The Digital Economy & Privacy Protection: the Challenges Ahead

Author Marc Rotenberg

By Marc Rotenberg

The transformation is taking place rapidly. Services and sectors that were once distinct are now being joined together through digital networks. The thermostat in a home now connects to a cell phone. A car is connected to a computer network. A camera at a street corner broadcasts images to a police station far away.

These changes, brought about by the digital revolution, have also brought about far-reaching questions of law and policy. Some of the challenges are familiar — will automation lead to unemployment or will it create new, more advanced jobs? What is the appropriate balance to promote innovation while safeguarding important rights, such as privacy? Some questions appear new — should robots or their designers be responsible for the consequences of their acts? Does artificial intelligence (AI) mean that we can no longer assess the basis of outputs generated by automated procedures? For governments, business leaders, and representatives of civil society these problems are real and complex.

As new technologies converge in this information-enabled economy, I propose a central focus on transparency and accountability. The American inventor Thomas Edison once remarked, "What we create with our hands, we must control with our head." It is good advice as we explore this rapidly changing world.

The Internet Age & the Protection of Privacy

Over the past two decades, we have witnessed the rapid change brought about by the Internet. The transition from a centralized voice network to a distributed data network has made possible the emergence of new businesses, new government services, and new forms of economic activity. But the Internet economy has also brought with it growing concerns about the loss of privacy, financial fraud, and identity theft. In the United States, the Federal Trade Commission (FTC) reports that identity theft is the second-biggest concern of American consumers, just behind debt collection (FTC, *Annual Summary of Complaints Reported by Consumers*, March 1, 2018). Data breaches are on the rise in the US, as there in much of the world, and there is growing concern that the attacks on personal data, stored by well-established companies with a commitment to privacy and security, are engineered by foreign adversaries. Again, the US has a warning tale for other countries. In 2015, the government records of 22 million federal employees, their friends, and family members were breached by foreign adversaries. The records disclosed included also the 5 million digitized fingerprints, the unique authenticating details upon which security and financial transactions rely.

There is, therefore, real urgency to ensure that governments establish comprehensive programs for privacy and security to safeguard the personal data that is stored by both the private sector and government agencies. Central to the structure of modern privacy law are "Fair Information Practices", the rights and responsibilities associated with the collection and use of personal data. The allocation of rights and responsibilities is necessarily asymmetric because the individual loses control over the use of personal data when it is transferred to another party. That is why organizations in possession are responsible for its protection. It is also the reason that individuals are given rights when their personal data is breached, misused, or expropriated.

There is also a need to develop, what I have called, "Privacy Enhancing Techniques" that minimize or eliminate the collection of personally identifiable information (Testimony of Marc Rotenberg, United States Congress, *Privacy in the Commercial World*, March 1, 2001). Such techniques include stored-value cards for transportation and communications that enable services without capturing the identity, or placing at risk the personal details, of the user. Robust techniques for de-identification and anonymization also permit the use of aggregate data and minimize the risk to the individual.

The European Union has taken a leading role in the development of a new legal framework to address the data protection challenges of the Internet age and to encourage the development of innovative techniques to provide consumer safeguards while safeguarding privacy and identity. The General Data Protection Regulation (GDPR), which went into force in May 2018, sets out a comprehensive approach to privacy protection. The GDPR builds on the Data Protection Directive of 1995 which was the first international framework for data protection.

The Japanese Act on the Protection of Personal Information, which came into force in May 2017, is part of the effort to build privacy frameworks that establish trust and confidence in the digital economy. Although there are some differences in the EU approach and the approach in Japan to data protection, the two frameworks have much in common. At a historic meeting in July 2018, the EU and the Japanese government agreed to work together to provide protection for personal data. Such an agreement will avoid the need for complicated business arrangements, such as standard contractual clauses, binding corporate rules, or privacy certifications.

The outcome will be the largest trading region in the world for the exchange of digital information with legal assurances of privacy protection. While it is too soon to evaluate whether the laws are sufficient or what new challenges may arise, both the EU and Japan are to be commended for this important step forward in the evolution of data protection.

