COMMENTS OF THE AMERICAN CIVIL LIBERTIES UNION

OF NORTHERN CALIFORNIA

TO THE FEDERAL TRADE COMMISSION

Re: Privacy Roundtables – Comment, Project No. PO95416

BY NICOLE A. OZER, ESQ
TECHNOLOGY AND CIVIL LIBERTIES POLICY DIRECTOR,
ACLU OF NORTHERN CALIFORNIA

December 21, 2009

Introduction

The American Civil Liberties Union of Northern California (ACLU-NC) hereby submits comments to the Federal Trade Commission for the Federal Trade Commission's "Exploring Privacy: A Roundtable Series."

The ACLU-NC, based in San Francisco with a second office in San Jose, is the largest ACLU affiliate in the nation, with over 50,000 members. For 75 years, the ACLU-NC has been at the forefront of every civil liberties battle in the state. In response to a growing need to address issues related to privacy, free speech, and new technology, it launched its Technology and Civil Liberties Program in December 2004.

The Commission's second Privacy Roundtable seeks to answer the question, "What challenges do innovations in the digital environment pose for consumer privacy, and how can those challenges be addressed without stifling innovation or otherwise undermining benefits to consumers?"

This question fits squarely into the focus of the ACLU-NC's new online privacy campaign, Demand your dotRights (www.dotrights.org). The campaign's goals are: (1) to create awareness and debate around the privacy implications of emerging technologies; and (2) to mobilize community members, policymakers, and businesses to work together to upgrade privacy protections to match our modern world.

The Demand your dotRights campaign's policy papers, written materials, and multimedia and technology-based public education materials focus on the balance between privacy and innovation related to social networking platforms, cloud computing, mobile services, digital book and video privacy, search, and online photos sites. We have also recently produced, *Privacy and Free Speech: It's Good for Business*, a primer of real-life case studies and hands-on tools to help companies plan how to build privacy and free speech safeguards into the business development process and avoid mistakes that can lead to government investigations and fines, costly lawsuits, and loss of customers and business partners. This primer has been widely-

distributed in the venture capital, entrepreneurial, legal and technical communities and received praise from diverse audiences.[1]

We hope that some of our recent work will be useful to the Federal Trade Commission in exploring how to address privacy challenges related to innovations in the digital environment. In these comments we will briefly discuss two areas of innovation—cloud computing and the growth of third party applications in social networking—and how these two innovations pose challenges related to notice to consumers and transparency about third party access to personal information. In both cloud computing and social networking, consumers are not currently given adequate notice of how often personal information is disclosed. Without such information, consumers cannot make informed decisions as to whether and to what extent to trust companies with their personal information. Recent work on the ACLU-NC's Facebook quiz about Facebook quizzes also reveals that the growth of third party applications on social networking platforms has raised additional issues related to notice and choice for many users.

Cloud Computing

"Cloud computing" services—tools accessed via the Internet that allow consumers to easily create, edit, and store documents (such as private photos and videos, calendars and address books, diaries and journals, and budgets and financial spreadsheets) online—are growing in popularity as Internet speeds increase and the cost of data storage drops. According to a 2008 Pew Internet & American Life Project memorandum (Pew memo), at least 40% of American Internet users, and at least 59% of such users in the 18-29 age range, have engaged in some form of cloud computing activity by either storing data online or using Web-based software applications.[2] From the user perspective, cloud computing services make the transition from offline to online activities increasingly seamless. But while it may be easy for consumers to transition information into the cloud, privacy protections for that personal information may not transition as smoothly.

Storm Warning for Information Disclosure

The Electronic Communications Privacy Act (ECPA), which is supposed to supplement Fourth Amendment privacy protections and safeguard the privacy of consumer electronic communications, in transit or in storage, has not been updated since 1986—twenty three years ago.[3] This law, written more than a decade before the Internet as we know it even existed and far before the advent of cloud computing, may not fully apply to all the different ways that consumers are interacting with cloud computing services today. ECPA provides protection where content is stored with a service "solely for the purpose of providing storage or computer

[1] All materials available at www.dotrights.org

[2] *See* PEW INTERNET & AMERICAN LIFE PROJECT, USE OF CLOUD COMPUTING APPLICATIONS AND SERVICES [hereinafter PEW MEMO] at 5, Sep. 2008, *available at* http://www.pewinternet.org/Reports/2008/Use-of-Cloud-Computing-Applications-and-Services.aspx?r=1. This study found that 40% of users used multiple cloud computing services under their definition, which includes Web-based email, and thus used at least one cloud computing service under ours. More specifically, the study found that 34% of Internet users store personal photos online, 29% use online applications, 7% store personal videos, 5% pay for file storage, and 5% use online hard drive backup services. *Id.* at 1. Among users in the 18–29 age range, 50% store personal photos. 39% use online applications, 14% store personal videos, 9% pay to store computer files, and 7% back up hard drives to an online site. *Id*. at 5.

