Should a "Digital Bill of Rights" be adopted? If so, what rights, protections, and obligations should be established within this framework for protecting data privacy?

Pris Regan

Over the last ten years or so, there have been several iterations of a "Digital Bill of Rights." Most model themselves on the original Bill of Rights in that they include 10 so-called rights. Most also include rather lofty ideals or goals and operate at a high level of abstraction. One of the earliest "Digital Bill of Rights," proposed in 2012 by Representative Issa (R-CA) and Senator Wyden (D-OR), includes: rights to a free, uncensored, open and unobstructed Internet; rights to share ideas, to access equally, to participate, to create, grow, collaborate and be held accountable, and to freely associate; a right to privacy; and a right to what they create and be secure in their intellectual property. In 2018, Representative Ro Khanna (D-CA) penned an Internet Bill of Rights that is somewhat more concrete and includes: access to and knowledge of the collection and use of personal information; opt-in consent for collection of personal information; a right to correct or delete information where context appropriate and with a fair process; data security and notification of data breaches; data portability; net neutrality; no unnecessary data collection for internet service; access to multiple platforms, services and providers with clear and transparent pricing; no discrimination based on personal data; and reasonable business practices and accountability. And in 2019, the Free Press, a non-profit, issued a Digital Bill of Rights that it asks presidential candidates to endorse which is quite concrete with clear policy actions including: net neutrality with passage of the Save the Internet Act of 2019; restoration of the FCC's Lifeline program; promotion of media ownership diversity; prohibition of social media monitoring by law enforcement agencies without Fourth Amendment protections; and support for comprehensive privacy legislation.

All of these rights, protections and obligations are legitimate and important to foster the development of an Internet that reflects the importance of online activities for public and social purposes rather than for commercial and financial purposes. But there are at least two problems with framing discussion and policy regarding roles and responsibilities in terms of rights. The first is that rights often imply a black and white, all or nothing, approach – either one has a right or one doesn't – that is unrealistic in general and definitely unrealistic given the complexity of the online environment. The second is that none of these rights is meaningful unless there is some effective means of enforcement; otherwise, these are rights without a remedy. And, given the social and public importance of these rights, the remedy should not be individual enforcement but enforcement by public bodies.

Frank Reeder

Whether we need a "Digital Bill of Rights" seems to me to be almost a rhetorical question. There has been a virtual consensus on the need for such a shared set of principles governing the collection and use of personal data since the publication of

- the U.S. Department of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens in 1973; and

- the OECD's 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. (See OECD's 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

(See https://simson.net/ref/2004/csg357/handouts/01_fips.pdf for a brief summary of each.)

Early efforts to legislate on information privacy were focused on the state – we had all read Orwell's *1984* and were reading about governmental internal security agencies like East Germany's Stasi and the Soviet Union's NKVD. While the power of governments to violate individual rights remains a concern - witness the Chinese' government's recently reported efforts to build a facial recognition database – we have long understood that technology gives private actors the ability to abuse individual rights.
The U.S. national approach has largely been sectoral –the Privacy Act of 1974 for the Federal government, the Family Education Right to Privacy Act for education, the Fair Credit Reporting Act and the Gramm-Leach Bliley Act for credit and financial organizations, HIPAA for the health information sector. Two are agency specific – the strict confidentiality provisions in the Census statute and the Internal Revenue Code. All of these well-intended laws fail on two counts: (1) they apply to defined organizations, not to the information; and (2) they have not kept up with the nature of the threat. They did not contemplate the breakthroughs that have allowed information powerhouses like Google, Amazon and Facebook to exploit their information holdings, all of which collect vast stores of sensitive personal information and none of which is subject to any of the foregoing set of laws.

Privacy advocates and policy-makers have not been standing still. In 2016, the European Union adopted a broadly-based General Data Protection Regulation – the notices you have seeing on web sites advising you of a site's use of cookies are the result of that statute. More importantly, the EU imposes stiff sanctions. Most recently, California enacted the California Consumer Privacy Act, which goes into effect on January 1, 2000, the nation's first comprehensive and ambitious privacy laws. It is modeled on the GDPR.