The Internet of Things (IoT)

Still, the new challenges ahead are substantial and worrisome. The Internet has made possible not only the transfer of personal data across national borders, it has also connected physical devices to electronic networks on a mass scale making possible both the remote monitoring of machinery and services and also remote hacking. For example, in March 2018, Atlanta, Georgia suffered a ransomware attack that crippled the city's ability to provide services and to collect payments. City employees had been instructed to disconnect computers and perform their jobs manually.

In 2017, hackers using a ransomware program called "WannaCry" infected more than 300,000 computers worldwide, crippled the National Health Service in the United Kingdom, and disabled numerous international companies, including Federal Express. Hackers have demonstrated the ability to remotely deactivate the brakes on an Internet-connected car, disable door locks at a hotel, and adjust thermostat settings in networked home devices. Security experts, such as Bruce Schneier, have warned that we are seeing only the beginning of the risks of Internet-connected devices (*Click Here to Kill Everybody: Security and Survival in a Hyper-connected World Book*, by Bruce Schneier, W. W. Norton, New York, 2018).

Unlike the early challenges, which focused on privacy and data protection, these new challenges increasingly implicate public safety. Current safety regulations should be extended to take account of the risks of Internet-connected devices. The National Cyber Security Centre in the UK, perhaps drawing on the lessons from the attack on the NHS, urged the adoption of new measures to boost cyber security in Internet-connected devices. Critically, "manufacturers of 'smart' devices will be expected to build-in tough new security measures that last the lifetime of the product." (National Cyber Security Centre, *Secure by Design*, March 2018). This approach follows also earlier recommendations from the Aspen Institute 2015 conference on communications policy which recognized the ongoing risk that consumer devices would likely become more vulnerable to attack over time and that it was therefore necessary to establish a robust security plan for the lifetime of the device.

The US has been slow to recognize the growing threat of the IoT. The Consumer Product Safety Commission, the agency tasked with protection for consumer products, has stated that the security of Internet-connected devices falls outside its domain. It is a surprising conclusion when products such as Google Home Mini are produced with a manufacturing defect that permitted remote monitoring of conversations within the home with no action by the user (CNN, *Google admits its new smart speaker was eavesdropping on users*, Sept. 11, 2017).

In contrast, the response in Europe to Internet-connected dolls appears very different. After a Norwegian consumer organization determined that the toy "My Friend Cayla" allowed the remote monitoring and recording of a child's conversation, European regulators responded quickly (Forbrukerradet, *Connected toys violate European consumer law*, Dec. 6, 2016). The German consumer agency banned the dolls and warned families that had purchased them to destroy them. The French data protection agency, the CNIL, warned the company that sanctions would be imposed if safeguards were not established.

Competition & Innovation

Another challenge facing societies today concerns the relationship between data protection and both competition and innovation. It is certainly true that personal data enables scientific innovation, medical breakthroughs, and the more efficient delivery of government benefits and private sector services. But the general proposition that data is useful does not answer the question whether firms should have unrestricted access.

Consider, for example, the decision by regulators to approve Facebook's acquisition of the popular messaging service WhatsApp. At the time the deal was proposed Facebook and WhatsApp offered competing services though with very different business models. Facebook relied on the advertising derived from knowledge of the user's interest and was able to offer the service, without much privacy, at no cost. WhatsApp chose instead to rely on a subscription model that offered strong protection for users but also required a small annual payment. Internet users had a choice of two messaging services.

Facebook's acquisition of WhatsApp created a real problem for regulators. In Europe, Facebook assured the European Commission that it would be unable to join the data sets of the two firms. In the US, Facebook told regulators it would respect the privacy commitments that WhatsApp had made to its users and not use personal data for advertising purpose. Both statements turned out not to be true. In fact, Facebook could join the data sets and did

indeed plan to break the commitments to Internet users WhatsApp had made. The Commission fined the company 110 million Euros (New York Times, *E.U. Fines Facebook $122 Million Over Disclosures in WhatsApp Deal*, May 18, 2017). In the US, it remains unclear whether the FTC will impose any sanctions on the company.

