Federal Trade Commission

International Association of Privacy Professionals
Practical Privacy Series
Washington, DC

Remarks of David C. Vladeck[1]
Director, FTC Bureau of Consumer Protection
December 7, 2010

Thank you for inviting me to speak today. It is always a pleasure to come to the IAPP – you all grapple with privacy issues day to day, and many of you have made important contributions to the public discussion about online privacy. I am especially gratified by the participation of so many of my colleagues at the FTC. Their presence reflects that there is a lot going on at the agency in the privacy realm.

As you all know, on Wednesday we released our privacy report setting forth preliminary recommendations for a new privacy framework, which was an important step forward in the Commission's work on privacy. Commissioner Brill spoke extensively about these recommendations this morning, though, so while I'll talk a bit about the report – particularly the recommendation for a universal opt-out mechanism – and will leave plenty of time for questions about it, I'll talk mostly about the work we've been doing to enforce privacy laws.

Enforcement Cases and Partnerships – Echometrix

[1] The views expressed here are my own and do not necessarily represent the views of the Federal Trade Commission or any Commissioner.

First, I'd like to discuss a case we announced last week against Echometrix. EchoMetrix sells software — called Sentry — that enables parents to monitor their children's online activities. When EchoMetrix's software is installed on a computer, parents can view the activity taking place on the target computer. EchoMetrix also advertised a web-based market research software program that it claimed would allow marketers to see "unbiased, unfiltered, anonymous" content from social media websites, blogs, forums, chats and message boards. We alleged that one source of this content was the online activity of children recorded by the parental monitoring software.

We charged in our complaint that EchoMetrix failed to adequately disclose to parents that it would share the information it gathered from their children with third-party marketers. EchoMetrix made only a vague disclosure about information sharing and placed it about 30 paragraphs into a multi-page end user license agreement. Again, this goes back to one of the main themes in the privacy report: we've talked a lot in the past year about the importance of transparency, and burying an ambiguous statement in the EULA just doesn't cut it. That's especially true when personal information about children is being collected and shared.

The consent order requires EchoMetrix not to use or share the information it obtained through its Sentry parental monitoring program — or any similar program — for any purpose other than allowing a registered user to access his or her account. The order also requires the company to destroy the information it had transferred from the Sentry program to its marketing database.

I want to acknowledge that petitions from the Electronic Privacy Information Center (EPIC) and the Center for Digital Democracy spotlighted the problems with Sentry.

Enforcement Cases and Partnerships – Data Security

Turning to data security, the FTC has aggressively enforced data security laws. We've now brought 29 data security cases, ranging from cases against retailers, software providers, mortgage companies, data brokers, and others. These cases have involved companies that failed to take reasonable measures to protect against both high tech hackers – most recently, a case against Twitter – as well as low tech dumpster divers. These cases send a strong message that companies have to take reasonable measures to safeguard consumer data: companies are stewards of the consumer information they maintain, and they've got to be responsible stewards.

To leverage our resources to best effect, we are always looking to partner with other enforcement agencies. For example, the Commission just finalized our most recent data security case, against the Rite Aid pharmacy and drug store chain. We coordinated our investigation with the Department of Health and Human Services, which was looking into Rite Aid's handling of health information under HIPAA. We alleged that Rite Aid failed to implement reasonable and appropriate procedures for handling personal information about customers and job applicants, particularly with respect to its disposal practices. Our action followed media reports that Rite Aid pharmacies across the country were throwing pharmacy labels and employment applications into open dumpsters. By cooperating with HHS, we were able to get broad relief: their order covered Rite Aid's pharmacy practices regarding prescription information, and our order required security for the "front part" of the store and for employee information. Although we did not have authority to get civil penalties, HHS was able to get a $1 million fine against the company. We reached a similar agreement the previous year with CVS Caremark relating to similar conduct, again working with HHS to coordinate the scope of relief.

We also cooperate closely with the states. For example, the Lifelock case involved not just an FTC order but concurrent settlements with 36 state attorneys general in one of the largest federal-state cooperation efforts on privacy ever. We charged that LifeLock had falsely promoted its identity theft protection services, which it widely advertised by displaying the CEO's Social Security number on the side of a truck. Lifelock also failed to safeguard its customers' personal information. Irony of ironies, the CEO was himself a victim of identity theft as we were settling the case. The settlement bars deceptive claims, required data security measures, and required LifeLock to pay $1 million to the states and $11 million to the FTC for consumer redress. Last month, we mailed out about $11 million in checks to nearly a million LifeLock customers all across the country.

