December 17, 2020

Directions

Nick Doty
UC Berkeley, School of Information

Status of This Document *This is a chapter of a published dissertation: Enacting Privacy in Internet Standards.*

6 Directions for future work

What this leaves for the future is the question, or rather, the challenge, of what practices we could use in technical standard-setting to more effectively enact privacy and security for the Internet and the Web.

6.1 A triad for interventions

Throughout this research project and throughout my personal and professional efforts to support privacy on the Web, I have seen how potential improvements can involve three distinct but connected areas:

1. the people involved in the development of the technology;
2. the processes used in organizing its creation; and,
3. the tools used for design and implementation.

These might conceivably apply to questions of values in the design of technology generally, but I have observed them explicitly in the collaborative, rough consensus standard-setting process in particular.

6.1.1 People Leaders have played a substantial role in the support of security and privacy in Internet and Web protocols, perhaps especially because the standard-setting process doesn't rely on a single firm's hierarchical model but instead pushes for interoperability and collaboration between disparate and competing organizations. Leaders have provided both a backstop and a motivation for security and privacy to be considered more directly in the design of the Internet and the Web.

In recognizing the inherently ethically-laden nature of engineering, a shift towards integration of values in design and engineering and the potential for techno-policy standards that explicitly involve values such as privacy, particular combinations of expertise are increasingly useful. Those with both technical and legal backgrounds may be able to recognize and evaluate possible socio-technical configurations. While it may not be a rapid intervention, education can help meet this need. Schools of Information pursue an interdisciplinary approach, typically combining computer science topics with social science, law and policy and user-centered design.[1] Technology & Delegation, a seminar class, a lab class and a set of curricular resources,[2] has been an explicit project to encourage students with varying backgrounds to confront direct intersections of technology and policy and how they interact.

The need for technologists engaged in public interest work and helping civil society and philanthropy has been described as a "pivotal moment" (Freedman et al. 2016). Scholars, foundations and practitioners have sought to develop a new field of public interest technology (Eaves et al. 2020), not unlike our earlier definition of a "citizen technologist" (Doty and Panger 2015). A network of universities is committed to "growing a new generation of civic-minded technologists" – an urgent and important goal.[3] Clinics provide students with experiential learning while fellowships directly integrate technologists into traditional policymaking spaces.[4]

6.1.2 Process While motivated individuals or community leaders have made a significant difference, organizational processes can bring broader and more systematic considerations of privacy, security and other values to the Internet standard-setting process. Rotating assignments in a Security Directorate at IETF is

[1] What an iSchool is remains an open question welcoming constant refinement and definition, but see for example the iSchools organization: https://ischools.org/About.

[2] Most recently taught in Fall 2019, with a wiki of Techdel resources.

[3] https://www.newamerica.org/pit/university-network/about/

[4] See, for example, TechCongress: https://www.techcongress.io/

credited with improving the consistency of security reviews in Internet protocols, and similar attempts have been made with triggering wide review, including privacy reviews and architectural design reviews, at W3C.[5] Procedural requirements can also be a hook for interested individuals to provide feedback on features that affect important values like privacy.

Clear and systematic process also provides an opportunity for more confidence in how consensus technical standard-setting can apply to policy-related topics. Removing uncertainty could remove confusion or even encourage cooperation. Along the same lines, we might ask for clearer roles from policymakers in their participation in consensus techno-policy standardization – how invested they are and what they aim to contribute, whether that's requirements, some democratic legitimacy, incentives to participate or the power to enforce standards.

Finally, process implies or perhaps even requires continual application. Systematization, clarity, establishing roles – these would all benefit from repeated, ongoing processes that proceed to address the next tech policy and continually review and revise existing systems. Periodic events, or development lifecycles that follow a linear waterfall model, don't provide the same opportunities for building relationships and effective institutions.

6.1.3 Tools Technologists must not forget the tools that influence tool-building. Tools here can range from simple, automated checks to comprehensive high-level design principles. Regarding security and privacy considerations in Internet standards, automated prompts can ensure that specification authors are at least aware of the need to directly address those values in new protocols. But simple, blunt requirements alone will also prove to be insufficient (Doty 2015). Detailed guidance might prove fruitful, perhaps especially for those interdisciplinary or values-minded individuals who want to directly address privacy or security details in their domain of interest. I've tried to contribute for my part guidance on mitigating browser fingerprinting (Doty 2019), because it is a detailed privacy topic that accumulates across different features and could benefit from some coordinated and comprehensive response.

Tools may be most effective, though, when they work in concert with people and processes. Questionnaires, for example, allow experts close to a particular domain area but not necessarily trained on privacy or policy issues in general

[5] This theme was highlighted in Doty (2015) and I believe systematization has slowly increased since.

to help in identifying potential areas that may need further review[6] and collect details that a privacy expert who isn't intimately familiar with the domain can use in evaluating implications. W3C now sees widespread use of a self-review questionnaire for both security and privacy ("Self-Review Questionnaire: Security and Privacy" 2020) and a similar questionnaire is included in IETF's privacy considerations guidance (Hansen et al. 2013).

