

Subj: Online Privacy: Perspectives of Privacy Right
From: Paul Sholtz, Chief Technology Officer, PrivacyRight Inc., c/o Amy Hanson, 703-299-9470
To: Internet Caucus Advisory Committee

Elements of Privacy Policies

The privacy policies posted on most Web sites do a decent job of disclosing to consumers what information is collected, how it is used and with whom it is shared. Unfortunately, these privacy policies are little more than an informal contract, and consumers have no way of verifying or enforcing that Web sites are limiting their data practices to what they outline in their privacy policies. Consumers have no way of controlling or changing how much personal information the Web site knows about them. Also, if the Web site resells personal information, the consumer to whom it belongs does not realize any economic benefit.

What is adequate notice? Adequate notice" usually means that the Web operator has gone to some reasonable length to disclose to consumers what personal information is being collected and how it is being used. Usually, posting a privacy policy in a prominent place on the Web site constitutes adequate notice.

Adequate notice is probably one reason for the backlash against companies like DoubleClick, which track and profile users without the individual's knowledge and consent. This is because online advertising networks attach cookies to banner ads across a network of affiliate Web sites, which are otherwise unrelated to DoubleClick. Since the Web operator and DoubleClick have different domains, even if the consumer is informed about the Web operator's privacy policy, the person is most likely unaware of the profiling DoubleClick is simultaneously doing.

As Browser Displays Get Smaller Cell phones and PDAs have their own host of privacy problems. Since the devices are wireless, the service providers must be able to track the location of the device with a fairly high degree of accuracy (in order to send data back and forth to the device). A law, which was enacted last year, requires cell phone operators to be able to locate a cell phone call within 100 feet when a 911 call is placed. It gives service operators the ability to do novel "real-time location-based" marketing to wireless subscribers (a notion that raises very significant privacy concerns).

Notice for Aggregate Data. Aggregate data is different than individually identifying data, and in general less sensitive. However, in terms of customer control, disclosure should be provided for all collected data, even for internal use of aggregate data.

Subj: Online Privacy: Perspectives of Mr. Stewart A. Baker, Partner, Steptoe & Johnson LLP, Member of FTC Advisory Committee on Access & Security
From: Mr. Stewart A. Baker, Partner, Steptoe & Johnson LLP, 202.429.6413, sbaker@steptoe.com
To: Internet Caucus Advisory Committee

Concurring Statement of Stewart Baker, Steptoe & Johnson LLP, Regarding the Report of the FTC Advisory Committee on Access and Security

The Advisory Committee on Access and Security was established to report on two issues relating to privacy and commercial Websites. First, we were asked when and how Websites should provide a customer with **access** to information that the Website has gathered about the customer. On the access question, the Committee reaches no conclusion, presenting instead a range of options. Second, the Committee was asked how Websites should provide **security** for customer information. On this point, we reached consensus, recommending that Websites adopt a security program, that the security program have specified elements, and that the security program be appropriate to the circumstances (e.g., stronger security for more sensitive data).

I fully concur in this report. Indeed, I am proud to be part of the process that produced it. The Committee included practically every stripe of opinion, yet its debates were always respectful and, against the odds, they produced at least partial consensus. That said, I write separately to point out the strict limits of our consensus on security, the serious nature of the issues that prevented us from reaching a similar consensus on the access question, and the lessons that should **not** be drawn from this report.

First, security. Our recommendation on this point is made in the context of voluntary action by commercial Websites. In other words, these are things that responsible Websites should consider implementing as a matter of good business practice. There was no agreement on government-mandated security standards, and in particular no agreement that the FTC should be more heavily involved in setting standards in these areas.

Why not? Well, first because the FTC, like this Committee, lacks jurisdiction. The FTC may have authority over commercial Websites. But as the report also notes, the risks to personal information are not restricted to commercial Websites. In fact, the risk of a data compromise may be worse on, say, political Websites that gather both credit cards and sensitive political data about individuals. What's more, every business in America gathers some customer information, including a large volume of credit card numbers. The security of personal data is not a problem limited to Web sites. If the issue requires regulation, we should impose security programs on every bookstore and restaurant and dry cleaner in the country that handles credit cards and other personal data. We certainly should not make "Regulate the Net First" our slogan.

