UNIVERSITY OF CALIFORNIA, BERKELEY

BERKELEY • DAVIS • IRVINE • LOS ANGELES • RIVERSIDE • SAN DIEGO • SAN FRANCISCO SANTA BARBARA • SANTA CRUZ

SCHOOL OF INFORMATION
102 SOUTH HALL # 4600
BERKELEY, CALIFORNIA 94720-4600
(510) 642-1464
(510) 642-5814 Fax

UNITED STATES DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

In the Matter of

Information Privacy and Innovation in the Internet Economy **Docket No. 100402174-0175-01**

COMMENTS OF Deirdre K. Mulligan

June 14, 2010

Thank you for the opportunity to offer comments on this important inquiry. It continues a long tradition of thoughtful inquiry into the resilience of regulatory, market, and self-regulatory mechanisms of privacy protection in the face of disruptive technological change. While continuing this long-standing U.S. tradition, it is distinct in its emphasis on the connections between privacy and innovation. This comment, therefore, seeks to highlight a set of issues where innovation and privacy are inextricably intertwined. Below, I set out three new concepts that are necessary to buttress privacy frameworks (represented in existing and international privacy laws and self-regulatory initiatives reflecting Fair Information Practice Princiles) that are undergirded, to varying extents, by assumptions of market competition and innovation on privacy terms; I discuss the inefficient and counterproductive effect of the current U.S. legal framework governing law enforcement access to personal information, email and private files stored in the Internet; and conclude with a discussion of some perhaps unexpected or unanticipated benefits of the Federal Trade Commission's defacto status as the regulator of privacy in the commercial marketplace, and the importance of transparency-forcing laws, such as the state security breach notification laws, in fostering improved stewardship of personal information.

Competition, innovation and privacy

The belief that competition and consumer trust would foster robust privacy practices in the private sector was a bedrock assumption of, *"A Framework for Global Electronic Commerce,"* issued by the Clinton Administration in 1997, and strongly influences today's dialogue about the necessity of new privacy legislation to govern the private sector. Companies routinely tout the ability of consumers to vote with their feet about privacy in comments such as "competition is a click away"[1] as a market mechanism that protects consumer privacy. On the flip-side the lack of mass exodus after publicized privacy failures has

[1] Miguel Helft, "Google Makes a Case That It Isn't So Big", *The New York Times*, June 28, 2009. http://www.nytimes.com/2009/06/29/technology/companies/29google.html
E.B. Boyd, "Google Privacy Chief: 'We Absolutely Compete on Privacy'", *BayNewser*, January 29, 2010 http://www.mediabistro.com/baynewser/privacy/google_privacy_chief_we_absolutely_compete_on_privacy_150406.asp

been used to defend companies privacy-corrosive actions after the fact. For example, in responding to journalists questions about changes to Facebook's privacy settings CEO Zuckerberg said, "We look at how many people leave the service and deactivate their accounts. Privacy was not a major meme among Facebook users…We have seen no meaningful uptick in the number of people who deleted their accounts."[2]

Surely, there is no doubt that a market for privacy, whether undergirded by a regulatory floor or not, would be beneficial to consumers: For at least some consumers will desire and seek out privacy in excess of whatever regulatory minimum is established. Yet, given the rather heated public outcry about shifts in privacy practices by entities such as Google and Facebook—who both trumpet consumer's ability to exit as an important check on their behavior—followed by limited actual consumer exit, it appears that the threat of exit may be empty, or at best limited.

I submit that for the threat of exit, fueled by robust competition on privacy, to inhibit over-reaching corporate behavior, the following additional market conditions must exist: 1) consumers must be able to easily port their information to alternate providers and services through the use of technical tools supported by open interfaces and data formats; 2) services and products that comprise part of the communication infrastructure of the Internet must be interoperable; and 3) data practices, including those that impact privacy and security, must be accessible in standard formats, using standard terms. The absence of these conditions in today's marketplace undermines privacy and innovation by allowing early market entrants to exploit users' sunk costs and network effects. Companies exploit users' sunk costs, represented in the Web 2.0 environment largely in reams of user-generated content (personal information, contact lists, copyrighted works, etc.), through the standard use of Terms of Service provisions that forbid the use of automated tools by users to interact with their own data. These provisions are buttressed by the deployment of technical protection mechanisms to thwart consumer use of such automated tools. They are then further hardened by background legal rules (including but not limited to the anti-circumvention provisions of the Digital Millennium Copyright Act and the Computer Fraud and Abuse Act) that chill the provision and use of such tools. Companies limit the ability of consumers to interact with individuals using other services in a manner that substantially magnifies the benefit of network effects the company enjoys and further reduces the capacity of consumers to take the value they and their network add to a given service with them. Collectively, the lack of data portability and interoperability stifle innovation and competition on privacy as well as other terms in the current Web 2.0 marketplace.