[3] Electronic Communications Privacy Act of 1986, 18 U.S.C §§ 2510-2711 (2000).

processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing."[4] Does this mean that there may be no ECPA protection if a consumer uses a cloud computing service that provides collaboration and sharing functions or utilizes a targeted advertising model based on mining information contained in the documents? Technology and business model innovations have outpaced upgrades in privacy law and it is not clear what privacy protections consumers have against disclosure of their sensitive information to third parties in the cloud computing context.

A lack of clarity about privacy protections in the cloud computing context is worrisome to consumers and should be worrisome to the FTC. It is time to update privacy law so that it keeps pace with how individuals are utilizing new technology and current business models. It is not good for consumers or business when individuals have to worry that what goes into the cloud might not stay in the cloud. Consumers are already "very concerned" by scenarios in which their cloud computing information ends up being used in ways that they did not intend, such as when companies:

- Turn their data over to law enforcement (49% of users);
- Keep copies of files even after they try to delete them (63%);
- Analyze data in the cloud for targeted advertisements (68%);
- Use cloud documents in marketing campaigns (80%); and
- Sell files to others (90%)."[5]

The Pew study summarized the underlying message of consumers to cloud computing providers as, "Let's keep the data between us."[6]

Notice and Transparency is an Important First Step

Consumers are concerned about losing control of personal information and currently many are not able to make an adequately informed decision about how well a particular company is protecting their information because few companies will provide any data about how often personal information is requested and disclosed to third parties and the government. For example, Google, which runs both Google docs and Picasa photo services, has continually refused to state the number of requests it receives for consumer information or its number of disclosures.[7] When recently asked by Wired News to make this information public, Google again refused to answer, stating that "We don't talk about types or numbers of requests to help protect all our users."[8] It is unclear how Google's refusal to be open with its customers about how often information is disclosed helps protect users. Wired has been asking Google to disclose this information since 2006, as has the ACLU of Northern California. This lack of transparency about how often online companies disclose consumer information is systemic. Few companies have even provided partial information about disclosure. Verizon only recently admitted that it

[4] §§ 2702(a)(2)(B), 2703(b)(2)(B).
[5] *See* PEW MEMO at 4, 10.
[6] PEW MEMO at 1, 10.
[7] http://www.wired.com/threatlevel/2009/12/google-talks-out-its-portal/.
[8] *Id*.

receives "tens of thousands of requests" annually from law enforcement.[9] Facebook has admitted it receives up to 20 law enforcement requests per day but has not provided consumers with any information about disclosures to third parties in the civil context.[10]

It is very difficult for consumers to feel confident about utilizing cloud computing platforms if they are left to worry that their personal information is far more vulnerable in the cloud than it is on their hard drive or in their filing cabinet because they have no basic information about disclosure rates. The Fair Information Practice Principles notes that "without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information." It goes on to state that such notice should give "consumers meaningful and effective notice of what will happen to the personal information they are asked to divulge."[11] Without basic information about disclosure, consumers do not have meaningful and effective notice about what can happen to their personal information stored or processed with online services and cannot make an informed decision about whether to utilize such services. This lack of notice can lead some consumers to underestimate the implications of using such services, while others might have more fear than necessary.

Reporting Mechanism Necessary to Improve User Notice and Awareness

To ensure that consumers have the information that they need to make a reasoned and informed decision, there should be a mechanism in place to require all online companies to keep an annual record of all information requests. And, unless information pertaining to a particular request or set of requests is specifically prohibited by law, that company should submit to the FTC an annual report detailing:

(A) The number of Federal warrants, State warrants, grand jury subpoenas, civil and administrative subpoenas, and court orders received in the previous year;

(B) The number and types of action taken by the company for each category of request;

(C) The number of individuals whose personal information was disclosed by the provider by category of request;

(D) The type of personal information disclosed by category of request; and

(E) The total amount of money received by the company to fulfill each category of request.