Putting aside the business ethics associated with Facebook's acquisition of WhatsApp, it is important to consider whether such mergers promote data protection, innovation and competition, or whether the outcome is the opposite. Speaking at the World Economic Forum in Davos earlier this year, the American investor George Soros offered a clear warning about the future direction of the Internet economy, noting that Internet companies have often played an innovative and liberating role but also observing "as Facebook and Google have grown into ever more powerful monopolies, they have become obstacles to innovation, and they have caused a variety of problems of which we are only now beginning to become aware." Soros has proposed "the fact that they are near-monopoly distributors makes them public utilities and should subject them to more stringent regulations, aimed at preserving competition, innovation, and fair and open universal access."

I share his views. Increasing consolidation of Internet companies is not only bad for data protection, it has also stifled innovation and competition. Government regulators should be particularly skeptical of claims that joining mass troves of personal data will lead to further innovation. I have already described the growing risks of data breaches and the growing threats from foreign adversaries. After the mistaken decision to allow Facebook to acquire WhatsApp, we see also a collapse in competition in a key market for Internet services (*The Facebook-WhatsApp Lesson: Privacy Protection Necessary for Innovation*, Techonomy, May 4, 2018).

Algorithmic Transparency & Accountability

Among the greatest challenges today in the digital economy is also one of the most familiar challenges in modern privacy law: how to ensure the fairness, accuracy and accountability of decisions concerning individuals? This central concern, more so than secrecy or confidentiality as privacy is often understood, is also at the core of our modern right to privacy. Throughout the world privacy laws guarantee individuals with the right to know what information about them is held by others and how it will be used. Banks in the US, for example, have an obligation to explain the reason that a loan application was denied. And consumers are entitled to know the general factors that are considered in the creation of credit scores. But the precise factors, and the weight they are given, when consumers are evaluated for loans and other commercial opportunities have never been made available with much precision. That will soon change.

With the adoption of the GDPR and the updated Privacy Convention of the Council of Europe, a new effort is underway to make transparent the algorithms that make decisions about consumers in the marketplace, that determine the placement of news on Internet platforms, and that make decisions in the criminal justice systems. Provisions of the GDPR now require that individuals be given an explanation and access to the logic of automated processing. Newly required data protection impact assessment will also require data processors to assess the use of rule-based decision-making. And the Council of Europe seeks to ensure that the protection of human rights and democratic values remain at the forefront of public policy concerning AI and algorithms (Council of Europe, Algorithms and AI Development, https://www.coe.int/en/web/freedom-expression/algorithms-and-human-rights).

Japan is now a leader in the effort to establish a comprehensive framework for the use of AI. Beginning in 2016, Japan urged the adoption of global policies for AI at the meeting of the G7. At the time, communications minister Sanae Takaichi described an international set of basic rules for developing AI (The Japan Times, *Japan Pushes for Basic AI Rules at G-7 Tech Meeting*, April 29, 2016). The "AI R&D Principles" seek to "achieve a human-centered society where all human beings across the board enjoy the benefits from their life in harmony with AI networks, while human dignity and individual autonomy are respected." (The Conference Toward AI Network Society, Draft AI R&D Guidelines, July 28, 2017). The Principles address such issues as collaboration, transparency, controllability, safety, security, privacy, ethics, user assistance, and accountability.

There is growing support for this approach among the member countries of the Organization for Economic Cooperation and Development. Scientific societies also support the effort to establish a global framework for AI. The Association for Computing Machinery, one of the world's largest computing societies, has stated, "the ubiquity of algorithms in our everyday lives is an important reason to focus on addressing challenges associated with the design and technical aspects of algorithms and preventing bias from the onset." (U.S. Public Policy Council of the Association for Computing Machinery, *Statement on Algorithmic Transparency and Accountability*, Jan. 2017). The IEEE-USA has said, "Effective AI public policies and government regulations are needed to promote safety, privacy, intellectual property rights, and cybersecurity, as well as to enable the public to understand the potential impact of AI on

society." (IEEE-USA, *Artificial Intelligence Research, Development and Regulation*, Feb. 10, 2017). And the European Commission recently appointed 52 experts to a new High Level Group on Artificial Intelligence, with broad representation from academia, business, and civil society. The group will examine "issues such as fairness, safety, transparency, the future of work, and more broadly the impact on upholding fundamental rights, including privacy and personal data protection, dignity, consumer protection and non-discrimination." (European Commission, *Commission appoints expert group on AI and launches the European AI Alliance*, June 14, 2018).

