Toward Objective Global Privacy Standards

Ari Schwartz
Senior Internet Policy Advisor
National Institute of Standards and Technology[1]
US Department of Commerce

Summary

Technical standards offer a new ability to support the important public policy goal of better protecting privacy. To do so most effectively, we must begin to move from the privacy standards based on subjective and procedural efforts to a series of objective performance driven privacy standards. Better scientific metrics tied to each Fair Information Practice Principle are a necessary precursor to the reproducible measurements for any set of objective criteria that could be the basis for such standards.

Introduction

Privacy standards offer the ability to develop technology that can improve privacy practices and actively create privacy protections in several different ways, namely:

- Interoperable Privacy Enhancing Technologies (PETs),
- Privacy By Design,[2] and
- Related and Other Outcomes, such as:
    - Reducing the cost related to differing global privacy oversight,
    - Reducing the risk of developing new technologies,
    - Increasing voluntary compliance,
    - Providing thought leadership in a scarce resource field, and
    - Easing the cost of compliance.[3]

Each of these goals represents an important public policy outcome. Yet, setting privacy standards is not an easy task and, to date, has not been as successful as many of those who have worked on the problem have hoped.[4] Therefore, before delving deeply into any standard setting process specifically for privacy, it seems

---

[1] Official contributions of the National Institute of Standards and Technology; not subject to copyright in the United States

[2] See From the Ontario Information and Privacy Commission — http://www.privacybydesign.ca/ and related writings by Commissioner Ann Cavoukian.

[3] Adapted from John Borking, "Privacy Standards for Trust" — http://www.privacyconference2005.org/fileadmin/PDF/borking.pdf

[4] Ari Schwartz, "Lessons for Future PETs Standards: Looking Back at P3P: Novemember 2009 http://ec.europa.eu/justice/news/events/workshop_pets_2009/presentations/SCHWARTZ_Ari_paper.pdf

important to review of other efforts to set standards in support of specific public policy outcomes.

In fact, there has been a great deal of both scholarship and consensus building in standards organizations about how to create standards in support of public policy.[5] Notably, the International Standards Organization (ISO) and the International Electrotechnical Commission (IEC) have jointly developed "Principles for Developing ISO and IEC Standards Related to or Supporting Public Policy Initiatives." Here is a shortened version of these principles:[6]

> 1) ISO and IEC are committed to creating market-driven International Standards, based on objective information and knowledge on which there is global consensus, and not on subjective judgments, in order to provide credible technical tools that can support the implementation of regulation and public policy initiatives.
>
> 2) ISO and IEC are committed to developing International Standards that are market relevant, meeting the needs and concerns of all relevant stakeholders including public authorities where appropriate, without seeking to establish, drive or motivate public policy, regulations, or social and political agendas.
>
> 3) ISO and IEC recognize that the development of regulation, public policy and/or the development and interpretation of international treaties are the role of governments or treaty organizations.
>
> 4) ISO and IEC standards supporting regulation, regulatory cooperation and public policy are best developed within ISO and IEC structures and under operational approaches and participation models that have been proven successful and that are detailed in the ISO/IEC Directives.

In general, these principles return to a couple of important points. First, technical standards should support and not make public policy and therefore extra attention has to be paid to ensure that a particular law or policy is not being favored over interoperable technical solutions. Second, objective measures offer a means to have a scientific discussion about public policy. As discussions veer to the subjective, there is a greater risk that policy will be created and not simply supported.[7]

These points offer particular challenges in an effort such as standardizing privacy. The expectation of privacy is often discussed in subjective terms (different people have a different sense of when their privacy has been invaded) yet validated in objective terms (laws, regulation and related policy determine a

---

[5] For example, see Standards and Public Policy; Shane Greenfield and Victor Stango, Editors; Cambridge University Press (January 22, 2007).

[6] http://www.iso.org/iso/principles_for_developing_iso_and_iec_standards_related_to_or_supporting_public_policy_initiatives.pdf

[7] I have simplified by raising one means by which technical standards bodies create public policy. Laura DeNardis at Yale Information Society Project of the Yale Law School has written extensively on these issues and addresses this issue in much greater detail in several recent writings. See http://lauradenardis.org/writing/

point at which governments get involved in a privacy invasion).[8] To make this breaking point easier for organizational compliance and for governments to enforce, some have suggested that this objectivity can only be determined by some monetary or related harm has befallen the privacy victim.[9] Yet determining actual harm is clearly not the only means to reach an objective measure for privacy.

