts it, "What happens when one person at a group meeting or part of a community invokes a privacy clause but it affects everyone?"

The greatest challenge may be ensuring companies in the EU and beyond adhere to the spirit of GDPR. Many companies lack expertise in how they will need to implement and manage data under GDPR; they also do not know the levels of expertise or staffing required to conduct crucial data protection impact assessments.

"If businesses view GDPR as a checklist activity rather than an issue that requires ethical reflection—and if they look to exploit loopholes and skirt the intent of the law—the long-term outcome could be negative," Cool says. "When you look at groups like bioethicists and physicians, the starting point for discussion is how to do the right thing for society; it's not about avoiding getting sued or how to sidestep legal and ethical provisions."

Cracking the Code on Privacy

How GDPR will play out is anyone's guess. The initiative could revolutionize the data landscape—or it may fizzle into a footnote in digital history. It could also change the way the Internet works and how data and information flow across sites, clouds, and more.

One wild card is how consumers react to GDPR. If large numbers of people revoke access to PII or challenge the way companies use their data, businesses may reach an inflection point where they will have to rethink the fundamental way they approach and navigate data management, or reevaluate the fundamental value of data and how it is monetized. GDPR also might mandate new tracking and data management tools, such as blockchain.

Above all else, GDPR represents the ongoing battle between unfettered capitalism and human dignity.

Le Métayer argues that businesses need to address complex issues such as conducting data protection impact assessments and implementing data portability, which requires agreeing on standard data formats. Other sources of uncertainty include the compatibility of GDPR with big data, and the rules concerning automated decision-making. Article 22 of GDPR states individuals have the right to "not be subject to a decision based solely on automated processing, including profiling." GDPR also allows consumers to contest a decision, but it is not clear what type of explanations should be provided to make this right effective. "The issue is also technical, since providing useful explanations about certain types of algorithms is a challenge in itself," he says.

GDPR could also prompt companies to directly pay for PII data, Frischmann says. "If the power balance shifts and consumers gain leverage over their personal data, companies may look to provide incentives, discounts, and direct compensation for the use of data. It could flip the current model and even lead to entirely different ways to approach data," he explains.

In fact, a recent study conducted by digital marketing agency Syzgy in Germany, which polled 1,000 respondents each from the U.S., U.K., and Germany, found citizens in all three countries would sell their data for between €130 (about US$150) and €140 (US$165) per month.

One thing is certain: amid a litany of security breaches and breakdowns, from Equifax to Cambridge Analytica, there is a growing focus on data privacy. What is more, other government entities are exploring ways to control how data is collected, managed, and used. In the U.S., the State of Vermont enacted a law in May 2018 that established standards for data. California is now eyeing an initiative—the California Consumer Privacy Act—that could extend many of the same GDPR protections to the state. Other countries, from Australia to Japan, have also revised data standards and privacy controls in recent years.

Frischmann says GDPR, above all else, represents the ongoing battle between unfettered capitalism and human dignity. The whole point of it is that it is not designed to be an efficient regulation for businesses. "To some extent, it's about a person's ability to exercise their own free will about their life."

Cool says that, in the end, it is vital to strike a balance between privacy and laws. "We need more research that looks carefully at how personal data is collected and by whom, and how those people make decisions about data protection. Policymakers should use such studies as a basis for developing empirically grounded, practical rules." C

Further Reading

Wachter, S., Mittelstadt, B.D., and Russell, C.
Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR, *Harvard Journal of Law & Technology*, 31 (2), 2018. November 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3063289

Casey, B., Farhangi, A., and Vogl, R.
Rethinking Explainable Machines: The GDPR's 'Right to Explanation' Debate and the Rise of Algorithmic Audits in Enterprise, *Berkeley Technology Law Journal*. February 19, 2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3143325

Kaltheuner, F. and Bietti, E.
Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR. *Information Rights, Policy & Practice Journal*, Vol. 2, No. 2. 2017. https://journals.winchesteruniversitypress.org/index.php/jirpp/article/view/45

Samuel Greengard is an author and journalist based in West Linn, OR, USA.

© 2018 ACM 0001-0782/18/11 $15.00