COMMENTS OF CONSUMER WATCHDOG

To

THE FEDERAL TRADE COMMISSION

Regarding

A Preliminary FTC Staff Report on "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers"

February 18, 2011

750 Ocean Park Boulevard, #200
Santa Monica, CA 90405-4938
310-392-0522 • Fax: 310-392-8874

EXPOSE. CONFRONT. CHANGE.

www.ConsumerWatchdog.org

413 E. Capitol St., SE, First Floor
Washington, D.C. 20003
Tel: 202-629-3064 • Fax: 202-629-3066

COMMENTS OF CONSUMER WATCHDOG

To

THE FEDERAL TRADE COMMISSION

Regarding

A Preliminary FTC Staff Report on "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers"

February 18, 2011

Introduction

The Federal Trade Commission's report *"Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*," offers an important review of many of the threats to privacy in the online environment. It clearly and correctly makes the point that the self-regulatory model has proved inadequate. Consumer Watchdog believes the Report should ultimately lead to the implementation of necessary laws and regulations based on Fair Information Practices (FIPs) that would offer consumers control of their information, how it is used and if it is used at all. Before focusing on one of the potentially most powerful tools to protect consumers online – A Do Not Track Me mechanism – here are some general comments about the Report.

General Comments

We endorse the framework for protecting consumer privacy as it is outlined by the Report. In scope, the framework must apply to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device such as a mobile phone. We endorse the

principles of privacy by design, simplified choice and greater transparency by companies about their data practices.

One of the problems with the current "notice and choice" model of privacy protection is that businesses' privacy policies have become incomprehensible. They are written in dense legalese that appears to have been crafted by lawyers who were paid by the word to obfuscate a company's practices. Privacy polices should be simplified so they are comprehensible and a company's practices transparent. There should be regulations or guidelines detailing what must be covered in a policy. Something as simple as the nutrition labels on food could be the model for the sort of clear disclosure that is needed. Ideally clear, concise and comprehensible privacy polices would give consumers more options and could prompt real competition to offer the best privacy protections, in some cases going well beyond the minimum required by law and regulations.

The Report's suggestion that consumer choice would not be necessary for a limited set of "commonly accepted" data practices makes sense. The devil will be in the detail of defining those practices. While Consumer Watchdog agrees that product and service fulfillment, internal operations such as improving services, fraud prevention and legal compliance should be included in the definition; first-party marketing should not automatically be included.

Some businesses and trade associations claim that strong privacy protections will hinder business innovation. This is simply not the case. Privacy enhancing technologies have enabled the commercial use of the Internet. For example, were it not for SSL encryption using the HTTPS protocol, it would be impossible to take payments, or to transfer credit card numbers online. The fact of the matter is that commerce is enhanced when consumers have confidence in the entity with which they are doing business. Knowing that their privacy is protected will build such trust and will prove to be a win-win for

consumers and businesses alike. What sort of long-lasting business model can be built on surreptitiously spying on customers?

In a related matter Consumer Watchdog has also offered comments on the Department of Commerce's report, *"Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework."* In that report Commerce calls for the creation of a Privacy Policy Office in the Department of Commerce. Its primary function, as described, would be convening "multi-stakeholder discussions" about privacy best practices. The Department of Commerce is, by definition, focused on business interests, not consumer protection. We believe a comprehensive federal privacy law should provide for the creation of an independent Privacy Protection Office. However such an office, and multi-stakeholder discussions run out of the Commerce Department, will almost inevitably be industry-dominated forums more likely to hinder strong privacy rules than promote them. The Commerce Department – as it should – primarily seeks to promote the interests of business. It is not, nor should it be expected to be, the primary protector of consumers' interests. Commerce, therefore, must not have the lead role in online privacy protection. That is a task best left to a new independent Privacy Protection Office and the Federal Trade Commission.

With other privacy groups such as EPIC, Consumer Watchdog supports the Council of Europe Convention 108. We urge that the United States begin the process of ratification of Council of Europe Convention 108. We fear that in a drive for harmonization of global privacy practices, there will be an effort to circumvent the relatively strong protections in Europe and weaken consumer protection in the United States. Consumer Watchdog calls on the FTC to continue to lead on consumer privacy protection both in the United States and internationally.

Do Not Track Me

As the Report makes clear, data collection is ubiquitous online. The *Wall Street Journal* has done a groundbreaking investigative series over the last few months. It calls spying on users "one of the fastest-growing business on the internet." The nation's 50 top Websites install an average of 64 pieces of tracking technology on users' browsers – all without your knowledge. This tracks all of your activity online, adds it to your profile, and then puts it up for instant sale in a stock market-like auction.

Consumers should have the right to choose if private information – from shoe size, to health concerns, to religious beliefs – is collected, analyzed and used to profile them by companies tracking activities online. Do Not Track is the simple way for consumers to say 'no thanks' to being monitored while they surf the Web.

Right now much of the online advertising market is based on unauthorized spying on consumers. A Do Not Track mechanism would give consumers better control of their information and help restore their confidence in the Internet. That's a win-win for consumers and business. What kind of lasting business can be built on snooping on your customers?

Marketers argue that consumers can already protect themselves. But existing "privacy" options:

- **Don't actually work**: Opt-out often means you don't get targeted ads, but your information is still tracked.
- **Are too confusing**: Consumers don't have the expertise to choose what companies to block, or where to go to block them.
- **Require too many choices**: Ad companies, Web browsers, search companies, and Websites all have different privacy tools and consumers must act to protect themselves with each.