The FTC should then make all reports accessible to the public in an online, searchable format within a reasonable time after filing. Any company with an online privacy policy should also create a prominent hyperlink from the disclosure section of its privacy policy to its latest report.

As cloud computing continues to develop and expand and the boundary between personal devices and the Internet "cloud" becomes less meaningful, it is imperative that privacy laws and policies are updated so that users do not have to choose between using cloud computing and

[9] *Id*.
[10] Nick Summers, Facebook's *'Porn Cops' Are Key to Its Growth*, NEWSWEEK, May 18, 2009, *available at* http://www.newsweek.com/id/195621.
[11] Fair Information Practice Principles, FTC, http://www.ftc.gov/reports/privacy3/fairinfo.shtm

keeping existing control over their personal information. An immediate first step to better protect user privacy would be for the FTC to lay the groundwork for greater notice and awareness for consumers by supporting mechanisms for companies to report about disclosure rates to third parties and the government. Such a reporting mechanism would not stifle innovation or undermine benefits to consumers. Indeed by helping to ensure greater transparency, it may build consumer trust and help lead to additional privacy and security innovations in the cloud computing arena.

Social Networking

Online social networking is one of the fastest growing activities on the Internet. Hundreds of millions of Americans use sites like Twitter, MySpace, Facebook, and LinkedIn to connect and network with others. Over 100 million Americans are using Facebook—posting contact information, personal photos and videos, up-to-the-minute status updates about activities, and lists of friends and organizations that they support.[12] Many users, even users that one might think would be relatively sophisticated, do not realize that once this information is posted or collected by Facebook, it can end up in the hands of third parties. At a recent presentation at a Bay Area law school, a student asked, "Wait, do you mean that if I make my Facebook profile private, it isn't private to the government or third parties?" Not only do social networking sites have many of the user notice and awareness issues related to disclosures that are discussed above, but consumer information is also increasingly accessed by third party application developers on social networking sites, often without the real knowledge or informed consent of consumers. Facebook's platform is a prime example.

Lack of Notice and Consent for Third Party Application Access

Facebook's developer platform allows companies to create games and quizzes that Facebook users can install on their profiles. Every month, more than 70% of Facebook users run an application or take a quiz.[13] Even if a user has selected the most restrictive privacy settings available, running a third party application like a quiz allows the developer to gain nearly unfettered access to a user's profile information, including religion, sexual orientation, political affiliation, photos, events, notes, wall posts, and groups.[14] And every time that individual takes a quiz, they might not just be sharing information in their own profile with the application developer, but also the personal information of each one of their friends. Every Facebook user is automatically set to share information with the application developer whenever a friend runs an application.[15] Facebook's current position is that if you are friends with someone, you are friends with all of the applications they decide to run as well. This means that in order to minimize the information being accessed by applications, consumers must: (1) know that applications can access their profile information when a friend takes a quiz, and (2) be able to find the specific setting to opt-out of sharing the information they still have control over.

---

[12] Facebook, *Statistics*, http://www.facebook.com/press/info.php?statistics (last visited Dec. 18, 2009).
[13] *Id*.
[14] *See* ACLU of Northern California, "Take Our Quiz: See What Do Facebook Quizzes Know About You!", http://www.aclunc.org/issues/technology/blog/take_our_quiz_see_what_do_facebook_quizzes_know_about_you.shtml (last visited Dec. 21, 2009).
[15] *See* ACLU of Northern California, "What Does Facebook's Privacy Transition Mean For You," http://dotrights.org/what-does-facebooks-privacy-transition-mean-you (last visited Dec. 21, 2009).

When the ACLU-NC produced a Facebook quiz of its own to give consumers a behind-the-scenes look at what information third party applications could access about friends, people were shocked at what they learned.[16] Here are just a few of the comments made by Facebook users who took the quiz:

- "Thanks for putting this together, it's ABSOLUTELY crucial that someone exposes this publicly. I have my privacy settings maxed out and this quiz still exposed tons of information about my network which is why I never allow 3rd party apps on facebook.
- I had no idea ... THX this opened my eyes!
- Wow, this was scary... and insightful. It makes me think twice.
- Wish this information had been posted BEFORE all these quizzes were taken and posted.
- If you choose to take quizzes and expose your information is your decision. But to expose your friends information at the same time without their permission is unacceptable. And it is unacceptable for FB to allow this and for developers to do it.
- Everyone should take this quiz and demand that Facebook safeguard our information!!! [17]

To date, more than 125,000 people have taken the ACLU's Facebook quiz about Facebook quizzes and more than 43,000 consumers have signed a petition demanding that Facebook change its default settings.

