Federal Trade Commission

Consumer Watchdog Conference
"Online Consumer Protection After the Midterm Elections: What's Next?"
Washington, DC

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

Thank you for inviting me here to speak today. I'm eager to talk about the work we've been doing to enforce privacy laws and to think broadly about privacy protection going forward.

As I will explain in a few minutes, today marks an important step forward in the Commission's work on privacy. Later today we will issue a report setting out Staff's preliminary recommendations for a new privacy framework. I will give you a sneak preview of the topics covered by the report at the end of my presentation — largely to keep you captive until the end. We hope that the report will be posted on the FTC's web site (www.ftc.gov) by mid-day, and there will be a telephone press availability for members of the press at 1 pm. Members of the press who want to participate should contact our press office directly.

So . . . now we know that there is an elephant in the room, let me turn to more mundane but important matters.

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.

Let me begin by talking about our enforcement efforts, including a privacy case we announced just yesterday 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. 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 that 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 law enforcers both in the US and, as I will talk about in a few minutes, with our partners overseas. 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 customer's 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. Two weeks ago, 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. I would like to see us bring 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.

One such case is Echometrix, which I've already discussed. Another 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 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.

Our investigations don't necessarily result in the filing of a litigation complaint or a settlement.

Last summer, I sent a letter to individual stakeholders in XY Corporation, which operated a now-defunct magazine and website directed to gay male youth.[2] 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

[2] See Letter from David C. Vladeck to Peter Larson and Martin E. Shmagin (Jul. 1, 2010), available at http://www.ftc.gov/os/closings/100712xy.pdf.

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.

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 informing the company that we wouldn't take action – more press than we get about the cases we do bring, actually. 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. We shared and continue to share Consumer Watchdog's concern 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. We found no deception here. Google made no promise that it breached. Nor did we find unfairness, at least as that term is defined in our statute. To meet our unfairness test, the conduct must, among other things, cause or be reasonably expected to cause significant harm to consumers. In this case, there is no evidence of harm that would satisfy that test.

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 — from pursuing their own investigations and taking 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 statute, 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. Let me talk about a couple of these initiatives.

CSS History Sniffing

Another initiative concerned "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 similar tactics that companies can use to extract consumer information by technical means.

Roundtables and the Privacy Report

Let me turn now to the subject you've all be waiting for: Our reexamination of the FTC's policy approach to privacy. I've talked about how some of our past approaches to protecting consumers' privacy – including the notice and choice and harm-based models – have not been keeping pace with new technologies. And we've also talked about our frustration with the pace of self-regulation. I want to be fair — industry has made some efforts to enhance privacy protections for consumers; there have been some important innovations. But self-regulation has not kept pace with technology, and consumers face a daunting burden in today's marketplace to safeguard their privacy.

Take mobile devices. It simply isn't realistic to expect users to scroll through literally hundreds of screens to read a privacy policy. And in the 21st century marketplace, with the ubiquitous collection, use, and storage of data, it is increasingly difficult to identify or pinpoint the harms associated with misuse of information.

Over the last year we hosted three major roundtables to get public input as part of this privacy reexamination. We also sought and have reviewed many public comments. Based on these efforts, we've been putting together a report that sets forth a framework for privacy that makes sense today.

Our report will be coming out later today. Let me preview some of the big-picture issues, without giving away too many of the details. After all, I want each of you to read the Report.

First, we need to reduce the burden on consumers, and one way to do that is to build privacy into products and services at the outset — that is, privacy by design. There's tremendous value in building privacy and security into companies' procedures, systems, and

technologies by design. That means thinking about ways to practice good data hygiene from the very beginning, such as providing reasonable security for consumer data, limiting collection and retention to the least amount necessary, and implementing reasonable procedures to promote data accuracy. The more companies do to establish good practices by default, on the front end, the less burden on consumers to expend lots of effort to salvage some privacy on the back end.

Another way to reduce the burden on consumers is to greatly simplify consumer choice. We heard a lot at the roundtables about streamlining choices for consumers so that consumers can focus on the choices that really matter to them – uses of their data that they would not expect. The way to make privacy choices meaningful to consumers is to present them in a short, concise manner at the point when the consumer is providing the data, so they're top of mind and easy to access when needed. We're also thinking about whether it would be helpful to have more consistent privacy policies, so consumers can compare competitors' privacy practices at a glance, which may lead to more competition around privacy practices. And strong protections for sensitive information such as health, financial, children's, and geolocation data should be a given.

To simplify choice even further, we are considering the elimination of the disclosure of extraneous information – commonly accepted business practices such as giving your address to a shipper – then it will be easier for consumers to pay attention to what really matters and will ease the burdens on business as well.

It should go without saying that consumer choices, once exercised, must be respected. Yet, we've seen less reputable marketers abuse technologies in a variety of ways to circumvent consumers' clearly expressed preferences for privacy. We will not tolerate a technological arms race aimed at subverting privacy-enhancing technologies that consumers have chosen to enable.

We also need to increase transparency. The Report discusses ways to increase transparency about commercial data practices. Despite the many issues raised with existing privacy policies, getting rid of privacy policies is not the answer – privacy notices help promote accountability for companies, for one thing. What we need is better privacy notices, perhaps in more consistent, shorter, more easily comparable formats.

We're also looking at ways to address concerns raised at the roundtables about the roles of data brokers, most of which have no direct interaction with consumers but collect and compile storehouses of data about consumers from myriad sources. Some panelists at the roundtables suggested that consumers should get access to their data as a means of improving transparency, while others discussed the costs of providing access and recommended that any access should vary with the sensitivity of the data and its intended use. Access is an important ingredient in accountability. The Report addresses this issue as well.

We are also continuing to focus on consumer and business education. We already provide a fantastic amount of privacy-related information for consumers on our Onguard Online website, including, for example, recent guidance on the danger of P2P file-sharing software. We also provide a wealth of privacy and data security guidance to businesses, now housed in the new FTC Business Center site. But we are constantly looking for new ways that businesses, consumer groups, and government can use educational materials to broaden and deepen consumers' understanding of information collection and sharing practices, steps they can take to preserve privacy, and privacy trade-offs.

The Report also addresses the viability of 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 to allow — by browers and companies — 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 against can simplify consumer choice.

Tomorrow I will testify before a House hearing on Do Not Track and provide more details about the Commission's position on this issue. I trust you'll understand that I cannot today preempt my testimony tomorrow.

I do want to ask for one thing today: 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. As you'll see, the Report lays out a framework for moving forward, but it also asks many questions about policy and implementation that we need feedback on. Please give us your thoughts.

Thanks.