patientprivacyrights

February 18, 2011

Federal Trade Commission
Office of the Secretary
Room H-113, Annex
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: FTC Staff Preliminary Report on Protecting Consumer Privacy - File No. P095416

We applaud the FTC for creating a report focused on protecting consumer privacy. The proposed framework upholds many of the practices we believe in: informed consumer consent, privacy protection and data security, and greater transparency.

Patient Privacy Rights is the leading consumer voice for building ethical, trustworthy health IT systems. We have over 12,000 members and lead the bipartisan Coalition for Patient Privacy, representing 10.3 million Americans. We seek to restore the right to informed consent, and the right to health information privacy in electronic systems. Individual consent and control are imperative for patients and consumers to willingly participate in electronic systems and data exchanges.

We promote privacy-enhancing technologies and practices, inside and outside of the healthcare system. Patients are concerned about health data privacy. Consumers also feel strongly about the privacy of other personal information. Neither is aware of how their data is being used. All companies and businesses should be required to comply with the proposed framework; and all consumer data, however limited, should be held to the same stringent privacy and security standards and protections. Effective data privacy requires comprehensive and meaningful protections that apply everywhere data flows.

Anonymizing/De-Identifying Data: A Continuing Myth

> Currently, there is no effective way to anonymize data sets and prevent re-identification. As the amount and variety of publicly available information about individuals grows exponentially[1], the ability to re-identify the data also grows exponentially. The work of Latanya Sweeney, Paul Ohm, and Mark Rothstein is well known, proving that de-identifying data in a way that prevents re-identification is EXTREMELY difficult. One example is the large-scale re-identification of a Netflix database; Netflix posted "de-identified" movie ratings data online, which were re-identified by UT computer scientists using public

[1] Narayanan, Arvind, and Vitaly Shmatikov. "Privacy and Security: Myths and Fallacies of "Personally Identifiable Information"" *Communications of the ACM* 53.6 (2010): 24-26. Print.
http://www.cs.utexas.edu/users/shmat/shmat_cacm10.pdf

records. Any single data set may be de-identified, but combined with other data sets it can again become personally identifiable information. Therefore de-identified data should be protected with the same privacy practices as all sensitive consumer data, and require informed consent for use. This is even more critical when it comes to de-identified data sets of protected health information (PHI). PHI is the most sensitive data of all, and every consumer is a patient at one time or another. It is common practice for the data mining industry to combine multiple sources of de-identified information into real-time, sensitive, identifiable profiles of individuals, which can be used to affect job and financial opportunities, and other critical aspects of patients' lives. Patients and consumers must be aware of who has their information, must opt-in before data is collected, and there should be no secret data bases. Individuals must control where personal data is held and where it goes.

Online Behavioral Advertising: Do Not Track

We support the option for consumers to opt-out of behavioral advertising through a "Do Not Track" list. Every browser and website that tracks user information should have a clear and visible way consumers can prevent their online actions from being tracked. Patient Privacy Rights has received countless complaints, asking how or why individuals had been targeted for prescription drugs or other health-related materials about sensitive health issues they did not knowingly disclose. Many patients use online resources such as insurance sites, personal health records, health information or management, or research sites. Websites often collect and use information for behavioral advertising and sell real-time individual consumer profiles. Most consumers are unaware. The WSJ's series on data mining, called "What They Know"[2] reveals some of the many secret collectors and users of Americans' personal information. The "Do Not Track" option, along with a framework requiring upfront and understandable privacy policies, transparency about what information is collected, consent for data use, and ensuring the data is private and secure will help prevent the collection and sale of personal digital profiles without consent.

In conclusion, we commend the FTC for recognizing the urgent need for consumer privacy protection, and for making clear that even "de-identified" consumer data should be treated as sensitive and require consent before use. The current environment where consumers cannot control who collects their information, and secret data bases of personal individual profiles can exist, is untenable. We believe that federal legislation is essential for the proposed framework to be an effective data privacy regime. When it comes to personal, sensitive information, allowing industry to self-regulate is like asking the fox to guard the hen house. The words "consumer privacy" will continue to be an oxymoron unless protected by law and robust enforcement. We also want to support the comments submitted by Privacy Rights Clearinghouse[3] . Patient Privacy Rights' focus is on securing health information privacy, but increasingly health data privacy is threatened by the use of advanced data mining techniques of websites far from the healthcare system.

[2] http://online.wsj.com/public/page/what-they-know-digital-privacy.html
[3] http://www.privacyrights.org/ftc-protecting-consumer-privacy-report-comments

P.O. Box 248 • Austin TX • 78767
Phone 512.732.0033 • Fax 512.732.0036

http://patientprivacyrights.org

We thank the FTC for inviting and considering public comment, and continuing to work toward consumer and *patient* privacy.

Deborah C. Peel, MD
Founder & Chair

Katherine Johnson
Director of Communications

P.O. Box 248 • Austin TX • 78767
Phone 512.732.0033 • Fax 512.732.0036

http://patientprivacyrights.org