THE PRIVACY ADVISOR
The Official Newsletter of the International Association of Privacy Professionals
iapp
Editor, Kirk J. Nahra, CIPP
March 2011 • Volume 11 • Number 2

Government options for encouraging use of online privacy-enhancing technologies

By Steven C. Bennett

Both the U.S. Federal Trade Commission (FTC) and the U.S. Department of Commerce (DOC) recently issued reports that highlight the need for new thinking about e-commerce and privacy protection. Among the suggestions in the FTC's preliminary staff report "Protecting Consumer Privacy In An Era Of Rapid Change: A Proposed Framework for Businesses And Policymakers" and Department of Commerce Internet Policy Task Force green paper "Commercial Data Privacy In The Internet Economy: A Dynamic Policy Framework" were several points about the desirability of improving the quality of information and privacy choice control mechanisms available to individual users on the Internet. The FTC, in particular, proposed the development of a do-not-track mechanism to be made available via browser tools. The FTC also discussed the use of some form of icon to be placed on Web sites to indicate (in very simple terms) the form and quality of privacy protection available on the site. These kinds of solutions essentially fall into the category of "privacy-enhancing technologies" or "PETs." Assuming the desirability of making these or other PETs available, however, the question arises: how best to encourage use of such technologies? This article briefly surveys the array of regulatory tools available to the government and suggests that government mandates of specific PETs are a tool of last resort.

At one end of the spectrum, the government could essentially do nothing and let the market take care of the problem. On this view, if consumers truly care about privacy, they will shun Web sites that do not provide sufficient privacy protection and will search out technology (such as browser applications) that permit them to avoid "cookies" and other tracking intrusions from Web sites. Even if consumers do not have the time or qualifications to evaluate a site's privacy policy or the wherewithal to investigate appropriate browser technologies, if there is sufficient demand for privacy, then private self-regulation in the form of privacy certification groups will identify good privacy practices and will lend their "seal of approval" to sites that meet such standards. Indeed, a host of such services—TRUSTe, EuroPriSe and others—exist. In addition, private groups may develop more comprehensive self-regulatory codes to establish industry best practices for their members, such as the Network Advertising Initiative Self-Regulatory Code of Conduct or the Internet Advertising Bureau Self-Regulatory Principles for Online Behavioral Advertising.

The government, however, need not sit by idly and let the market regulate itself (and the buyer beware). The FTC already has jurisdiction to bring suit to enjoin "unfair or deceptive acts or practices." Additionally, most states have "little FTC" statutes that grant similar powers. Under the authority of these statutes, government agencies have brought dozens of suits to preclude deceptive online activities. In particular, the FTC has actively enforced its view that companies commit deceptive practices when they fail to follow their own stated privacy policies.

Government, moreover, can use the bully pulpit to investigate allegations of systemic privacy violations in online sectors. Indeed, the FTC has conducted nearly a dozen hearings on privacy-related issues in the past decade and has produced a large volume of detailed reports.

But those types of enforcement proceedings do not directly stimulate the market for PETs. The government can do so in a number of ways. Government can encourage innovation in this area by funding research (either directly through support for academic efforts or indirectly through tax incentives to businesses that innovate in this area). Moreover, government can serve as a model user of PETs and can encourage technology development by creating demand for such technology. The federal government, for example, has long required federal agencies to offer machine-readable privacy policies using a system known as the Platform for Privacy Preferences (P3P). Government also can encourage demand by sponsoring public education campaigns.

In addition, government can raise the profile of the issue by making it a high priority for interagency coordination. In the cyberspace security arena, for example, in early 2009, the Obama administration directed an interagency review of national policy. The government team, coupled with representatives from industry, academia, civil liberties, state government and international constituents issued a May 2009 "Cyberspace Policy Review," which, among other things, suggested "bridging previously disparate agency missions" and forming "partnerships with the private sector and academia to articulate coordinated national information and communications infrastructure objectives," including a "national public awareness and education campaign" and government "procurement strategies that will incentivize the market to make more secure products and services available to the public." (See www.whitehouse.gov/assets/documents.)