Even if we decided to focus only on Internet security, the FTC is not the place to address the issue. Exposure of personal data from Web sites is not the Internet's biggest security problem – not by a mile. The Committee did not hear any evidence that consumers had actually suffered significant losses from exposure of their personal data on the Internet (it appears that losses from the well-publicized hacker thefts of credit card information fell mainly or exclusively on merchants and banks). Yet at the very time the Committee was meeting, Web businesses were cut off from customers by denial-of-service attacks, and the Committee's own deliberations were disrupted by a global computer worm. If a handful of script kiddies and a second-rate computer programmer can do that much damage, hostile nations employing talented computer scientists can do far worse. In the long run, these security issues will be more important to Americans than protecting their shoe sizes or even their credit card numbers from voyeurs.

So, before rushing forward with legislation or regulation to solve what may be the least significant of the Internet's security problems, we need to look at Internet security from a much broader perspective. This, of course, is an inquiry far beyond either the FTC's experience or its expertise.

Next, the access question. It sounds like a good idea for consumers to be able to see the data that Web sites have assembled about them. In fact, it is a good idea, but one with clear limits. We heard estimates from Web companies that less than one percent of customers who are offered access actually take advantage of the offer. (Just ask yourself whether you've exercised your access rights recently. If you're like me, your answer is, "Hey, life's already too short.") But maintaining a system to satisfy the most curious one percent of American consumers could be quite costly, and the costs would be borne almost entirely by the other 99%..

And financial costs are the least of the problem. Far worse is that, as the Report says, "Giving access to the wrong person could turn a privacy policy into an anti-privacy policy." If access to personal data is turned into a legislative right, Americans' personal data will be at risk of exposure to con men, private investigators, suspicious spouses – anyone who has the *chutzpah* and the scraps of information needed to plausibly impersonate their target.

That's bad for all of us, but it is especially bad for the companies forced to set up some sort of access system. If they demand clear and convincing proof of identity before releasing personal data, they will be accused of offering access in theory while denying it in practice. But if they relax the rules, they will surely be sued every time a con man exploits the relaxed rules to steal a consumer's identity.

This "damned if you do, damned if you don't" liability problem makes it particularly clear that the FTC has no business imposing an access requirement on its own, not even in the context of consent decrees and other quasiregulatory programs. Why? Because if society chooses to require access – and to accept the risk of improper disclosure that goes with it – then surely the businesses that are required to provide access should be protected against liability if the access results in improper disclosures. Unless the FTC can protect companies against the liability risks that go with consumer access, it should not demand that they throw themselves into harm's way.

Finally, a word in closing about the use that will be made of this report. Although the FTC completed a "sweep" of Internet sites and privacy policies during the Committee's deliberations, it refused to share that data with the members of the Committee. Too confidential, we were told. But on the day our report was put to bed, details of the "sweep" were leaked to the press and Congress.

That was unfortunate, but what was worse was the way the sweeps study – which we still have not seen -- apparently ignores the lessons of this Committee's report. If the leaks are to be believed, the FTC's sweeps study acknowledges that many more Web sites have privacy policies than even a year ago, but it criticizes the policies for not including access and security elements.

The lesson of this Committee's report, however, is that neither of these elements needs to be part of every Web site's privacy policy. Of security notices, we said: "Since it is difficult to convey any useful information in a short statement dealing with a subject as complex as the nuts and bolts of security, most such notices would be confusing and convey little to the average consumer. Further, providing too many technical details about security in a security notice could serve as an invitation to hackers."

On access, of course, there was no agreement. Many of the Committee members thought that there would be few times when providing access to Web site data was really necessary. Access is

worth the cost mainly when it allows consumers to correct information that could hurt them if left uncorrected – credit reports, school transcripts, and the like. But most Web sites don't collect information or use for those purposes. More commonly, the data is maintained for the purpose of knowing more about their customers' likes and dislikes, or for advertising demographics and tailoring, and the like. The data may also be mixed with proprietary and third-party information that should be protected. If any of that is true for a particular Web site, then that site has no need to provide access to personal data -- and by the same token no need to add an "access" section to its privacy notice. In short, the Web sites that do not provide access to personal data quite likely base their policy on views that are featured prominently in the report of the FTC's own advisory committee. These are not consensus views, but they are part of the mainstream. To criticize such Web sites for lacking an access policy – or to suggest that the FTC needs to step in and solve some kind of "access crisis" on the Web -- is to ignore the lessons of this Report.