COMMENTS ON DEPARTMENT OF COMMERCE INTERNET POLICY TASK FORCE REPORT
Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework

RESPONSE FILED BY:
U.S. PUBLIC POLICY COUNCIL OF THE ASSOCIATION FOR COMPUTING MACHINERY

On behalf of the U.S. Public Policy Council (USACM) of the Association for Computing Machinery (ACM) we are submitting the following comments on online privacy in response to the report from the Internet Policy Task Force of the Department of Commerce.

With nearly 100,000 members, the Association for Computing Machinery (ACM) is the world's largest educational and scientific computing society, uniting computing educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges.. The ACM U.S. Public Policy Council (USACM) serves as the focal point for ACM's interaction with U.S. government organizations, the computing community, and the U.S. public in all matters of U.S. public policy related to information technology. Our comments are informed by our previously issued statement on Privacy.[1] Should you have any questions or need additional information, please contact Cameron Wilson, our Director of Public Policy, at 202-659-9711 or at Cameron.wilson@acm.org

Introduction

We appreciate and welcome the attention the Department of Commerce and the Internet Privacy Task Force have placed on data privacy. Striking a balance between individual privacy rights and valid government and commercial needs is a complex task for technologists and policy makers, but one of vital importance. It is important for the Department of Commerce to be involved in seeking this balance, to complement the efforts of agencies like the Federal Trade Commission. We believe that effective data privacy policies and practices can provide benefits to consumers and commercial interests alike.

FIPPs and a Lexicon to Support Privacy

We support the broad adoption of Fair Information Practice Principles (FIPPs), which underlie our USACM Privacy Policy Recommendations. Because so many FIPPs—including the minimization of data collection and data retention, as well as use limitation—are relative to the purpose of the system or business process in question, purpose specification serves as a lynchpin and therefore deserves special emphasis. In particular, and also reflective of practical problems observed with notice and choice, a more rigorous yet concise means of specifying purpose and other characteristics, would yield significant benefits. This requires a dataflow-based lexicon - a compendium of standard representations of how personal information flows between different entities in the context of a particular purpose, such as the online purchase of a material object. The lexicon would define the specifics of personal information flows at an appropriate level of granularity, while providing a concise reference term for each representation. This lexicon must accommodate multiple meanings and explicit industry-standard data purposes, while being easily adaptable in response to changing technological possibilities. Such a lexicon makes it harder for interpretations of terms to become outdated or limited in scope. An appropriate body must oversee development and maintenance of this lexicon; the proposed Privacy Policy Office (PPO) is one possibility.

The lexicon should explicitly and unambiguously distinguish among the diverse set of industrial and government data purposes, with the aim of moving towards a national standard for the terms it covers. As a catalogue of data practices, this proposed lexicon is similar in nature to the North American Industrial Classification System (NAICS) published by the U.S. Census Bureau. However, it would be smaller, more focused and more domain-specific than NAICS. In those respects, the lexicon would resemble something like the International Classification of Diseases (ICD) published by the Centers for Disease Control. By indexing data purposes uniquely in a lexicon, purposes can be more easily identified in privacy policies and potentially linked to

[1] USACM Privacy Policy Recommendations, http://usacm.acm.org/usacm/Issues/Privacy.htm

enterprise business practices and information assets. This easy identification would make it easier to judge compliance with FIPPs and to monitor data collection practices.

For consumers to make informed choices, they must be able to differentiate between meaningful variations in the same class of privacy control or data practice. For example, businesses may present consumers with "opt-out" controls that are limited to either third party secondary uses of personal information, or to first party secondary uses, or both. Similarly, the meaning of "online tracking" can include many different things, including: tracking to deliver targeted, third party advertisements; tracking for analytics to improve website navigation; or tracking for website functionality, such as managing shopping carts or other user sessions. Therefore, the lexicon should allow consumers and businesses to uniquely distinguish terms for privacy controls or data practices, and their varieties, in privacy policies and other statements of record. Such a lexicon must be machine readable, so that web browsers and other relevant applications (as well as privacy controls, potentially) can automatically reference and *effectively* communicate salient information.