A major report from the interagency team appeared in June 2010, calling for government to become "early adopter" of technology, to "leverage" buying power as a "significant customer" and to "enhance the business case and marketplace for these solutions." In October 2010, the White House announced the creation of a permanent interagency group. This committee, co-chaired by representatives from the Commerce Department and the Justice Department, will operate under the auspices of the National Science and Technology Council with input from more than a dozen cabinet-level and independent federal agencies. The stated purpose of the group is to help formulate policies that will "strike the appropriate balance between the privacy expectations of consumers and the needs of industry, law enforcement and other public safety governmental entities, and other Internet stakeholders." At a minimum, the creation of this permanent entity ensures that the issue will receive high-level attention.

Finally, even if the government wishes to go beyond mere encouragement of the development and implementation of PETs, it need not directly mandate use of such technologies. Rather, many possibilities exist for "co-regulation" in this field. For example, government might establish tax incentives for companies that follow the self-regulatory "best practice" principles (to the extent that such standards incorporate the use of adequate PETs). These, and other incentives (such as government procurement preferences) constitute "carrots" to encourage technology adoption. Conversely, companies that do not adopt "best practice" technologies could be subject to "sticks" (disincentives such as increased reporting requirements).

A variation on this co-regulation notion appears in the implementation of the Children's Online Privacy Protection Act (COPPA). Under COPPA, a safe harbor exists for companies that follow industry self-regulatory guidelines approved by the FTC. Businesses that comply with the safe harbor guidelines are presumptively deemed by the FTC to be in compliance with the law. Another form of safe harbor appears in the U.S.-EU safe harbor agreement. These co-regulatory approaches, moreover, follow analogous efforts at regulation in other fields, such as environmental pollution.

Even where the government mandates use of technology, it need not specify the exact form and operation of any systems. Under the HIPAA "Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information," for example, the Department of Health and Human Services (HHS) requires that covered entities implement appropriate administrative, technical and physical safeguards to protect the privacy of protected health information. The HHS privacy framework, however, is flexible and does not prescribe any specific technical practices. Thus, entities of different sizes and functions may adopt technology appropriate to their specific needs. The HHS privacy framework also allows the formation of self-regulatory standards for information exchange to meet the needs of specific segments of the healthcare industry. The HHS privacy framework, moreover, only applies to "covered" entities, leaving open the possibility that some businesses are too small, too new or too far removed from the central problem (protecting the privacy of patient health information) to require regulation.

Ultimately, privacy regulation involves considering an array of options, which may range from market self-regulation to full-scale "command and control" by one or more agencies for one or more purposes. Creating an optimal privacy protection regime requires clear understanding of the size and character of the problem to be addressed, the nature of the marketplace (including the inevitable imperfections that appear in the market) and the advantages and disadvantages of each form of regulation. Furthermore, government regulators (both federal and state) must recognize the fast-paced changes in technology, business practices and consumer preferences that inhere in our information-based economy and must plan for the possibility (indeed, likelihood) that any regulatory approach adopted today may become obsolete (and even harmful) sometime in the future. Finally, government regulators must acknowledge that no single form of regulation is necessarily "best" in the view of all. Regulation involves subjective value choices and balancing of many interests. Input from all affected stakeholders, coupled with a willingness to experiment and abandon approaches that do not work under the circumstances will ensure (at least) that government may come closer to "getting it right."

Read more by Steven Bennett:

Israeli attitudes on privacy

The author is a partner in the New York City offices of Jones Day, and chair of the firm's Ediscovery Committee. He teaches Electronic Discovery at New York Law School and Conflicts of Law at Hofstra Law School. The views expressed are solely those of the author and should not be attributed to the author's firm or its clients.