Federal Trade Commission

International Association of Privacy Professionals Privacy Academy
Baltimore, Maryland

A New Vision for Consumer Privacy?
David C. Vladeck[1]
Director, FTC Bureau of Consumer Protection
September 29, 2010

Thank you. It is a pleasure to be here this morning to share the latest developments on privacy at the FTC, especially before an audience of privacy professionals, who care deeply about these issues. As you'll see in your program, the title of my talk is called "a new vision for consumer privacy." The term "vision" necessarily implies predicting what will occur down the road. As an FTC official, I can't be party to false advertising, so I suppose I have to deliver on the promise of talking about my vision of privacy protection in the future. But as Shakespeare famously said, "past is prologue." We cannot look to the future without learning from the past. So as I speak on privacy enforcement, policymaking, and legislation, I'll try to tackle each of these subjects by discussing where we've been and how it has informed where we intend to go.

I. Enforcement

First, enforcement. As you know, the FTC has distinguished itself by aggressively enforcing privacy and data security laws. So far, we've brought 29 data security cases, ranging

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

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 as well as low tech dumpster divers.

Where possible, we join forces with other federal and state authorities in our data security enforcement program. For example, in the Rite Aid case, we coordinated our investigation with HHS. We alleged that the company 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 — including patient names — and employment applications into open dumpsters. HHS's investigation involved Rite Aid's handling of health information under HIPAA. Our investigation focused on Rite Aid's violations of the FTC Act by failing to safeguard sensitive information. By working with HHS, we were able to get broad relief that neither agency could obtain on its own: HHS's order covered Rite Aid's pharmacy practices regarding prescription information, and the FTC order required security for the "front part" of the store and for employee information. Although the FTC does not have authority to get civil penalties in this kind of data breach case, HHS was able to obtain a $1 million fine against the company.

We also work closely with the states. For example, we announced the Lifelock case earlier this year, in which we filed concurrent settlements with 36 state attorneys general. This is one of the largest federal-state cooperation efforts on privacy ever.

Looking to the future, we will continue to bring cases to ensure that companies reasonably safeguard consumer information. We will also continue to look for opportunities to

cooperate with other state and federal agencies, as we have done in the past. But let me mention three newer areas of focus for the FTC in the enforcement area.

First, rather than bringing only data security cases, I would like to see us bring more cases involving pure privacy — that is, practices that attempt to circumvent consumer understanding and consumer choice about how their information will be used. I've talked to this group previously about the Sears case that we brought last year, in which the company tracked users' web-browsing activities without their informed consent. You can expect more cases like this in the coming months.

Indeed, just last week, we announced an action against a data broker, US Search, that charged consumers $10 to opt out from its database — but didn't always opt them out. US Search promised it could "lock" consumers' records so others could not see or buy them. We alleged that, contrary to the company's claims, the service did not block consumers' names from showing up in many instances — for example, if the database contained entries for both "John Smith" and "John T. Smith," one of the entries could remain, even though it was the same John Smith. The settlement requires US Search to give full refunds to nearly 5,000 consumers and prohibits misrepresentations about the effectiveness of any service that purports to remove information about consumers from its website. 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 equally true without regard to whether the consumer has paid to opt out or not.

Second, we will be focusing our enforcement efforts on new technologies. A few months ago, we announced our first data security order involving a social networking company – Twitter. The Commission alleged, among other things, that the company failed to require strong

administrative passwords and to suspend passwords after a reasonable number of log-in attempts. The complaint further alleged that this failure resulted in a hacker being able to use a simple automated password-guessing tool to gain administrative control of Twitter, through which the hacker could view all Twitter accounts. Some people reflexively think that anything done on a social networking site is meant to be broadcast to the world, but consumers who use social networking sites may choose to share information with people they select — and not everyone. Users have a right to expect that their private tweets will be kept private and secure.

To assist our attorneys in bringing these types of technology cases, we have been using some new tools. We've hired new technologists to work with them on a day to day basis, and have found their expertise to be invaluable. We also have created and staffed a mobile lab to make sure that we are fully equipped to respond to the startling growth of smartphones and the burgeoning marketplace for mobile apps.

The third new enforcement trend is increased international cooperation on privacy. Just last week, we announced the new Global Privacy Enforcement Network. We're excited about this initiative, which we hope will foster increasing collaboration on privacy enforcement with our foreign counterparts. Thirteen agencies from twelve nations are taking part. These types of initiatives enable us to establish working relationships that can really bear fruit – for example, international cooperation with our sister agencies overseas allowed us to take down what some described as the largest spam operation in the world, which included participants in Australia, New Zealand, China, India, Russia, Canada, in addition to the United States. Information flows are increasingly global, so government must respond.