Data portability and service interoperability must be touchstones of a privacy framework that relies, at any degree, on market competition to advance privacy. Regardless of what additional privacy regulatory constraints or requirements do these market conditions must be considered an integral component of the U.S. privacy framework.

Yet, even if such conditions exist, the difficulty consumers face in parsing and understanding an ever-growing list of privacy policies make privacy concerns difficult to act upon in today's marketplace. For that reason, efforts should be taken to revitalize the work begun at the World Wide Web Consortium in the Platform for Privacy Preferences initiative, and continued in activities such as the Internet Engineering Task Force Geopriv working group, to simplify the ability of companies to communicate privacy practices in simple standard formats and consumers through user agents and other automated

---

[2] Frederic Lardinois, "Mark Zuckerberg talks about new Facebook privacy controls (Live Blog)", May 26, 2010.
https://wave.google.com/wave/waveref/googlewave.com/w+w0tNX3NxA

tools to parse and act upon them. Meta-data about privacy practices is an important element of a competitive privacy environment. The U.S. privacy framework must consider not just the substance of privacy disclosures, but, similar to the ongoing work by the Administration to promote government transparency, it must concern itself with the form and format of such disclosures.

Through data portability, service interoperability, standardization and automation U.S. policy can advance privacy by reducing the transaction costs facing consumers seeking to understand and act upon privacy issues in the marketplace.

Digital Due Process

The Electronic Communications Privacy Act (ECPA), passed in 1986 and not significantly updated since, establishes standards for government access to email and other electronic communications in criminal investigations. It is very much a product of its time—reflecting both the technology and its specific use by businesses and consumers at the time of its enactment. While the law remains a critical and indispensable aspect of the U.S. privacy framework, it is mired in the technological past and therefore distorts the marketplace by drawing privacy-lines that pit innovation against privacy at nearly every turn. The law must be updated to provide consistent privacy protections in a technology-neutral manner that respects the growing dependency of individuals, companies, and the government on the internet for an increasing array of sensitive activities.

Specific aims of ECPA reform can be found in the comments of the Digital Due Process coalition, of which I am a member and comment signatory.

Leveraging the existing benefits of the current U.S. legal framework

I wish to draw the attention of the Department to a set of forthcoming articles by Kenneth Bamberger and me.[3] These articles present findings from the first study of corporate privacy management in fifteen years, involving qualitative interviews with Chief Privacy Officers identified by their peers as industry leaders and information from internal organizational charts, process documentation, and discussions with managers responsible for policy implementation.

In Privacy *on the Books and on the Ground*, we identify important regulatory elements neglected by the traditional story of privacy in the U.S.—the emergence of the Federal Trade Commission as a privacy regulator, the increasing influence of privacy advocates, market and media pressures for privacy-protection, and the rise of privacy professionals—and trace the ways in which these players and tools supplement a privacy debate largely focused on processes (such as notice and consent mechanisms) with a growing corporate emphasis on substance: preventing violations of consumers' expectations of privacy. This article reveals the importance of two alterations to the U.S. legal landscape that have been underappreciated in the literature and should be considered in the context of reforms to the U.S. and global privacy frameworks. First, the emergence of the FTC as a roving regulator with broad yet ambiguous power to evaluate privacy practices in the marketplace through its consumer protection lens. The FTC's mandate to protect consumers from "unfairness" and "deception" permits dynamic regulation that evolves with changing contexts, and forces corporate practices to develop accordingly. Second, state security breach notification laws raised the soft and hard costs of mismanaging personal information.

---

[3] Bamberger, Kenneth A. and Mulligan, Deirdre K., *Privacy on the Books and on the Ground*. Stanford Law Review, Vol. 63, 2010; UC Berkeley Public Law Research Paper No. 1568385. Available at SSRN: http://ssrn.com/abstract=1568385; and Bamberger, Kenneth A. and Mulligan, Deirdre K., *Catalyzing Privacy*, (currently under submission with Law & Policy)

Together these changes have led companies to integrate substantive considerations of consumers' privacy expectations into their workflows, rather than leaving privacy to the lawyers and their process-based "click through if you 'consent' to the privacy policy" approach.

In *Catalyzing Privacy* we document specific shifts in corporate privacy management that have occurred during the period of regulatory shift described in *Privacy on the Ground*, including the increased power of corporate privacy leaders within the corporate and their external orientation, privacy reframed as a risk management function and integrated into mechanisms that relate to core firm values, and privacy's operationaliztion within the firm through distributed networks of dedicated privacy professionals and specially-trained employees within business units empowered with practices and tools that assist with identifying and addressing privacy during the design phase of business development.