Privacy Risk Models and Privacy Impact Assessment

A broad adoption of FIPPs is not enough to effectively ensure appropriate privacy protection, which relies upon thorough privacy risk assessment, much as security relies on thorough security risk assessment. Ultimately, privacy risk assessment must be based on a rich privacy risk model that includes norms and harms, neither of which is fully addressed in FIPPs. As a result of this gap, practices that are at odds with reasonable expectations and could result in a variety of harms can still be fully compliant with FIPPs. Such a model (or sector-specific models) should incorporate, as appropriate, the latest relevant research in this area. This research (some of which is cited in the report) speaks directly to issues regarding social context, the range of potential privacy harms, and the analysis of novel socio-technical systems. Moreover, such a model or models must also be capable of accommodating new or changed contexts and harms, as well as technical developments that invalidate previous assumptions.

Greater use of privacy impact assessments (PIAs) would provide a useful mechanism, amenable to standardization at some level, for disseminating and applying these privacy risk models. A PIA can be both descriptive and analytical. Unfortunately, many PIAs are heavily weighted toward the former. The aforementioned lexicon would do much to support the descriptive aspect of PIAs. Enhanced privacy risk models, though, would bolster the analytical perspective. For PIAs to be both descriptive and analytical, they must assess privacy risk and force those who use PIAs to actively manage privacy risks. Ideally, individual PIAs would evolve throughout the system development life cycle (SDLC) to support ongoing privacy risk analysis, providing feedback into SDLC activities and guiding the design and the selection of privacy risk controls. A PIA can pay significant benefits, even if not performed until the later stages of the SDLC, particularly if it is based on a privacy risk model that goes beyond potential violations of FIPPs. FIPPs are important, and both privacy and security can be improved with their implementation. But they are insufficient by themselves. They need to be supplemented with a PIA based on enhanced privacy risk models.

As with the proposed lexicon, privacy risk models and/or the PIA templates through which they might be used would benefit from some form of coordination and standardization for purposes of convergence and maintenance. Again, the PPO represents one option, even if just to serve a "meta-coordination" function across multiple sectors.

Do Not Track and Breach Notification

A dataflow-based lexicon and enhanced privacy risk models, applied through PIAs or some other mechanism, would provide a better analytical framework for supporting decision making on any number of thorny privacy issues, including those raised by online behavioral advertising practices and data breach notification.

The appeal of Do Not Track (p.47 in the report) reflects an emerging understanding that simple opt-in and opt-out choices for consent are inadequate for the very different kinds of online data collection and use that consumers may or may not be willing to accept, depending on the circumstances. As indicated above, tracking takes place for a variety of different purposes. However, it also takes place in a variety of different online contexts. Tracking in a social networking context is different from tracking in an e-commerce context and both

are different from tracking consumption of news and opinion. How do the privacy risks differ and how should this be reflected in the selection and implementation of privacy risk controls, be it Do Not Track or something else?

The complexity of tracking online behavior makes a single, simple technical solution like a white list, persistent cookie, or special server header insufficient. There needs to be enforceable means on both the client side and the server side of online interactions in order for a Do Not Track option to be effective. Enforcement of Do Not Track will be at least as important, if not more so, as any technical options made available to consumers or companies. Browser vendors are already working on settings and/or plug-ins to assist consumers in avoiding unwanted data collection (though current offerings do not represent a comprehensive means for consumers to protect against all possible data collection). However, it will be relatively easy for a website to hand-off data collection to a third-party outside of the U.S. and circumvent the enforcement capacity of the U.S. government. How the Department deals with this and other international aspects of enforcing a Do Not Track policy needs to be addressed before the policy is implemented.

Breach notification is also highly contextual and the privacy risks posed by a particular breach are not necessarily straightforward. Certainly, more robust privacy risk models could prove a highly useful tool in weighing the need to provide notice. Indeed, one would expect a risk analysis of a potential breach to flow naturally from a PIA. However the nature of a breach is such that these models must reflect a broad consensus to serve as legitimate instruments for determining whether a breach has exceeded a notification threshold. Otherwise, there is too much room for assessments that are more convenient than rigorous.

Specific Questions

We now address some of the questions noted in the ANPRM. The questions are in **bold**.

7) What are the elements of a meaningful PIA in the commercial context? Who should define these elements?