II. Roundtables

Let me turn now to our reexamination of the FTC's policy approach to privacy. This effort is premised on the notion that we must learn from the lessons of the past and build on them to create a vision for the future. When I last spoke at this conference in December, I described how some of our past approaches to protecting consumers' privacy were not keeping pace with new technologies. At one point, we advocated an approach based upon giving consumers notice about information-handling practices, and providing them choices over such practices. This was the so-called notice and choice approach. As implemented, this approach has resulted in long privacy policies that simply ignore the realities of busy, harried consumers in modern-day life. These policies have also become so opaque that even veteran lawyers have trouble deciphering them. The problem is exacerbated by mobile devices. It is hard enough to read a privacy policy on a computer screen. On a phone, one may need to scroll through literally hundreds of screens to read a privacy policy. Another approach we have advocated for in the past is one that focused on targeting the tangible harms that resulted from the misuse of consumers' information. In the 21st century marketplace, however, with the ubiquitous collection, use, and storage of data, it becomes increasingly difficult to identify or pinpoint the harms associated with misuse of information.

So our roundtable project aims to build a privacy vision for the future. I have spoken before about some of the key lessons learned from the roundtables:

- information is now cheaper to save than to destroy, meaning data hangs around for a long time — and may later be given a new purpose that may or may not be consistent with consumer expectations;

- the distinction between PII and non-PII is blurring; it is increasingly difficult to be truly anonymous as more and more information is collected, and as economic incentives drive the collection of increasingly "granular" information;

- consumers understand very little about how their information is handled and with whom it is shared, in part because they are often presented with unfamiliar new business models where the trade-offs in terms of privacy are not clear;

- consumers are also confused because many businesses who have access to their information don't interact directly with them. In addition, for consumer-facing companies, we heard plenty about the shortcomings of privacy policies that are too complicated, too vague, and too long;

- last but by no means least, we also heard loud and clear that the flow of information brings tremendous benefits to consumers; that consumers like the highly personalized on-line environment that modern technology can create; and that technology does not just pose privacy concerns but also will be employed to address them.

So for some time now — beginning the day after the last roundtable, in fact — I've been peppered with two questions over and over: when's your report going to come out? And what's it going to say?

The first question is easy: we're still on target to release the report this fall. The second question, for those familiar with Commission practice, is an impossible one for me to answer, because we have a very vigorous group of Commissioners well-versed in privacy issues who will be reviewing the staff's draft report very closely. The Commissioners are not shrinking violets. They have their own views, and undoubtedly each one will wrestle with the ideas that we present in his or her own way. But let me preview some of the big-picture issues that we'll likely be examining in the report.

First, 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 that necessary, and implementing

reasonable procedures to promote data accuracy. The more companies can do to establish good practices by default on the front end, the less burden there is on consumers to have to expend lots of effort to salvage some privacy on the back end. Fortunately, many businesses already are doing this.

Second, increased transparency. We're looking at 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, that might foster competition on privacy.

Third, simple 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 — instead of commonly accepted business practices, such as giving your address to a shipper so it can be delivered to you. Eliminating this kind of extraneous information will help consumers pay attention to what really matters and ease the burdens on business too.

The other way to make privacy choices more meaningful is to present them 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 policies, so consumers can compare competitors' privacy practices at a glance, which, as I said, may lead to more competition around privacy practices. And strong protections for sensitive information such as health, financial, children's, and location data should be a given.

It should go without saying that consumer choices, once exercised, have to 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.

Fourth, the thorny question of access. 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 many sources. My own view is that what drives the privacy debate is not the delivering of targeted ads — unless those ads address matters of sensitivity — but is instead public wariness of companies collecting and aggregating data that may be used for purposes beyond consumer expectations and in ways consumers fear may be contrary to their interest. 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. There are no easy solutions here, so as we ponder the policy issues we'll be carefully considering the costs and benefits of various alternatives to promote transparency in the data broker industry.

Finally, consumer and business education. The Commission is looking at ways that businesses, consumer groups, and government can employ business and consumer education to broaden and deepen consumers' understanding of information collection and sharing practices, steps they can take to preserve privacy, and privacy trade-offs.

