Commissioner Pamela Jones Harbour

Remarks Before Third FTC Exploring Privacy Roundtable
Washington, D.C. via Barcelona, Spain
March 17, 2010

INTRODUCTION

Good morning, and welcome to the third FTC Exploring Privacy Roundtable. Thank you, for the introduction. And let me personally thank all of the wonderful FTC staff who have worked tirelessly over the past year to make these events happen.

You all may be wondering where I am this morning, and why I am coming to you by video. I am in Barcelona, Spain. A few hours ago, I delivered one of the keynote speeches to the Cloud Security Alliance SecureCloud 2010 event. But I certainly did not want to pass up the opportunity to deliver remarks at today's third and final Privacy Roundtable.

When I spoke back in December, I mentioned that I would soon be leaving the Commission. This time, I really am serious. I recently announced that I will depart on April 6th. This will be my final public speech, albeit from 3500 miles away. For the last time, I note that my comments today reflect my own views, not necessarily those of the Commission or any other individual Commissioner.

I've said it so many times before, and I will say it again today: protecting consumer privacy is of utmost importance. It must be a driving force for businesses in all stages of product and service development. Unfortunately, many of the companies that consumers look to as leaders – and that we expect to be leaders – still have not taken this message entirely to heart.

First, I want to challenge what I see as a dangerous precedent, being set by some of the biggest and most influential technology companies, when they publicly expose consumers' data.

Second, I want to challenge companies that are not adequately protecting consumers through SSL technology.

PRIVACY IS A FUNDAMENTAL RIGHT

At the last Roundtable in Berkeley, I discussed the comments of a technology executive who claimed that privacy expectations and "norms are changing." More recently, since the Berkeley event, the press has recycled the comments of another prominent tech executive who stated, "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place."

Speaking for the last time as a regulator, let me be very clear: I could not disagree more with that assertion. ***Privacy is a fundamental right that people do care about.*** And I believe the Commission, and my fellow Commissioners, share this opinion. The Commission will continue to view privacy as an important value, as reflected in the norms and expectations of consumers, until it is proven that consumers feel otherwise about their privacy. The Commission will continue to evaluate consumers' preferences, and armed with these insights, I hope and expect that the Commission will continue to shape the conversation about the intrinsic value of privacy. But make no mistake: the Commission will unfailingly step in to protect consumers where we believe the law has been violated, and that includes violations relating to privacy promises.

WHAT’S ALL THE BUZZ ABOUT?

I’m going to be even more specific in my admonition, to provide some concrete examples for today’s discussion. The recent launch of Google Buzz was, quite frankly, ***irresponsible*** conduct by a company like Google. I would use that same word to describe the prior rollout of Facebook’s new privacy settings, as well as the November 2007 release of Facebook Beacon, but for now I will focus on the Buzz example.

Google is one of the greatest technology leaders of our time. Google consistently tells the public to “just trust us,” and has adopted as a company motto, “Do no evil.” We have high expectations for Google as a corporate citizen. But for me, based on my observations, I do not believe that consumer privacy played any significant role in the release of Buzz. In the rush to compete with Facebook, FourSquare, Twitter, FriendFeed, Loopt and a host of other companies, it appears that Google really did not think through the privacy implications of this launch.

New technologies such as Buzz, like some of the updated features offered on Facebook, represent a laudable effort to help consumers integrate and make sense of the daily overload of information that bombards them via email, chat, photos, blogs, tweets, news feeds, and the like. Today, consumers tend to have separate online accounts for a variety of services, and often they maintain multiple profiles to separate personal and professional uses. Plus, many companies do one thing well, and accordingly consumers are willing to enter relationships with multiple firms. A common characteristic of the most successful Web 2.0 companies is that they thrive on network effects – the greater the number of users or number of inputs, the better the experience – which further enhances the trend toward interacting with multiple data sources.

When Buzz was launched, Google described its function as "finding relevance in the noise." It is no wonder that, seeking to capitalize on network effects, Google decided to build its service by turning to its installed base of approximately 150 million Gmail users. Unfortunately, ***none of those users were consulted*** before Google unilaterally decided how best to use their data.

When users created Gmail accounts, they signed up for email services. That is their primary use of Gmail. Several years ago, when Google first introduced chat, many users were taken aback that their email address book contacts were automatically suggested as chat contacts. Publicly there was a backlash, and Google rolled back its "Talk" offering.

Google apparently failed to learn from prior mistakes. Buzz was designed as a social net for users, but the net was cast too widely. News reports indicate that the company claims to have tested Buzz extensively, with thousands of employees. The problem is, Google employees are in no way representative of the Gmail user base (a combination of young, old, tech-savvy, novice, and so on). The Buzz Product Manager admitted as much, saying that "Getting feedback from twenty thousand Googlers isn't quite the same as letting Gmail users play with Buzz in the wild."

