



Federal Trade Commission

**International Association of Privacy Professionals Privacy Academy
Baltimore, Maryland**

A New Vision for Consum

¹The 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

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 — that is, p8h TD0T1.0 wobeaa.

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 shortcoming

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

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 Commi00000 0.25200 0.(r d4u)TjET000b00 hep ofr d4u

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

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