There is also support in the US. Former US presidential candidate Michael Dukakis has called for a global accord on AI. Governor Dukakis has recently launched the Artificial Intelligence World Society to make AI "safe, trustworthy, transparent, and humanistic" (The Michael Dukakis Institute, *Boston Global Forum and Michael Dukakis Institute will recognize two world leaders for achievements in Artificial Intelligence (AI) this April*, https://dukakis.bostonglobalforum.org/tag/aiws/). The proposals set out by the AIWS build on the recommendations of the Japanese government set out at the G7 in 2016.

Algorithmic Transparency

We at the Electronic Privacy Information Center (EPIC) welcome these developments. We first urged recognition for Algorithmic Transparency at the OECD Global Forum for the Knowledge Economy in Tokyo in 2014. We explained then that companies are too secretive about what they collect and how they use personal data. We called for the swift enactment of the Consumer Privacy Bill of Rights and the end of opaque algorithmic profiling.

The progress over the last several years is notable. But so too are the new challenges. In May 2017, EPIC urged the FTC to investigate a company that had launched a new commercial service for the secret rating of young athletes. We explained that neither the athletes nor their families could determine how these scores were assigned and that the rating system could determine not only success in sports, but also educational opportunities and scholarships. We said that it was very unusual to assign secret scores to athletes as most athletic achievement, whether measured in time or distance, is objective, public, and easily verified. We pointed also to the ELO system, the non-proprietary, scientific technique used to rate chess players that has been adopted in other activities.

More than a year has passed since we filed our complaint and still there is no action from the FTC. The secret and unaccountable scoring of young athletes continues. Moreover, concerns are growing over the possibility that government will adopt techniques to score citizens. In China, for example, a social scoring system is underway that will create detailed profiles and ratings for each person in China. The rating system will determine opportunities for individuals in education, employment, housing, travel, and more. We believe such a government rating system is contrary to the principles of individual liberty and democratic society. There is even a risk that countries that create such systems may lose control over their creation as the systems become more complex and more decision-making is delegated to machines.

The Public Voice

This brings us then to our final challenge of data protection in the information age — to ensure that the public has a meaningful voice in the decisions made by government about the deployment of AI techniques. Earlier this year, EPIC submitted a formal petition to the US Office of Science and Technology Policy urging the creation of a public process to the development of AI policy for the US (EPIC, *Scientific Societies Call for Public Input on U.S. Artificial Intelligence Policy*, July 3, 2018), Leading scientific organizations in the US, including the American Association for the Advancement of Science, the Association for Computing Machinists, the Federation of American Scientists, and the IEEE, have joined the EPIC petition. Together we believe it should be possible to create policies to govern the use of AI that will preserve the dignity, autonomy, and freedom of the individual. And we have reported our call in statements to the US Congress.

We are therefore at a critical moment in our ability to regulate the technologies we create. The EU and Japan have put forward important legal frameworks to update protections for privacy in our digital age. We see also the new threats arising from the IoT, the growing concentration of Internet companies, and the increased dependence on AI techniques for a wide range of government and private sector services.

It would be a mistake to assume that either technology or markets alone will solve these challenges. Wise public policy, guided by evidence and meaningful public participation, is the key to our digital future. JS

Marc Rotenberg is president of the Electronic Privacy Information Center in Washington, DC, a non-partisan research center that focuses on emerging privacy and civil liberties issues. He has served on expert panels for the American Association for the Advancement of Sciences, the American Bar Association, the Aspen Institute, the International Working Group on Data Protection, the National Academies of Sciences (US), the OECD Science, Technology, and Innovation Directorate, the US Senate, and UNESCO.