Companies, regulators, and privacy advocates, however, have reached a significant level of agreement on high-level principles to protect privacy; and these principles offer a way forward on privacy standards. Beginning in 1973, different governance bodies have developed sets of fair information practice principles (FIPPs), sets of generally applicable obligations to guide handling of personal data.[10] FIPPs have been flexible enough to adapt to changing consumer expectations and new technologies and importantly have offered an international starting point to discuss privacy protections.

For example, FIPPs are the foundation of the OECD's privacy guidelines, the EU Data Protection Directive, and the APEC Privacy Framework. In the United States, the Department of Homeland Security (DHS) recently adopted a set of FIPPs to govern its use of personally identifiable information. To the extent that choosing to standardize around FIPPs (rather than alternative definitions of privacy) involves a policy choice, it is a choice that numerous governments, representing a large share of world economic output, have made.

For clarity, consider how standardization around the DHS FIPPs might proceed. The DHS FIPPs include:[11]

- Transparency: provide notice to an individual concerning the collection, use, and disclosure of personal information.

---

[8] In 1967, the United States Supreme Court developed what has been described as the existing international "litmus test" that a person can have a reasonable expectation of privacy only when (1) he has an actual "(subjective) expectation" of privacy in a certain situation, and (2) society is prepared to recognize this "(objective) expectation" as reasonable (see also section 4.2). *Katz v. United States*, 389 U.S. 347 (1967). Similar discussions have come up recently in understanding a user's expectation in location privacy see S Nouwt, "Reasonable Expectations of Geo-Privacy?", (2008) 5:2 SCRIPTed 375 http://www.law.ed.ac.uk/ahrc/script-ed/vol5-2/nouwt.asp and for social networks see Tony Bradley, "Privacy is Not Dead, Just Evolving" PC World, March 14, 2010.

[9] Peter Fleischer, Global Privacy Counsel "Global privacy standards should focus on preventing harm to consumers" November 14, 2007 http://googlepublicpolicy.blogspot.com/2007/11/global-privacy-standards-should-focus.html

[10] The first set was developed by the US Health Education and Welfare Department as part of its Report entitled "Records, Computers and the Rights of Citizens" — http://aspe.hhs.gov/DATACNCL/1973privacy/tocprefacemembers.htm

[11] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf

- Individual participation: seek individual consent for the collection, use, and disclosure of personal information; and provide mechanisms to correct information and obtain redress for misuse.
- Purpose specification: articulate specific purposes for information that is collected.
- Data minimization: collect only the information that is directly relevant to achieving a stated purpose, and retain information only as long as necessary to achieve these purposes.
- Data quality and integrity: ensure that collected information is accurate, timely, and complete.
- Security: implement appropriate safeguards against unauthorized disclosures.
- Accountability and Auditing: an organization should audit actual information use to demonstrate compliance with its policies.

The FIPPs provide a framework to which standards can be added. For example, we can build standards to provide transparency through specific notices or through specific access procedures. However, without some analysis of performance metrics, these standards would remain tied directly to subjective expectations rather than an objective understanding of public policy.

The main challenge to creating objective standards is to build objective measures for FIPPs. While actual harms could provide one measure, they do not need to be the only measure to use. There have been several efforts to create these kind of metrics. Professor Lorrie Cranor working with Aleecia McDonald has developed several empirical studies to examine things such as privacy notices and formats.[12] These studies utilize quantitative social science methods to make determinations about how users read information. This type of study could be replicated for other FIPPs. For example, counter claims have been made about whether individual access improves or harms data quality, but little empirical data has been used to defend either claim.[13] Empirical research to examine access and data quality in this context could help us create metrics and then standards to implement both FIPPs.