- **Don't make clear who to trust**: There is no way for consumers to know if a privacy tool is a legitimate site, or if it is trying to trick them into giving up even more info (or worse yet, money!)

Consumers don't understand the scope and implications of tracking – so can't make informed decisions. Even if they were well informed, they don't have the tools to make their desires known. Technology-based solutions to the privacy problem simply lead to a never-ending technological arms race. For example, when methods were developed to block tracking "cookies," trackers got around that by using flash cookies. The solution is a tool that enables a consumer to send an unambiguous message to all Websites of the desire not to have data gathered and used. When a site received such a message it would be required to honor it. A poll by Consumer Watchdog last summer found that 80% of Americans support a Do Not Track option. Download the poll results here: http://insidegoogle.com/2010/07/consumer-watchdog-poll-finds-concern-about-googles-wi-spy-snooping/

Here are Consumer Watchdog's principles for a Do Not Track mechanism:

1) Ease of use/ Simplicity: Consumers need one location to express their preferences. Most consumers could not name one data broker online, let alone identify the many different companies whose tracking they'd have to opt out of.

2) Enforceable: Privacy rules without an enforcement mechanism are useless. There must be a legal obligation by companies to comply, FTC needs authority to act, and consumers should have a right to hold a company responsible in court if their privacy is violated.

3) Penalty Free: There should be no penalties – either monetary (fees) or content-wise (making the content unavailable to users who opt out) for opting out of spying.

4) Device neutral: Must apply whether consumers access the Internet via computer, smartphone or some other device.

The concept of Do Not Track is analogous to the successful Do Not Call List maintained by the Commission. There would, however, be no actual registry. Instead, the consumers' browser would send a clear message of the consumers' desire not to be tracked to all Websites. Exactly what technology would be used should be left to the browser manufacturer, although so far Consumer Watchdog favors the header system that will be adopted by Mozilla's Firefox.

Under this system there would need to be a regulations mandating the legal responsibilities of Websites that receive a Do Not Track message. Under this system the definition of "tracking" is critical. Consumer Watchdog believes this is the appropriate definition:

Tracking is the collection of data about Internet activities of a particular user, computer, or device (including mobile phones), over time and across a Website or Websites, for any purpose other than site maintenance and improvement, fraud prevention or legal compliance.

In other words, tracking includes all collection of data by Websites and applications whether they are first or third party. The line between the two is increasingly blurred. While there may be some allowable first-party uses, they must be defined as exemptions through a rulemaking process. Simply put, tracking is tracking and consumers must have the right to opt out of it. We presume many, if not most, consumers will agree to tracking by a company with which they have a relationship, but they must have the choice.

FTC staff asks in the Report, "If the private sector does not implement an effective uniform choice [Do Not Track] mechanism voluntarily, should the FTC recommend legislation requiring such a mechanism?" In fact, as the Report notes, self-regulation has not worked. It will not work. Legislation has already been introduced by Rep. Jackie Speier, D-CA, that authorizes the Commission to enact and enforce regulations that would create a Do Not Track mechanism. Instead of waiting for industry yet again to demonstrate the insufficiency of self-regulation, the Commission should recommend Congress approve legislation requiring a Do Not Track mechanism, and endorse HR 654, the "Do Not Track Me Online Act."

Opponents claim that Do Not Track or other privacy protections – if placed into law rather than developed by industry at their own pace, and completely voluntary – will put an end to the Internet as we know it.

In fact, some of the traditional publishing Websites – like *The Washington Post* – would benefit from a move away from tracking-based advertising. The ability of companies to follow consumers around the Internet and advertise to them anywhere based on all of their other activities reduces the value of advertising with traditional sources like the news media.

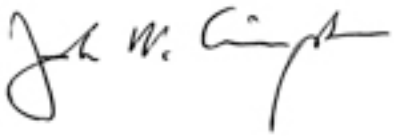
As a *New York Times* editorial noted: "Even if regulation limits advertisers' ability to precisely target their ads according to consumers' tastes, they will still need to advertise. They will just do it differently. Advertising spending in the United States amounted to 1.8 percent of G.D.P. last year. In 1990, before Yahoo even existed, it amounted to 2.2 percent of G.D.P. It has remained within that range over nearly two decades."

The sky-is-falling argument is the same thing the telemarketers said before the Do Not Call list was implemented – and their industry didn't collapse. The premise is that strong privacy laws will stifle the innovation of companies on the Internet. However, it's just that spirit that will keep companies innovating, whether or not data miners are allowed to continue to spy on consumers' every move online. Content will continue to be supported by advertising, even if that advertising can't be micro-targeted to consumers based on their purchases, searches, and Websites they've visited for the past year.

Conclusion

The Commission's Report is a thoughtful analysis of the challenges faced in protecting consumers' privacy in a rapidly changing and developing technological environment. It proposes a solid framework with principles drawn from Fair Information Practices (FIPs) that will go far to ensure that consumers are protected. That framework must be enacted by regulation through a rulemaking process. One substantial tool that will empower consumers and allow the Internet to thrive while protecting consumers' basic right to privacy when they travel in cyberspace is a Do Not Track Mechanism. Such a mechanism also must have the force of law behind it. The Commission should support HR 654, the "Do Not Track Me On Line Act," introduced by Rep. Jackie Speier.

Respectfully submitted,



John M. Simpson

Consumer advocate
Consumer Watchdog
1750 Ocean Park Blvd.
Santa Monica, CA
90405