Facilitate, don't mandate

Ari Rabkin, Nick Doty and Deirdre K. Mulligan; UC Berkeley November 2010

Many government actions require an Environmental Impact Statement; some now require a Privacy Impact Assessment.[1] One might imagine a requirement that IETF protocol designers go through some similar activity. The IETF already requires proposed standards to have a "security considerations" section, why not a public policy considerations section? In 2003, Morris and Davidson proposed that a "public policy assessment should be done for all standards adopted by the IETF".[2] This proposal, however, was met with near-total apathy. There were no public comments on the submitted Internet draft, the document has never been cited, and has since expired. As Morris put it: "Not many people paid much mind."[3]

Where systematically addressing public policy considerations in standards was met with a lack of interest seven years ago, there are good reasons to think it might be welcomed today. Standards bodies and their members have recently shown considerable interest in privacy implications (see the series of W3C workshops) and technology companies face increased scrutiny from the media, advocates and regulators for their privacy policies and even the interaction of Web standards with their business models.[4] Just this week the European Commission set out its agenda for modernizing the EU Data Protection Directive specifically including efforts to consider operationalizing the principle of "Privacy by Design" — embedding privacy and data protection throughout the development, deployment, use and ultimate disposal of technologies.[5] How should standards bodies address these growing concerns?

We argue that standards bodies should undertake efforts to incorporate privacy and data protection into the development of standards. However, we believe efforts to do so must advance in a manner that maximizes their substantive success. We currently counsel against the adoption of mandatory policy impact statements at the IETF, W3C and other open standards bodies. This conclusion is supported by the fundamentally voluntary nature of technical standards bodies; the relative immaturity of the tools for assessing the policy impact of technical design; and the lack of sufficient expertise in the standards-setting community to effectively use existing tools. Instead we suggest efforts to facilitate policy-awareness among standards bodies' members and encourage participation from experts in law, public policy, ethics and technology.

Participants who want to reach consensus on a protocol are in no way locked in to a particular standardization process. Many alternate standards bodies exist, such as the IEEE, ITU, OASIS, WHATWG and the Open Web Foundation. Indeed, participants seeking a standard need not use any formal standards process at all. The Java programming language was originally developed by Sun, Inc., and then further standardized by the Java Community Process, established by Sun. The distinction between "official" standards and corporate assertion is tenuous: an organization with nerve and resources can set up its own "standards body", or simply start issuing documents with "standard" in the title. Because developers have such alternatives, technical standards bodies face pressure to make standardization quicker and easier. For example, the ITU in 2001 launched the "Alternative Approval Process" — an administrative way of fast-tracking protocol approval, which can often result in approval within a few months — explicitly in response to pressure from members, and particularly corporate members.[6] Given these incentives to streamline the standards process, why is the IETF able to require security consideration in every document? And if security, why not also public policy?

Security provides a valuable comparison here, as in fact security reviews in technical standards took considerable time to become a meaningful part of the standards-setting process. We examined 20 RFCs (15 standards-track) from 1996, well after the imposition of the security mandate: only three had anything substantive to say about security. Even these remarks were brief and general — a few sentences, mostly pointing out in general terms that security issues might arise in deployment. Only as security grew as both a research sub-discipline and a professional field did RFC security considerations expand to

---

[1] In the US, the E-Government Act of 2002; in the EU, Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[2] John Morris and Alan Davidson. "Policy Impact Assessments: Considering the Public Interest in Internet Standards Development". TPRC 2003.

[3] John Morris. Personal Interview. May 14, 2009.

[4] For example:
http://voices.washingtonpost.com/posttech/Schumer-Franken-Bennet-Begich%20Letter%20to%20Facebook%204.27.10.pdf
http://voices.washingtonpost.com/posttech/2010/02/privacy_advocates_file_complai.html
http://online.wsj.com/article/SB10001424052748704513104575256701215465596.html

[5] This principle was set out in the Commission Communication on ‘A Digital Agenda for Europe’. COM(2010) 245.