The two fundamental components of a PIA are description, including data flows, and analysis. The lexicon we have suggested would serve as a resource for descriptions while the enhanced privacy risk models would be the resource for analysis. The development of the lexicon and the privacy risk models could be coordinated by the PPO and carried out by appropriately constituted cross-industry or sector-specific working groups.

8) What processes and information would be useful to assess whether PIAs are effective in helping companies to identify, evaluate, and address commercial data privacy issues?

The assessment effort should include evaluation activities, either cross-industry or sector-specific. Ultimately, the test of PIA efficacy is whether those who carried it out feel they learned something they didn't already know and that this knowledge made a positive difference in how they proceeded. In particular, if the PIA tracks the SDLC, it should be possible to compare the beginning and end states to identify insights gained and responses to them.

13) Are purpose specifications a necessary or important method for protecting commercial privacy?

Purpose specifications are critical to protecting commercial data privacy, as many FIPPs are contingent on purpose. These contingent FIPPs, including collection and retention minimization, cannot be properly implemented in the absence of a clear and sufficiently granular purpose specification.

17) How should purpose specifications be implemented and enforced?

Purpose specifications should be based on a standardized dataflow-based lexicon, supplemented by additional information as needed, but in a prescribed format or structure. Enforcing the purpose specifications is important, as is enforcement of FIPPs, but specific enforcement recommendations are outside our scope of expertise.

25) How can the Commerce Department best encourage the discussion and development of technologies such as "Do Not Track"?

An acknowledgment of the complexity of different tracking methods and the different means necessary to monitor tracking would be a good first step in encouraging the discussion and development of relevant technologies. However, enforcement challenges are going to be an important component of any solution, so the discussion should consider both technical and enforcement issues in tandem.

34) What factors should breach notification be predicated upon (e.g., a risk assessment of the potential harm from the breach, a specific threshold such as number of records, etc.)?

The impact of potential data breaches would be a part of any risk modeling activity and, as in any risk assessment, should focus broadly on relevant threats and the potential impacts on affected individuals. However, absent any generally accepted risk model upon which to base this analysis, notification should not be predicated on a risk assessment. Otherwise, there is too great a possibility of an underestimation of risk.

1828 L Street Northwest, Suite 800
Washington, D.C. 20036
http://usacm.acm.org/usacm
202-659-9711 *tel*
202-667-1066 *fax*

Privacy

USACM Policy Recommendations

Background

Current computing technologies enable the collection, exchange, analysis, and use of personal information on a scale unprecedented in the history of civilization. These technologies, which are widely used by many types of organizations, allow for massive storage, aggregation, analysis, and dissemination of data. Advanced capabilities for surveillance and data matching/mining are being applied to everything from product marketing to national security.

Despite the intended benefits of using these technologies, there are also significant concerns about their potential for negative impact on personal privacy. Well-publicized instances of personal data exposures and misuse have demonstrated some of the challenges in the adequate protection of privacy. Personal data -- including copies of video, audio, and other surveillance -- needs to be collected, stored, and managed appropriately throughout every stage of its use by all involved parties. Protecting privacy, however, requires more than simply ensuring effective information security.

The U.S. Public Policy Council of the Association for Computing Machinery (USACM) advocates a proactive approach to privacy policy by both government and private sector organizations. We urge public and private policy makers to embrace the following recommendations when developing systems that make use of personal information. These recommendations should also be central to any development of any legislation, regulations, international agreements, and internal policies that govern how personal information is stored and managed. Striking a balance between individual privacy rights and valid government and commercial needs is a complex task for technologists and policy makers, but one of vital importance. For this reason, USACM has developed the following recommendations on this important issue.

Recommendations

MINIMIZATION

1. Collect and use only the personal information that is strictly required for the purposes stated in the privacy policy.

2. Store information for only as long as it is needed for the stated purposes.

3. If the information is collected for statistical purposes, delete the personal information after the statistics have been calculated and verified.

4. Implement systematic mechanisms to evaluate, reduce, and destroy unneeded and stale personal information on a regular basis, rather than retaining it indefinitely.

5. Before deployment of new activities and technologies that might impact personal privacy, carefully evaluate them for their necessity, effectiveness, and proportionality: the least privacy-invasive alternatives should always be sought.