In my view, any privacy regime going forward must, at a minimum embody the following principles:

- transparency - full disclosure of how information is used
- anonymity
- choice – most rules to date allow those who collect information to make use limitations subject to opt-out; i.e., user consent. Thus, under the Family Education Right to Privacy Act a student-applicants may waive their right to see letters of recommendation. In my opinion, such consent provisions are meaningless, since one who is seeking a benefit is hardly exercising choice.
- the right to be forgotten

Perhaps most challenging, any new policy regime must include real, meaningful sanctions.

How can we more effectively and efficiently safeguard personal data, prevent data breaches, and protect data from cyberattacks (including ransomware)?

Pris Regan

Responsibility here rests with both individual users and the organizations with which we deal. As individuals, there are numerous steps we can take to protect our data including: limit the amount of information that we divulge online, avoid retention of information for convenience on our return to a website, avoid signing into websites through a Google or Facebook portal, and regularly delete cookies and clean browser history. All of these steps are fairly obvious and relatively simple – but they also add a step or two to the user experience and therefore are seen as inconvenient. Websites rely on users' willingness to disclose information and sidestep security for their convenience. So, a large part of more effective online security is changing the mindset of users so that they realize that more convenience generally equals less security.

No matter how diligent users are, they are still dependent on organizational security practices. Lax organizational practices come in many forms, increasing the likelihood of cyberattacks and data breaches. In many organizations for ease of internal operations, multiple databases are relatively open to most employees and users often bring their own devices to access work systems -- but as a result databases and networks become open to hackers. Schools have become particularly vulnerable to ransomware attacks as teachers, students and administrators have become more reliant on technology. It's been reported that more than 500 schools in the US were victims of ransomware virus attacks, with most having to pay the ransom in order to get their systems up and running again. Encryption of data and strict security practices are needed but the first is expensive and the second is hard to implement with so many users. Poor security protocols leave organizations open to data breaches, as was the case with both the OPM data breach in 2014 when the personnel records of 4.2 million current and former federal employees were stolen and also the Equifax breach in 2017 when the personal information, including Social Security numbers and credit card information, of over 140 million consumers was stolen. Strict security practices need to become a priority for organizational leaders and part of the organizational culture for employees. But, once again, tighter security slows down the ease of use – and entails an additional financial cost.

Frank Reeder

A complete answer to this question as posed would require a lengthy dissertation on what constitutes good/best security practices. Much work has been done in this space and I would assert that most if not all breaches are the result of failure to follow well-understood sound security practice. Organizations that do not rigorously observe those practices are guilty of malpractice. Among the leaders in this space is the Center for Internet Security, a not-for profit dedicated to identifying and disseminating that knowledge. [https://www.cisecurity.org/cybersecurity-best-practices/] (Full disclosure: I am a Director Emeritus and Founding Chair of the Center for Internet Security)

For individuals, there is similarly a basic set of good security practices. *Consumer Reports* continues to be an authoritative source of advice on good practices. In that regard it is important to understand that, as with any risk, absolute safety (or prevention) is an ideal, largely unattainable goal so any robust security regime must include recovery, not just prevention. In the cyber world, that means, for example, maintaining back-ups of critical, irreplaceable information AND periodically whether they are working. For most us, interestingly enough, that is probably digital photographs.

Specifically, to the matter of data breaches, recent history suggests that the question is not whether, but when our information will be breached. The worst consequence of a breach for individuals is the use of their stolen personal data (e.g., Social Security numbers) to steal one's identity and create accounts, usually loans. In the short term, a reasonably effective way of preventing identity theft is a credit lock with all of the credit-reporting agencies. With a credit lock, an organization seeking to "ping" your information to open a new account is blocked unless you have granted permission. That is why organizations that have had a breach invariably offer credit monitoring services. It is admittedly inconvenient when one is applying for a new account but the safety, in my view, outweighs the occasional inconvenience.