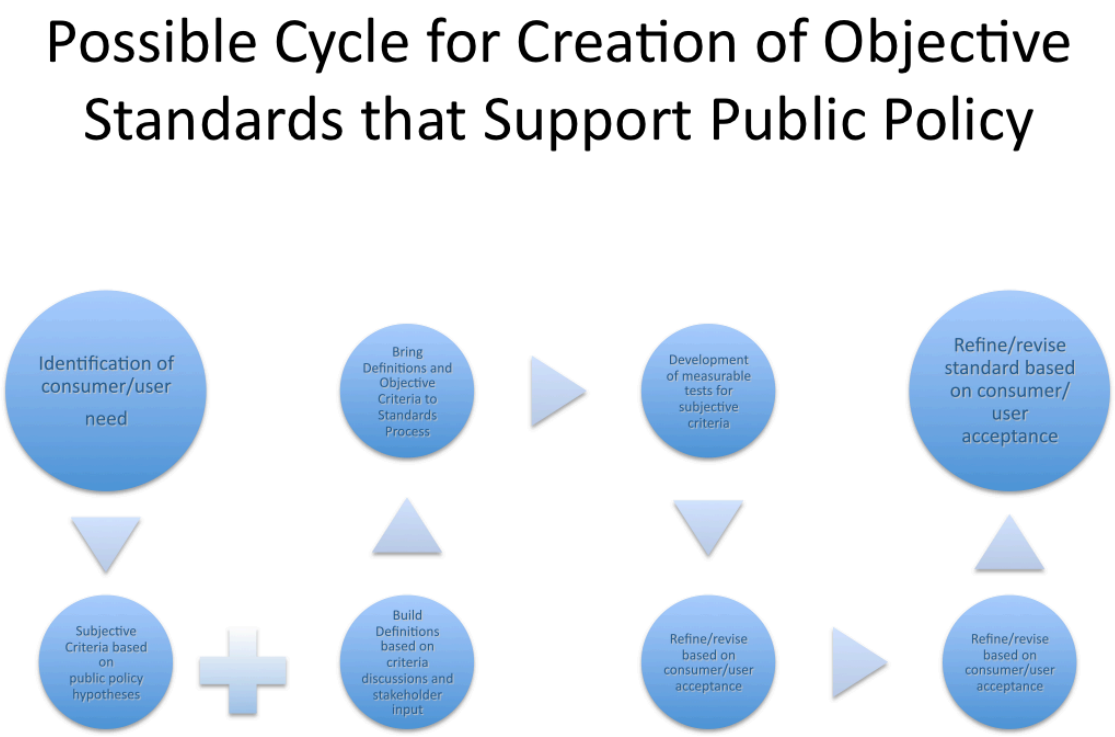
However, it must be noted that developing such measures will not lead to a single standard that magically protects privacy. Most other social problems are also not solved through single technical standards or technology or a single legal

[12] A.M. McDonald and L.F. Cranor. An Empirical Study of How People Perceive Online Behavioral Advertising. Carnegie Mellon CyLab Technical Report CMU-CyLab-09-015, November 10, 2009. http://www.cylab.cmu.edu/research/techreports/2009/tr-cylab09015.html

[13] Martin R. Gibbs, Graeme Shanks and Reeva Lederman's "Data Quality, Database Fragmentation and Information Privacy," http://www.surveillance-and-society.org/Articles3(1)/data.pdf discusses some views on this debate based on the Australian commercial privacy law but conclude that not enough data exists to prove whether concerns are warranted in either direction.

standard. In fact, other domains illustrate how a group of standards can help reduce social ills. For example, fire prevention utilizes standards for fire fighting equipment, smoke alarms, fire resistant fabrics, building codes, communications and many more that have been developed over the past 120 years. One single area might help prevent fires, but it is not the total solution. Privacy will certainly follow a similar path. We will need individual standards and technologies to help build privacy by design and to implement FIPPs.

Once it has been determined which FIPPs a collaborative body is trying to standardize around, it is important to develop common definitions and common criteria.[14] In the access example above, there may be different criteria access is granted to different types of information. These types of information will probably need to be defined in a way so that those measuring are using exactly the same terminology. Below is a model of how these steps interact with measurement until they are refined into a final standard:



[14] These components have been key areas in several ad hoc Internet public policy standards. For example, the Anti-Spyware Coalition — http://www.antispywarecoalition.com and Creative Commons — http://creativecommons.org both utilize common definitions and criteria to accomplish very different public policy goals.

As this model demonstrates, criteria and definitions are symbiotic in that it is often difficult to move one forward without also working on the other.[15] It is only after the first set of subjective criteria are built that measurement can occur and a move toward an objective standard can really begin. While we are discussing support for privacy policies, this same process could be used for any emerging area of a standard to support public policy.

Conclusion

Fair Information Practice Principles (FIPPs) offer a pathway to selecting areas to develop into privacy protecting processes and standards. More research and concerted effort to develop the measures that will be needed to create the objective criteria that can make up the basis for objective standards. This research should focus both on individual and organizational behavior as it relates to data privacy. Once objective standards are created, they will need to be utilized in concert with other technical and policy standards to create continually improving protections.

[15] In delivering an earlier keynote on this topic at the The First ISO Privacy Standards Conference in Berlin, Germany on October 8, 2010 — http://isotc.iso.org/livelink/livelink/open/conference — questioners suggested that it is difficult to do definitions prior to criteria or vice versa. This has been my experience as well so I've altered the process accordingly.