Enforcement Cases – Privacy

Our data security work is critically important, but I'm equally excited about work we've been doing to make sure that businesses respect consumer choice. We are bringing more challenges to what I see as privacy practices that are not transparent and that attempt to circumvent consumers' choices about how their information will be used.

I've already discussed how *Echometrix* fit that rubric. Another example is our recent action against an online data broker, US Search, that charged consumers $10 to opt out from its database – but didn't always opt them out. US Search sells public record data – information such as names, addresses and phone numbers, marriages and divorces, bankruptcies, neighbors, associates, criminal records, and home values. So you could order up searches like "People Search," "Background Check," "Real Estate Reports," "Criminal Records/Court Records Searches," and a "Reverse Lookup" service that can return the name of an individual associated

with a particular phone number or property address.

US Search promised it could "lock" consumers' records so others could not see or buy them. But as we alleged in the complaint, consumers' information still showed up in many instances even after they'd paid to opt out. For example, if I opted out as David Vladeck, a separate entry with my middle initial could remain in the database. The settlement prohibits misrepresentations about the effectiveness of any service that purports to remove information about consumers from its website, and also requires US Search to give full refunds to nearly 5,000 consumers. Those who think people don't care about privacy might be surprised to hear that nearly 5,000 people found this site and paid for the privilege of opting out.

The message here again is that when consumers choose to take advantage of a company's opt out mechanism, the company must implement that choice effectively. And of course, that's true whether the consumer paid to opt out or not.

XY Letter

Our investigations don't necessarily result in the filing of a litigation complaint or a settlement. This past summer, I sent a letter to individual stakeholders in XY Corporation, which operated a now-defunct magazine and website directed to gay male youth. The letter expressed concern about these individuals' efforts to obtain and use old subscriber lists and other highly sensitive information – including names, street addresses, personal photos, and bank account information – from gay teens. The letter warned that selling, transferring, or using this information would be inconsistent with the privacy promises that were previously made to the subscribers, and may violate the FTC Act; thus, the letter urged that the data be destroyed. After receiving a copy of the FTC letter, the court overseeing bankruptcy proceedings involving the

XY Corporation ordered the destruction of the information.

Google Wifi

At the end of October, we ended our examination of whether Google's collection of unsecured Wifi transmissions was deceptive or unfair in violation of Section 5 of the FTC Act. Google's information collection was the subject of a petition by Consumer Watchdog. There's been a lot of discussion about my letter to Google informing the company that we wouldn't take action – more press than we get about the cases we do bring, actually, and much of it was critical of our decision. There is still much confusion about what happened. Here's what I think you should know about it:

First, Google's conduct involved the un-consented to, invisible, massive collection of data — including data that was personally identifiable. To be sure, we are concerned about the unconsented-to collection of private information.

Second, we examined Google's conduct thoroughly to see whether it violated any law enforced by the Federal Trade Commission. Our central charge is Section 5 of the FTC Act, which gives us authority over deceptive or unfair practices. To find that a company engaged in a deceptive practice, we would need to find a misrepresentation or a breached promise. To meet our test for unfairness, as that term is defined in our statute, the conduct must, among other things, cause or be reasonably expected to cause substantial injury to consumers. Our inquiry did not show a need for an enforcement action.

Third, we took steps to ensure that there would be no recurrence of this episode by

Google. At our urging, Google implemented a number of measures to prevent privacy violations in the future. Many of these measures build privacy into product development and ensure that Google engineers and managers receive core privacy training. These measures are summarized in a letter I sent to Google on Oct. 27, 2010, which is available on the FTC's website.

Fourth, our decision had no effect on the ability of other agencies — international, federal or local — to pursue their own investigations and take whatever action they believe is warranted. And as you know, there are ongoing investigations into Google's conduct.

Non-Enforcement Initiatives

In addition to investigations involving individual companies, we're also engaged in some broader privacy initiatives. First, we're reviewing our Children's Online Privacy Protection Act rule to see whether it provides adequate protection in light of significant changes in the marketplace affecting kids, such as the explosive growth in the use of social networking and smartphones and the development of technologies such as interactive TVs.

Our rule review is about how well this 12-year-old statute has stood the test of time. For example, does COPPA's coverage of websites located on the Internet and online services reach the kinds of electronic media children use today? How should we address the collection of mobile geolocation data or information collected in connection with online behavioral advertising under the Rule? What about online gaming sites – should they be covered? Are the methods for verifying parental consent, such as using a print-and-send form, obsolete?