From a public policy perspective, apart from adopting stricter security and privacy rules and sanctions (e.g., the EU GDPR), there is a simple fix. Rather than enacting breach notification laws that result in flurry of notices that, in most instances, are unnecessary and to which consumers are becoming immune, require credit reporting agencies to notify individuals when their information is inged – essentially lock by default.

How can the regulation of both the public and private sector's collection and utilization of personal data be improved?

Pris Regan

At this point, "regulation" of personal data in the US is not "regulation" in any traditional sense but "self-regulation" and has not been at all effective in addressing the problems posed by what has become ubiquitous collection and use of personal data. The public sector's data practices are subject to the Privacy Act of 1974, which entails compliance with certain principles and practices, as well as periodic reporting to the Office of Management and Budget. The Federal Trade Commission (FTC) is regarded as the closest institution to a data protection body in the United States. The FTC's authority, extending only to private sector organizations, is based on its jurisdiction over "unfair and deceptive trade practices" and is able to investigate complaints and issues fines. It does not have traditional rule-making authority and therefore is a reactive, rather than proactive agency. A critical improvement would be to give the FTC rule-making authority along with enforcement powers. Alternatively, and in my opinion preferably, the US could establish a new agency with regulatory authority over the personal data practices of both public and private organizations.

What adjustments to current statutory and regulatory frameworks are needed to keep pace with emerging technologies?

Pris Regan

One of the main concerns with legislating to protect personal data has been the challenge of writing laws that addressed the problem at hand but were also flexible to also address technological changes. Additionally, one of the main arguments against regulation has been that regulation will stifle innovation. Neither of these concerns is compelling. Congress can write laws that are sufficiently robust, effective, and flexible. And there is no evidence that regulation stifles innovation – and the lack of regulation in the 1980's and 1990's spawned the commodification of personal information on the Internet and the easy surveillance of our online activities.

Two "emerging" technologies, although both are actually current technologies, which are most in need of regulation are artificial intelligence (AI) and mobile technologies. AI is now integrated into decision-making in a range of contexts including health care, education, criminal justice, financial services, and social benefits. Often this has occurred without a full vetting of the risks and benefits but with an assumption that AI technology will speed decision-making, free personnel for other tasks, and provide more accurate and precise outcomes. The potential downsides of using AI – including possible bias or discrimination and questions about the locus of accountability for decisions based on AI – need to be fully and publicly debated and addressed in regulation that should include close auditing of AI systems.

Mobile technologies have become part of the fabric of modern life with 96% of Americans owning a cell phone according to a June 2019 Pew survey. People use their cell devices to access and organize all aspects of their lives. A number of policy issues need to be more fully addressed with respect to cell phones – including their default security and privacy protections, the degree of tracking of individual movements and activities that is enabled by mobile phones, and the security and privacy risks posed by mobile apps.

Costis Toregas

The lament of technologists and policy makers alike is the reality that the speed of legislation may never (and for good reason) match the speed of technology innovation. Many call this the Science Policy interface, and try to organize robust dialog around its creative resolution. Questions abound in such discussions:

- ➢ Who should be invited to the table? Scientists talk what sounds like unintelligible jargon when the receiver is a lay person, and policy makers have limited attention span made necessary by concerns over a huge number of issues
- ➢ What can be the role of legislation in impeding or modifying the course of technology innovation?
- ➢ Is it appropriate of government to interfere with market forces and become "king makers" in particular technology niches?

- How can this Grand Challenge dovetail, support or break new ground from existing efforts such as the proposed privacy bill of CDT, State of California's CCPA and Europe's GDPR (see here for a comparison of the last three)

For these and other equally compelling reasons, the Grand Challenge of the National Academy of Public Administration related to Privacy and Security could be an optimal Science/Policy platform to engage in this discussion. Meetings are planned and papers will be issued- so stay tuned for ways to engage. Here is the opening salvo - please let me know of your ideas!

