Promoting innovation, protecting privacy

Written by: Marc Rotenberg, President and Executive Director of the Electronic Privacy Information Center, Washington DC

Last update: 9 March 2017

© Anna Berkut/Alamy

Few issues are of greater concern to Internet users today than privacy protection. Everyone wants the benefits of Internet access, but few want to sacrifice their privacy or face the risk of cyber theft as a consequence.

According to a recent poll, an overwhelming percentage of people believe that their information is not private. They want new rules about how companies and governments can use online data about them. Its global survey found that 83% believe new rules are required to compel governments and companies to handle data more responsibly, whether personal or medical data, or data picked up on social websites or other platforms where people routinely engage.

A recent report found the rate of data breaches accelerating and the cost to business and consumers increasing. Clearly action is needed. But while governments have a critical role to play, they should be careful of the policy traps that have littered the privacy field in the past.

First, "balancing" is a popular term in the policy world. But balancing privacy protection with the availability of new services is the wrong starting point. Users want both innovation and privacy protection. They should not be asked to trade-off basic protections for new services. Governments and businesses should make a commitment to achieve innovation and robust safeguards for personal data.

Second, "notice and choice"–presenting boilerplate terms and conditions that users are expected to accept–is a bad choice for privacy policy. In the Internet

economy, the markets for personal data are two-sided. Companies stand between the users and the advertisers. Internet firms collect personal data and then sell the user preferences to the advertisers. The user is not the customer, but the product. And the very large firms that dominate search and social networking provide little opportunity for users to switch service providers because they are no real alternatives. Traditional market mechanisms, built upon transparency and competition, simply do not exist for the end user seeking to protect privacy. That is why it is critical to establish baseline privacy standards as the foundation for the Internet economy.

Third "interoperability" is also a policy dead end online privacy. The global network brings together consumers and businesses from around the globe. The key to online privacy are common standards for data protection that simplify data exchanges and provide trust and confidence in new services. End-to-end encryption, data minimisation, and Privacy Enhancing Techniques– not "interoperability"–are obvious solutions to many of the privacy and security challenges facing users today. Regrettably as user concerns about privacy have increased, and the risks of data breach and data theft have grown, many governments have followed these insufficient strategies, which have only increased public concerns.

The good news is that the OECD has been at the forefront of efforts to promote good policies and good technologies to promote growth and innovation while safeguarding privacy since the early days of the Internet. The OECD Privacy Guidelines of 1980 remain one of the most influential data protection frameworks in the world. The OECD Privacy Guidelines have provided the basis for national law and international agreements. For example, in the United States the OECD Privacy Guidelines provided the basis for the privacy law to protect the personal information of subscribers to cable television services. Of the many privacy laws in the United States, the subscriber privacy provisions in the US Cable Act are among the very best.

Now coupled with some of the recent innovations in privacy policy, including data minimisation and breach notification, the 1980 OECD Privacy Guidelines remain a good starting point for policymakers developing legal frameworks for privacy protection.

The OECD also promoted the use of robust encryption with the OECD Cryptography Guidelines in 1997. Encryption is a critical data security technique that has helped make possible the growth of the commercial Internet. No doubt crypto will pose some challenges for government, such as concerns about access to data of targets of criminal investigations. But the costs of poor security measures are also very real. Data breaches continue to rise, leading to identity theft and financial fraud. Many companies are collecting data they simply cannot protect. Governments should actively promote strong encryption particularly for

cloud-based services, because it is not possible for users and businesses to monitor the security standards of those who store data remotely.

Of course, hi-tech firms are not waiting for policy makers to solve these problems. Companies such as Apple and WhatsApp have decided to build in strong security techniques to protect the data that has been entrusted to them by their users. These companies should be supported for addressing privacy challenges.

Protecting the interests of citizens is a key responsibility for governments, yet many governments have experienced data breaches, including medical records, tax records, and even voting records. The Internet drives innovation, productivity growth and communication. But it is also a harbinger of data breaches, identity theft, and financial fraud, all of which have trended up during the Internet era. Users are rightly concerned about the protection of their personal information. And the indicators all suggest the problems will accelerate over the next several years.

Governments have a central role to play, but they should avoid hollow solutions, slogans, and failed strategies. If they want the digital economy to grow strongly, there is serious work ahead.

For more on privacy, visit EPIC.org. For more on civil society and the digital economy, visit CSISAC.org