We are also looking for creative ways to encourage compliance with consumer protection

laws. One initiative relates to an area of interest to the new Consumer Financial Protection Bureau: credit reports. In 2004, we issued a rule requiring the three nationwide consumer reporting agencies – Equifax, Experian, and Trans Union – to provide consumers, upon request, with a free copy of their credit report every year through the annualcreditreport.com website.

Unfortunately, as most of you know, lots of copycat sites were offering supposedly free reports with lots of strings attached, so there was a lot of confusion about how to obtain the truly free, no-strings-attached credit reports available by law. Congress passed a law requiring sites advertising free credit reports to disclose prominently that truly free reports are available at annualcreditreport.com. Our rule implementing the statute went into effect in April.

Some sites still didn't get the message. So in July we sent warning letters to 18 websites offering free credit reports, telling them that they better comply with the new disclosure requirements. And we've followed up since. I'm happy to say that as a result of the warning letters, a number of these websites shut down, and the rest changed their business practices. We continue to monitor the marketplace to look for companies that are not in compliance with the Rule.

CSS History Sniffing

Another initiative related to "history sniffing." Researchers at the University of California San Diego released a paper demonstrating that, at 46 websites, consumers' web history was being "sniffed" without their consent. History sniffing allows websites to surreptitiously collect private information regarding a consumer's web browsing – without installing cookies or using hacking tools and without any action on the consumer's part. This

technique deliberately bypasses the most widely known method consumers use to prevent online tracking: deleting cookies.

Companies can do this by exploiting a feature of consumers' web browsers that displays hyperlinks in different styles, depending on whether the consumer has previously visited the website associated with the link. When a consumer navigates to a website that contains history sniffing code, the code can check whether the consumer has visited a list of dozens or hundreds or even thousands of sites. In theory, history sniffing could be used to get extensive information regarding the domains or even sub-domains the consumer had visited. For example, the UCSD researchers found that, if a consumer visited a certain gaming site, web sniffing code would check whether the computer had visited www.amazon.com and www.ebay.com, among more than 200 other websites, creating an instant consumer profile. What's motivating companies to do this? You guessed it: one use is to serve targeted ads.

Commission staff met with the major browser vendors and urged them to implement fixes to take care of this problem. A couple of browser companies have rolled out fixes already, and we've been told that the others are implementing fixes now, so consumers who upgrade to the latest version of their browsers will no longer experience this vulnerability. We're on the lookout for other tactics companies can use to extract consumer information by technical means.

Roundtables and the Privacy Report

Let me turn now to our Privacy Report. Commissioner Brill spoke about the major themes in the Report, as did Jessica Rich, Deputy Director of the Bureau, who played a leading role in developing the framework set out in the Report, and who is deeply steeped in our privacy

policy-setting. I do want to talk more about the "Do Not Track" recommendation. On Thursday, I testified before a House hearing focused on this issue, and there has been a lot of interest in this proposal and how it might work.

The Report envisions some kind of universal mechanism, a one-stop-shop where consumers can register a preference not to be tracked, or not be targeted for online ads, and where marketers would have to respect such preferences. There have already been efforts — by browser companies and others — to give consumers tools to indicate that they don't want to be tracked, or to adjust or tweak how they're tracked. These efforts are laudable. It is hard to say, though, how consumers will respond if many different associations, companies, and groups offer different options in different formats. A Do Not Track option can simplify consumer choice.

Let me be clear that we're mindful of the benefits that online behavioral advertising has to offer, such as funding content or enabling the delivery of personalized ads that many consumers value. So the motivation here is to empower consumers by effectuating their choices.

Because we happen to enforce the Do Not Call Registry for telephones, there has been some confusion about how Do Not Track would work. Do Not Call is markedly different in some respects. One key difference is that Do Not Call is built around a database of phone numbers that people have registered with the Commission. Do Not Track would be implemented by the consumer either through the browser or some other means, so there would be no need for a database of any kind, anywhere. Do Not Track and Do Not Call do share one fundamental concept though: they're both designed to make it as easy as possible for a consumer to express their preference. As you may recall, even before we implemented Do Not Call, consumers could request that individual companies stop calling, and both industry and the states

offered mechanisms for consumers to express a preference not to be called. The revolution that made Do Not Call such a success was that consumers could register in one place and be done with it.

One final thought. The Report lays out a framework for moving forward, but it also asks many questions about policy and implementation that we need feedback on. So please read our Report. Let us know what you think. The release of the report will be the end of one phase of this project, but it is also the beginning of a second intense phase. Please give us your thoughts. Thanks.