In the longer term, though, support for privacy, security and other values could be more efficiently maintained if they were designed in from the beginning, rather than spotted as potential problems along the way. Higher level design principles could be tools for these more fundamental changes, but privacy-by-design can be difficult to put into practice, even for those engineers who may already share the ethical commitment to it. Design patterns are documentation tools to codify and communicate abstract solutions to common engineering problems. Privacy design patterns, then, may:[7]

- standardize language for privacy-preserving technologies,
- document common solutions to privacy problems, and,
- help designers identify and address privacy concerns.

As a tool for communication, privacy design patterns can also facilitate communication of detailed engineering practice to lawyers or policymakers. Anti-patterns can help to classify the misapplication of a technique or warn of its unintended consequences (Doty and Gupta 2013) or to document the common problems that lead to a lack of privacy in Web standards (Snyder 2019).

6.2 Recognizing future handoffs

I have argued that privacy and security are values of distinctive salience to the Internet and the Web. But those concepts are complex, contested and likely to involve new senses over time. Even in the course of writing this dissertation, the distinctive, topical senses of privacy have changed. Fairness was a new privacy-relevant topic, with the idea that privacy might be the protection against unfair, society-wide inferences about oneself or one's community. Or perhaps privacy is freedom from the harassment and abuse that trolling and dog-piling on social media have made so easy. More recently still, the trend toward toxic disinformation

[6] This is sometimes called "issue spotting," inspired by the term from legal practice.

[7] These project goals are taken directly from the collaborative privacypatterns.org project: https://privacypatterns.org/about/.

uses those same social network channels to target not just an individual, but an entire society's sense of what is real or reliable.

Seen through the handoffs model, there are likely to be many more shifts in how values are maintained (or not) in different socio-technical configurations and how responsibility is distributed. Some paradigmatic shifts around security may be linear trends away from discretion or false reliance on assumptions of goodwill or end user expertise – like the ongoing march toward encrypting the Web. But there will also be the possibility of handoffs to more distributed approaches that involve communication among people, technology and regulatory systems.

Technical standard-setting – or specifically what I have called techno-policy standard-setting – provides an opportunity for multistakeholderism's promise of democratic and technocratic advantages, in the line of new governance as well as the bridging property of boundary organizations. Standard-setting's practical focus on interoperability suits it for handoffs to cooperative configurations developed by diverse parties – if those various organizations have incentives to pursue it and that heterogeneous group of individuals can work together. The handoff model encourages holism and asks us to look at the broader socio-technical system and the network of actors involved. Any multistakeholder process takes place embedded in the context of ongoing technical, social, organizational and policy changes that influence it.

Whether these concerns are all considered senses of privacy or not, we face tech policy issues that are urgent, complex and have large impacts on public policy, including criminal justice, equal access to digital public fora, democracy and public health. We need comprehensive responses that integrate technical expertise, policy details and ethical understanding. To respond effectively and promptly, we must use what we have learned from our attempts to enact privacy on the Internet.

References

Doty, Nick. 2015. "Reviewing for Privacy in Internet and Web Standard-Setting." In *Security and Privacy Workshops (SPW), 2015 IEEE*, 185–92. IEEE. https://npdoty.name/privacy-reviews/iwpe/.

———. 2019. "Mitigating Browser Fingerprinting in Web Specifications." Interest Group Note. Privacy Interest Group (PING). World Wide Web Consortium. https://www.w3.org/TR/2019/NOTE-fingerprinting-guidance-20190328/.

Doty, Nick, and Mohit Gupta. 2013. "Privacy Design Patterns and Anti-Patterns: Patterns Misapplied and Unintended Consequences." In *A Turn for the Worse:*

Trustbusters for User Interfaces Workshop. http://cups.cs.cmu.edu/soups/2013/trustbusters.html.

Doty, Nick, and Galen Panger. 2015. "Introducing Citizen Technologist, the Blog." *CTSP Blog* (blog). September 9, 2015. https://ctsp.berkeley.edu/introducing-citizen-technologist-the-blog/.

Eaves, David, Ed Felten, Tara McGuinness, Deirdre K. Mulligan, and Jeremy Weinstein. 2020. "Defining Public Interest Technology." *New America* (blog). January 22, 2020. http://newamerica.org/pit/blog/defining-public-interest-technology/.

Freedman, Tom, Jessica Roeder, Alexander Hart, Kyle Doran, and Kaye Sklar. 2016. "A Pivotal Moment: Developing a New Generation of Technologists for the Public Interest." Freedman Consulting. http://tfreedmanconsulting.com/reports/a-pivotal-moment-developing-a-new-generation-of-technologists-for-the-public-interest/.

Hansen, Marit, John Morris, Alissa Cooper, Rhys Smith, Hannes Tschofenig, Jon Peterson, and Bernard Aboba. 2013. "Privacy Considerations for Internet Protocols." RFC 6973. Request for Comments. RFC Editor. https://tools.ietf.org/html/rfc6973.

"Self-Review Questionnaire: Security and Privacy." 2020. W3c Technical Architecture Group. World Wide Web Consortium. https://w3ctag.github.io/security-questionnaire/.

Snyder, Pete. 2019. "Privacy Anti-Patterns in Standards." *W3c Blog* (blog). June 12, 2019. https://www.w3.org/blog/2019/06/privacy-anti-patterns-in-standards/.