CONSENT

6. Unless legally exempt, require each individual's explicit, informed consent to collect or share his or her personal information (opt-in); or clearly provide a readily-accessible mechanism for individuals to cause prompt cessation of the sharing of their personal information, including when appropriate, the deletion of that information (opt-out). (NB: The advantages and disadvantages of these two approaches will depend on the particular application and relevant regulations.)

7. Whether opt-in or opt-out, require informed consent by the individual before using personal information for any purposes not stated in the privacy policy that was in force at the time of collection of that information.

OPENNESS

8. Whenever any personal information is collected, explicitly state the precise purpose for the collection and all the ways that the information might be used, including any plans to share it with other parties.

9. Be explicit about the default usage of information: whether it will only be used by explicit request (opt-in), or if it will be used until a request is made to discontinue that use (opt-out).

10. Explicitly state how long this information will be stored and used, consistent with the "Minimization" principle.

11. Make these privacy policy statements clear, concise, and conspicuous to those responsible for deciding whether and how to provide the data.

12. Avoid arbitrary, frequent, or undisclosed modification of these policy statements.

13. Communicate these policies to individuals whose data is being collected, unless legally exempted from doing so.

ACCESS

14. Establish and support an individual's right to inspect and make corrections to her or his stored personal information, unless legally exempted from doing so.

15. Provide mechanisms to allow individuals to determine with which parties their information

has been shared, and for what purposes, unless legally exempted from doing so.

16. Provide clear, accessible details about how to contact someone appropriate to obtain additional information or to resolve problems relating to stored personal information.

ACCURACY

17. Ensure that personal information is sufficiently accurate and up-to-date for the intended purposes.

18. Ensure that all corrections are propagated in a timely manner to all parties that have received or supplied the inaccurate data.

SECURITY

19. Use appropriate physical, administrative, and technical measures to maintain all personal information securely and protect it against unauthorized and inappropriate access or modification.

20. Apply security measures to all potential storage and transmission of the data, including all electronic (portable storage, laptops, backup media), and physical (printouts, microfiche) copies.

ACCOUNTABILITY

21. Promote accountability for how personal information is collected, maintained, and shared.

22. Enforce adherence to privacy policies through such methods as audit logs, internal reviews, independent audits, and sanctions for policy violations.

23. Maintain provenance -- information regarding the sources and history of personal data -- for at least as long as the data itself is stored.

24. Ensure that the parties most able to mitigate potential privacy risks and privacy violation incidents are trained, authorized, equipped, and motivated to do so.

USACM does not accept the view that individual privacy must typically be sacrificed to achieve effective implementation of systems, nor do we accept that cost reduction is always a sufficient reason to reduce privacy protections. Computing options are available today for meeting many private sector and government needs while fully embracing the recommendations described above. These include the use of de- identified data, aggregated data, limited datasets, and narrowly defined and fully audited queries and searches. New technologies are being investigated and developed that can further protect privacy. USACM can assist policy-makers in

identifying experts and applicable technologies.

Association for Computing Machinery (ACM)

With nearly 100,000 members worldwide, the Association for Computing Machinery is the world's largest educational and scientific computing society, uniting computing educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges. ACM strengthens the computing profession's collective voice through strong leadership, promotion of the highest standards, and recognition of technical excellence. ACM supports the professional growth of its members by providing opportunities for life-long learning, career development, and professional networking.

About the ACM U.S. Public Policy Council

The ACM U.S. Public Policy Council (USACM) serves as the focal point for ACM's involvement with U.S. government organizations, the computing community and the U.S. public in all matters of U.S. public policy related to information technology. Supported by ACM's Washington, D.C., Office of Public Policy, USACM responds to requests for information and technical expertise from U.S. government agencies and departments, seeks to influence relevant U.S. government policies on behalf of the computing community and the public, and provides information to ACM on relevant U.S. government activities. USACM also identifies potentially significant technical and public policy issues and brings them to the attention of ACM and the community. USACM publishes a monthly newsletter, the ACM Washington Update, which reports on activities in Washington that may be of interest to those in the computing and information policy communities, and highlights USACM's involvement in many of these issues. USACM is actively engaged in number of public policy issues of critical importance to the computing community.

For more information about USACM, please contact the ACM Office of Public Policy at (202) 659-9711 or see http://www.acm.org/usacm/.