These two articles provide several important insights for what we consider to be the "third wave" of privacy initiatives—tort laws being the first, data protection the second, and security breach notification and consumer protection analysis marking the beginning of the third—that should inform the process begun with this Inquiry.

Our account supports the argument that calls for federal regulation structured exclusively around fair information practice principles are ill-advised. Efforts to expand procedural mechanisms to empower individuals to control their personal information, must not eclipse robust substantive definitions of privacy and the protections they are beginning to produce, or constrain the regulatory flexibility that permits their evolution, for both have proved important tools in efforts to limit and police corporate over-reaching, curb consumer manipulation, and define and protect a shared expectation about the personal sphere in the marketplace. Within the corporation our interviewees indicated that Fair Information Practice Principles were insufficient to guide corporate behavior—particularly in times of profound technical or market change—and could unintentionally pigeonhole privacy as a purely legal matter. In contrast, it appears that the relationship between consumer protection and trust has allowed the CPOs against a dynamic external backdrop of engaed regulators, activists, academics and press, to transform internal perceptions about privacy from a compliance oriented, rule dominated, legal hurdle to be addressed at the end stage of product design, to a consultation and dialogue about how technical designs, business strategies, and policies can respect consumers' expectations and support trust in their companies. Relatedly, our interviewees echo the growing regulatory concern that absent a substantive touchstone, a data-protection regime can focus resources on developing a host of often meaningless consent processes, which must be designed and redesigned in an effort to do better—where the meaning of "better" is unclear and only partially tethered to individuals' expectations of privacy. Thus, any reform should foster the FTC's enforcement activities aimed at protecting consumers' reliance on conventional information flows because they have brought greater substance and meaning to an area routinely critiqued for its formalism. Viewing privacy as a context-dependent set of practices and expectations protects against corporate and bureaucratic desires to reduce it to a set of a priori process-oriented rules, and the legalization and regularization that critics and proponents alike claim plague data protection. And protecting existing social norms about information use, rather than leaving each individual to the mercy of the marketplace, is key to addressing both collective and individual interests.

Second, procedurally, our research identifies the important role of the forums provided by the FTC as sites for structuring and advancing a collective understanding of privacy among advocates, industry, academics and regulators. The collective engagement facilitated through these broad, inclusive stake-holder activities has yielded both substantively groundbreaking outcomes—a divergence from caveat emptor with respect to privacy disclosures—as well as unique changes in corporate privacy management. The FTC's combination of enforcement threats with its centrality in fostering a social network of entrepreneurial privacy advocates offers a model for avoiding both the shortcomings of static

top-down command-and-control regulatory approaches and the ways in which reliance on bottom-up self-regulation alone can subvert public goals by private interests. This model should guide the choice and design of whatever regulatory institutions take the lead on information privacy in the corporate sector moving forward. They must both possess and use regulatory tools that exploit market, corporate and advocacy capacity to develop collective understanding of risks and solutions to future privacy problems.

Finally, our articles begin to illuminate the ways in which corporate privacy professionals impart meaning and structure to societal privacy concerns within corporations. Debates about the establishment of a dedicated privacy agency in the United States emphasize the importance of governmental privacy expertise in shaping the rules governing corporate behavior. The U.S. may embrace a more formal institutional structure for privacy. And this would likely yield several important domestic and international benefits. However, whether the vision of a centralized privacy expertise within a free-standing or existing government agency is realized, it is important that regulators and civil society continue to leverage the broad, vibrant and entrepreneurial "cadre of specialists" on privacy that has developed in the private sector—within companies, advocacy organizations and academia. In the absence of a DPA staffed with data protection experts, and faced with increasing ambiguity as to what privacy requires, corporations depend on these new professionals to guide them through the challenges wrought by evolutions in technology and business practice. These professionals do not view themselves as compliance officers, but as norm entrepreneurs. Empowered by external threats that support their entrepreneurial efforts, they offer a unique capacity to embed privacy—as trust and consumer expectations—into the corporate psyche as well as business operations. Choices about regulatory form should be attentive to the important bridging role these insides play particularly as society becomes more pervasively networked, and privacy protection requires ongoing and on-the-ground attention to dynamic privacy interests that manifest in very different ways within different firms.

In conclusion, as the DOC continues this Inquiry and the broader domestic and international privacy community reflects upon the key global instruments of privacy and data protection, our research underscores the importance of empirical inquiry and thick institutional engagement in considering contested issues of regulatory strategy, technological complexity, social and institutional networks, and the protection of individual and communal interests in the private sphere. If privacy can be protected in an increasingly connected world, debates over its formal regulation must increasingly be informed by the ways that today's frameworks operate on the ground.

I look forward to engaging with DOC and other stakeholders on this important topic.

Sincerely,

Deirdre K. Mulligan