Think about it: when Gmail first emerged, social networking was barely even a reality. When consumers, especially early adopters, created their Gmail accounts, their expectations did not include social networking. In my view, therefore, a reasonable consumer would consider the initial opt-in of Buzz to be a material change in her relationship with Google. Consumers, not companies, should exercise the ultimate decision on whether they want to sign up for new "features" that might expose additional data.

I am especially concerned that technology companies are learning harmful lessons from each other's attempts to push the privacy envelope. Of course, providing new features to users, and making the user experience more enjoyable, are excellent goals. These efforts may win new users while also building additional loyalty in existing users. But even the most respected and popular online companies – the ones who claim to respect privacy – continue to launch products where their guiding privacy principle appears to be, “Throw it against the wall, see if it sticks – and if not, we can always pull it back.” Deeds speak louder than words, and this is turning into a dangerous game of “copycat” behavior. And unlike a lot of tech products, consumer privacy cannot be run in beta. Once data are shared, control is lost forever. In the extreme, it is only a matter of time before one might imagine the introduction of new “features” that incorporate, for example, genomic information, or data from personal health records. The privacy stakes will only get higher.

I recognize that, perhaps, companies continue to take a “testing the waters” approach to privacy because no regulatory agency has sent a clear message that such behavior is unacceptable. In my opinion, that message may need to change. I would like to see the Commission take the position of intolerance toward companies that push the privacy envelope, then backtrack and modify their offerings after facing consumer and regulator backlash.

In the meantime, however, companies should exercise greater responsibility, and be more circumspect before launching “game-changing” products. Computer algorithms should not be trusted to interpret consumers’ privacy expectations. Consumers still have an expectation of privacy. Those norms do not change, and cannot be assumed away, every time a company wants to compete in a new market. We cannot accept a new paradigm where products and services do not offer user choice, materially changing the bargain consumers understood when they established their relationship.

(IN)SECURE SOCKET LAYER TECHNOLOGY

I do not want to be accused of harping only on Google, so let me turn to my second admonition, which is targeted at a large number of prominent firms, and which addresses an important issue of data security. I worry that many consumer-facing computing services have significant data security vulnerabilities, especially services offered in the cloud.

Encryption technology is already built into every popular web browser. But here is an unpleasant truth: many popular services employ encryption technology only to transmit initial login information, such as user names and passwords. All subsequent data are sent in the clear, unencrypted. This problem affects services such as Microsoft Hotmail, Yahoo Mail, Flickr, Facebook, and MySpace. This practice exposes consumers to significant risks when they connect to popular cloud-based services using public wireless networks in coffee shops, airports, and other public hot spots. Without encryption, user data can be easily intercepted, using freely available off-the-shelf hacking tools.

I spoke last fall at the International Conference of Data Protection and Privacy Commissioners in Madrid. One of the most memorable speakers was a White Hat, or ethical hacker (for those not in the know). During his presentation, the hacker demonstrated how easily he could break into a netbook computer, in a matter of mere minutes. It was very sobering, indeed. Many users of cloud computing services lack the basic security protections that users of traditional PC-based software often take for granted.

These vulnerabilities are easily preventable. Many Web-based services – including online banking and certain online merchants – operate securely over open wireless networks. As a notable example, many banks in the financial sector use the industry-standard Secure Socket Layer (SSL) encryption protocol to protect their customers' information. These encryption technologies are widely available.

Yet, many service providers choose not to implement these technologies for all data transfers, and instead continue to provide products and services with unsafe default settings. Even though these service providers know about the vulnerabilities, and the ease with which they can be exploited, the firms continue to send private customer information over unsecured Internet connections that easily could have been secured.

My bottom line is simple: security needs to be a default in the cloud. Today, I challenge all of the companies that are not yet using SSL by default. That includes all email providers, social networking sites, and any website that transmits consumer data. Step up and protect consumers. Don't do it just some of the time. Make your websites secure by default.

CONCLUSION

I've been outspoken on privacy and data security issues for six and one-half years now. I have continually pushed companies to be leaders on privacy and data security. I hope my words have resonated with some of you, and that commentators and industry representatives will thoughtfully address my concerns.

Now that I am leaving the Commission, the voices of two new Commissioners will emerge. Edith Ramirez and Julie Brill are both incredibly bright and talented, and I know they will both continue to fight on behalf of consumers, as I have tried to do all these years.

It has been my great privilege and pleasure to serve the American public. Thank you.