Facebook's December Privacy Changes Did Not Address Application Privacy Issues

Facebook's changes to its privacy settings in December 2009 did not resolve the privacy problems related to access by third party applications. Rather, Facebook made it **more difficult** for users to prevent information from being accessed by third party application developers.[18]

Before the December changes, a user could completely opt-out of sharing any information with applications that were run by friends as long as the user herself did not run any applications. Under this previous system, users had to give up their ability to use applications themselves but it did provide some mechanism for those who wanted nothing to do with applications to ensure that their information was not being accessed by these third parties. Additionally, if a user wanted to run applications, she could still take advantage of particular privacy settings and opt-out of sharing any information other than her name, networks and friends list with third party application developers.

As a result of the December 2009 changes:

- A user can no longer completely opt-out of sharing information with applications even if she does not want to run any applications herself.

[16] Available at http://apps.facebook.com/aclunc_privacy_quiz. More information at www.dotrights.org.
[17] Selected user comments posted to Wall, What Do Quizzes Really Know About You, http://www.facebook.com/apps/application.php?id=114232425072.
[18] Resource page detailing the Facebook settings before and after the December changes available at http://dotrights.org/what-does-facebooks-privacy-transition-mean-you

- A user has lost the ability to keep her profile picture, fan pages, and gender from being shared with any application that a friend runs.

These changes mean that even the most privacy conscious and informed Facebook user, who is able to find and take advantage of every privacy setting currently available on Facebook,[19] still has no ability to keep information like her profile picture, fan pages, and gender from being accessed by the developer of any application that is run by a friend. The user is also given no notice of the applications that friends are running. [20]

Third Party Application Sharing Should Be Opt-In

More than 43,000 consumers have signed an ACLU petition demanding that Facebook change its default settings and not allow third party applications to access information about users without their opt-in consent.[21] The FTC should help ensure that consumers have proper notice and choice and that personal information is not being accessed by third party applications without the appropriate opt-in consent of consumers. The FTC's involvement is essential because advertising business models strongly incentivize companies to gather and share as much personal data as possible. Industry experts at the last FTC Privacy Roundtable reported that companies can currently expect up to 10 times the revenue for advertisements based on behavioral advertising data. [22] In fact, some Facebook quizzes are developed by advertising companies in order to learn more about consumers and target advertisements.[23] With such strong economic motivation for companies to access personal information about consumers, there is a disincentive for companies to make it easy for individuals to opt-out.

Conclusion

Cloud computing and the rise of social networking and third party application developers are two important areas where the FTC needs to examine the current level of consumer notice and awareness and how it is negatively impacting the ability of consumers to make informed choices. Important first steps to addressing privacy challenges in two emerging areas while not stifling innovation or undermining benefits to consumers would be to work to ensure that: (1) consumers have proper notice about how often companies disclose consumer information; and (2) consumer social networking information is not shared with third party developers without opt-in consent. We look forward to discussing these and other ideas during the upcoming Privacy Roundtables.

---

[19] The settings that still do exist for users to be able to have some control over access by third party application developers are difficult to find and were not included as part of the "transition tool" that was released by Facebook. *See id* for more information.

[20] *Id.*

[21] Petition available at https://secure.aclu.org/site/SPageServer?pagename=Nat_Petition_Facebook.

[22] Transcript of Panel 3, Exploring Privacy: An FTC Roundtable Discussion (Dec. 7, 2009), http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/transcripts/120709_sess2.pdf.

[23] *See, e.g.*, Pangea Media: Target your audience better with fun quizzes, Nov. 5, 2009, http://www.pangeamedia.com/in-the-news/pangea-media-target-your-audience-better-with-fun-quizzes (last visited Dec. 21, 2009) (Pangea Media CEO Seth Lieberman says " We use the quizzes as a framework to engage with our customers, understand a little about who they are, what their interests are, and then deliver them targeted results based on that.").