How should agencies leverage administrative data consistent with privacy protections to improve public services?

Costis Toregas

The digital revolution that started in the last two decades of the 1900s and continues with fury in the 21 Century has brought a lot of benefits to society. Its impact on government parallels the improvements we see in the private sector, but with some significant differences. Budget cycles and lack of consistent policy support for technology investments sometime mean a slower innovation adoption in government, and the emerging privacy concerns take time to become policy that an entire nation must adopt.

A good example is the use of data. The mantra of the 20th century IT systems was "capture once, use often!". In industry, it made a lot of sense, where our address, financial details and shopping patterns would empower a more fruitful contact between customer and salesperson. However, when flipped on its side and applied to government agency work, a different concern arose: if agency A asks for information, it is for a particular, legislatively authorized use; agency B "should not" enjoy this information as the legislative intent, breadth of impact and other policy concerns may not align with the ones resident in agency A. And this concern has given rise to a different mantra in government data use: "use only for the intent for which it was gathered".

So how should agencies "leverage" data to improve services consistent with privacy protections? Again looking back at the re-invention cycles and attempts to deploy and use cross-agency systems, the intent was clear: leverage existing data strongly, and do so across agencies. However, with the rise of privacy advocacy, and the emergence of egregious or potentially egregious behavior of unauthorized data sharing- both in unclassified and classified space- has put the brake on the leveraging strategies. Perhaps the balance between privacy, security and empowerment aspects of data use can be re-interpreted based on today's technology capabilities (including cloud, 5G and other advances) and policy desires of our elected officials and those who lobby them.

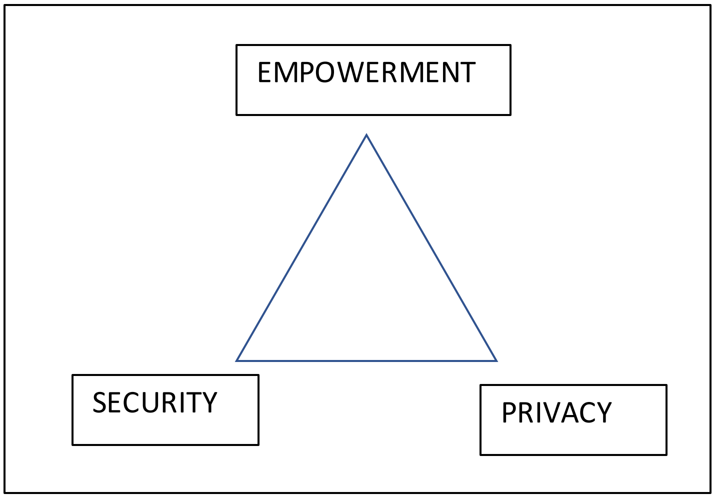

FIGURE 1: Data challenges and tensions

Pris Regan

The standard "fair information practices" – including limited collection, no secondary uses, consent of individuals, correction and amendment by individuals – are incorporated in the Privacy Act of 1974. These form the basis for how administrative agencies should be using data about individuals and building their administrative data systems. Some of these fair information practices have been modified by OMB guidance to provide less protection than originally intended, for example expansion of what is considered a "routine use." The E-Government Act of 2002 requirements for Privacy Impact Assessments, as well as its requirements for development and use of statistical records, are designed to provide increased protections.

The focus on evidence-based policymaking and the perceived benefits of "big data" have brought renewed attention to how administrative agencies can leverage administrative data to improve public services while also protecting privacy and ensuring security. The Census Bureau and the other principal statistical agencies have established a number of well thought out practices to be consistent with both the letter and spirit of the Privacy Act and the E-Government Act. Access and file transfer protocols, such as data sharing agreements and encryption of data, should be common practices. For research purposes, restricted use licenses are appropriate. Incorporation of "big data" – data from a myriad of sources, often messy, unreliable and noisy – into administrative systems provides a new set of challenges especially greater risks of reidentifying individuals and difficulties with deidentifying data. These challenges need to be addressed.