[6] http://www.itu.int/ITU-T/50/docs/ITU-T_50.pdf p16.

fulfill their intended purpose. While the use of privacy impact assessments, pioneered in the mid-1990s by data protection authorities in New Zealand and Canada, are becoming a more common component of the privacy regulatory landscape and there is a growing research community attempting to develop tools and methods to assess the social implications of technical design, privacy still lacks the robust set of instruments available in security.

Security also differs substantially from privacy in terms of expertise. Security is a recognized sub-field of computer science and is an increasingly standard part of the curriculum. In contrast, privacy has only more recently taken a prominent role; policy concerns are often considered apart from "technical" ones. Issues of public policy concern can rarely be as straightforwardly decided on as security is; social scientists continue to struggle over a workable definition of privacy. And while the goal of security in standards tends to be widely shared, views of privacy differ dramatically between cultures and individuals. Understanding and addressing the public policy implications of a technical standard not only requires a technical background, but also benefits from experience with law, social psychology, human-computer interaction, philosophy, economics and public policy for recognizing the values embedded in technology.[7] Privacy by design is inherently interdisciplinary and we should not expect that expertise to arise suddenly from the existing technical standards community made up largely of engineers from member companies.

Without engaged expertise, mandates of security, privacy or any other set of considerations will fall short of their intended goal. In the case of government, mandated privacy impact assessments at the US federal agency level hadn't successfully served to build privacy into the design of new RFID passports by the State department; a 1-page privacy assessment document (not unlike the 1-line disclaimers sometimes found in Security Considerations sections of specifications) missed the many serious implications of passports that could broadcast the identities of their owners at a distance, apparently because of a lack of in-house expertise and an over-reliance on industry assurances. Only after the plan was opened to public comment (where it was vigorously opposed by experts) were the privacy issues identified and (partly) addressed. In contrast, the Department of Homeland Security considering a similar RFID enabled document ably used the privacy impact assessment to identify threats, mitigations, and alternate designs.[8] In the long run, not only do we need to design a diverse set of tools, but we need to develop a field of professionals to use them.

The IETF, W3C and other technical standards bodies have many options for facilitating this sort of engagement:

- Provide guidance for "issue spotting" — Participants without an extensive background in privacy issues can be given tools to help identify issues likely to be of concern. We think the series of questions proposed by Morris and Davidson and recently updated by Tschofenig[9] is an excellent start.
- Match experts with working groups — Particularly for standards that are likely to have privacy implications, standards bodies should have a process for integrating experts in law, policy or privacy with working groups throughout the process. This can avoid the appearance of "helicopter" participation by advocates at the last minute. We at UC Berkeley are working to encourage faculty and students in computer science, law and the interdisciplinary School of Information to become more involved in these activities. We hope other academic organizations at the intersections between technology and policy will do the same.
- Codify known best-design-practices for reuse across standards — We're encouraged by the work that the W3C Device APIs and Policy Working Group is doing to standardize requirements and solutions to privacy problems that can be reused in several different standards in the mobile space. This may help both to provide a consistent experience to users and to remove some of the tedium and debate from individual working groups.
- Share general knowledge — Many principles of privacy (data minimization; notice and consent; etc.) apply across standards, across working groups and across standards bodies. Sharing developments from the academic literature and experiences from particular standardization efforts can help working groups focus on the key challenges specific to their topic. It might be valuable to identify a list of the most helpful academic papers for working group members (as was done recently for policymakers[10]). We also hope that the W3C and IAB will continue to hold workshops to discuss these topics in person.

---

[7] See, for example, M. Flanagan, D. Howe, and H. Nissenbaum. "Embodying Values in Technology: Theory and Practice".

[8] Kenneth Bamberger and Deirdre K. Mulligan. "Privacy Decisionmaking in Administrative Agencies".

[9] http://tools.ietf.org/html/draft-morris-policy-cons-00

[10] "The Future of Privacy Forum Releases Privacy Papers for Policy Makers Journal". September 15, 2010. http://www.futureofprivacy.org/2010/09/15/fpf-releases-privacy-papers-for-policy-makers-journal/