Some of you may be wondering, what about "Do Not Track" or something like it? We are examining the viability of some kind of universal mechanism, a one-stop-shop where consumers can register a preference not to be targeted that marketers would have to respect. Certainly, a number of good corporate citizens have implemented measures that allow consumers to declare that they don't want to be tracked, or to adjust or tweak how they're

tracked, on these companies' websites. These efforts are laudable. It is hard to say, though, how consumers will respond if diverse associations, companies, and groups offer different options in different formats. We'll continue to explore the most appropriate means for allowing consumers who prefer that data about them not be collected for marketing purposes to exercise that preference.

I want to make one last point about the report. Many people I've talked to seem to be looking at this upcoming report as the last step of a process, the final word from the Commission, at least, on privacy in the U.S. and where to go from here. While the report may be the end of one phase of this policy re-examination, we don't see this report as the end of something as much as a beginning. We expect to engage with the public as we explore the ideas and issues addressed in the report over the coming months.

III. Legislation and Self-Regulation

Ever since the Commission has been examining privacy issues, there has been an ever-raging debate about legislation vs. self regulation. The Commission has always supported self-regulation, and will continue to do so. We recognize that self-regulation is a vital piece of the privacy puzzle. At times and in various contexts, the Commission has also promoted regulation to protect consumers' privacy, such as when it enacted the Do Not Call provisions of the Telemarketing Sales Rule.

Let me say that in the context of privacy and in particular behavioral advertising, although the Commission has supported self-regulation, I am disappointed in its progress. I am not alone in this assessment. We know that industry has taken our call to action seriously. And we have heard some great ideas about guidelines for behavioral advertising, in ad disclosures and icons, better consumer choices, and an enforcement mechanism. But implementation of

these measures is still very much a work in progress. I urge industry to get moving quickly on these measures. Consumers — and the FTC — may lose their patience.

Turning to the future, the prospects for privacy legislation are more up in the air. I'm sure many of you are actively following the increasing activity relating to privacy and data security on Capitol Hill. As you know, two privacy bills have been put forward in Congress, one by Chairman Boucher and one by Chairman Rush.

The Commission has not taken a position on either bill. For myself, though, I'm concerned that the bills may place too much emphasis on putting a lot of information in privacy policies. As I said earlier, one clear message from the roundtables is that people don't read privacy policies because they're too long, they're not easy to understand, and they're not available at the point when you need them. The bills also create safe harbors for companies that are participating in self-regulatory initiatives. In my view, while we're following these initiatives with interest, it is premature right now to conclude that existing private initiatives are sufficiently robust to serve as safe harbors.

On data security, in December the House approved legislation sponsored by Chairman Rush that would require companies to take reasonable security measures to protect consumer information. The legislation would also require companies to give consumers notice of breaches creating a reasonable risk of harm. The Senate is now considering a companion bill sponsored by Chairman Pryor. These broad-based protections at the federal level are sorely needed, and the Commission announced its support for the bill's goals in testimony last week. One important aspect of the bills is that the Commission would for the first time have the right to obtain a civil penalty when a company fails to take reasonable measures to secure consumer data. We are still seeing companies leave themselves open to vulnerabilities that are well known and easily and

cheaply resolved; the ability to obtain a civil penalty would be invaluable in deterring future violations. The breach notification requirement is also critical: requiring companies to inform consumers of a breach not only alerts consumers so they can take steps to protect themselves, it gives companies an additional, reputational reason to secure their information properly. The bills would ensure for the first time that consumers will receive notice of a breach no matter which state they live in.

Conclusion

So, having learned from, and building on our work from the past, let me give you my vision for consumer privacy in 2011 and beyond. In my particular privacy utopia, companies are incorporating privacy protections as they design and develop an array of new products and services to make consumers' lives better. Consumers have access to information about privacy generally so they can make quick, at-a-glance, informed choices about how they share their information. The FTC continues its robust enforcement to promote reasonable data security, and to ensure consumers' privacy choices are being respected — with the help of industry self-regulation and the work of consumer watchdog groups. Of course, a real utopia would be a world in which FTC enforcement isn't necessary because companies are doing right by consumers rather than launching products without considering privacy, engaging in trial-and-error with the release of consumers' information, or failing to take reasonable measures to protect that information. But as long as there's a few bad apples, the FTC will continue to remain on the beat.

Thank you for your attention today and for your leadership on privacy issues. When our roundtable report comes out, I invite you to participate in a dialogue with us as we gauge the best way to protect consumer privacy. Thanks.