ThreatMetrix™

February 9, 2011

Via Federal Express/Electronic Mail

Federal Trade Commission
Office of the Secretary
Room H-113 (Annex)
600 Pennsylvania Avenue, NW
Washington D.C. 20580

Re: FTC Staff Preliminary Report on Protecting Consumer Privacy (the "Preliminary Report") – File No. P095416

Dear Sir or Madam:

Thank you for the opportunity to comment on the Preliminary Report. These comments are referenced to the particular headings set forth in Appendix A of the Preliminary Report. ThreatMetrix, Inc. is a technology company providing cyber security and fraud detection services to electronic commerce sites.

The Preliminary Report states that many of its recommendations are made in response to the privacy implications arising out of behavioral advertising. Privacy concerns may not be as great when the collected data is used to provide consumers a more secure environment in which to conduct electronic commerce. The recognition of the unique role of data collection for fraud prevention was recognized by the FTC staff. Because there may be tradeoffs between privacy and security, ThreatMetrix is providing these comments to acquaint the FTC staff with the impact of the Framework on online fraud detection and to propose certain modifications to the framework outlined in the Preliminary Report (the "Framework") which will increase consumer security in electronic commerce.

Cyber security is a continuing "arms race". As new technologies and defenses are created, fraudsters develop ever more sophisticated weapons to steal goods, services, and identities otherwise distributed and transmitted online. The more a fraudster knows about cyber security tools, the more likely the fraudster will evade discovery and thereby perpetuate its online activities.

Cyber security typically functions by reviewing the actions of a device, rather than a particular individual. Fraud can be detected by using, among other techniques, factual data and behavioral data associated with the device. Factual data reviews anomalies associated

with the particular device effectuating a transaction, while behavioral data compares the behavior of a device to its typical behavior or the behavior of a control group. Cyber security technologies gather individual device data directly from the device, such as when it is used to place an order, and can enrich the individual device by gathering data flowing through the internet which is otherwise derived from the particular device.

Scope

The Framework expands Fair Information Practice Principles to any entity which collects data that can be reasonably linked to a specific device, rather than just a specific individual. Because many cyber security technologies collect data linked to a specific device, the application of the privacy principles to devices directly impact cyber security firms.

The Framework emphasizes choice as an important right for consumers in connection with data collection and use. ThreatMetrix applauds the FTC's view that data collection and use for fraud detection purposes is a commonly accepted practice and should not be subject to consumer choice. The Framework, however, should go farther.

The importance of cyber security, and the nature of the data collected, requires that it be treated differently than the treatment accorded consumer data collected for behavioral advertising purposes. First, aside from personally identifying electronic mail addresses, much of the data used in cyber security is typically not, in and of itself, sensitive consumer data. Second, the Preliminary Report recognizes that fraud detection is part of "commonly accepted practices" for which consent is not required, recognizing the less sensitive nature of such information, and the importance of cyber security, from a consumer protection standpoint. Third, as discussed below, detailed disclosure of data use and collection for security purposes may make electronic commerce less secure and thereby reduce consumer welfare. Fourth, because the FTC, as part of the Framework, is suggesting that companies incorporate data security practices into their operations, security companies should not be hampered by the need to provide detailed disclosure concerning their data use and collection practices. The FTC's record in security-related prosecutions is testament to the need to create regulations that encourage, rather than hamper, cyber security.

For these reasons, ThreatMetrix does not believe that companies engaged in cyber security, particularly fraud detection, should be covered under the framework as proposed in the Preliminary Report (the "Proposed Framework"). Existing notice requirements coupled with the FTC's enforcement tools provide sufficient protection for any misuse of personally identifiable information in a security context.

Special choice for online behavioral advertising: Do Not Track

ThreatMetrix agrees with the FTC's approach to limiting "Do Not Track" to behavioral advertising, Preliminary Report @ 63, and urges that the FTC explicitly state that "Do Not Track" should not be expanded into cyber security applications. Tracking a packet or device as it travels through the internet creates critical factual data used to detect online

fraud. Removing tracking capability will provide anonymity to a fraudster and reduce the likelihood that fraud will be detected. This reduction of security could reduce cyber security and thereby reduce consumer use of the internet for commerce.

Companies should increase the transapaency of their data practices – Improved privacy notices

The Framework requires data collection entities to provide greater transparency concerning their data collection and use. If the FTC does not completely exclude cyber security firms from the Proposed Framework, then the disclosure required for security purposes should be standardized to be limited solely to a statement that data provided by a consumer or the consumer's device will be used for fraud detection.

The need for companies not engaging in commonly accepted practices to provide sufficient disclosure for choice may bleed into a requirement of greater disclosure for all entities that collect data absent a clear exception to the contrary. Detailed disclosure creates a number of adverse impacts to electronic commerce while not adding materially to privacy protection. Detailed disclosure may reduce consumer welfare by providing fraudsters with critical information to circumvent cyber security[1]. With the exception of personally identifying email, information valuable to security may not raise privacy concerns, making disclosure unnecessary. Detailed disclosure may also result in privacy policies that are long and difficult to understand, a current problem with privacy policies the FTC is attempting to resolve. Because cyber security companies have different approaches, it will be difficult to provide standardized disclosure. Last, many of the techniques used by cyber security firms are available in general form on their website, and are therefore available to those consumers who are interested.

The Preliminary Report discusses data enhancement and deep packet inspection as particular areas of concern. ThreatMetrix is apprehensive that the FTC's concerns may give rise to a disclosure requirement specific to these techniques.

Detailed disclosure regarding data enhancement and deep packet inspection is problematic and potentially counterproductive to security. Data can be collected from a number of different sources. Tracking the relationships between this data is an important security methodology. Providing detailed disclosure with respect to the collection and use of enhanced data in a fraud detection context would allow fraudsters to become aware of specific detection technologies used, thereby enabling them to develop workarounds to allow their activities to go undetected.

Deep packet inspection for fraud detection is an area of potentially fruitful technology development. Requiring detailed disclosure of deep packet inspection technologies for security purposes may limit further development in this important fraud detection tool. If

[1] Legal remedies regarding fraud and security circumvention may not be available against fraudsters operating in other countries, and may be too expensive to be pursued by an individual consumer or electronic commerce site. As a result, fraud detection technology is often the most effective method of promoting consumer use of electronic commerce.

the FTC determines that disclosure is necessary for use of deep packet information, then the specific disclosure should be limited to data describing children, financial and medical information, and precise geolocation information that can be linked to a particular individual.

Companies should increase the transparency of their data practices – Reasonable access to consumer data

Access to consumer data should be treated differently for non-consumer faceting entities, particularly those engaged in promoting fraud detection. ThreatMetrix supports a sliding scale where access depends on the sensitivity of the data and its intended use, especially for non-consumer facing entities such as security firms. Data collected and used for cyber security purposes should be highly sensitive to privacy concerns before access is permitted. Access to electronic mail addresses should be easier than access to a dynamic internet address, for example. Because much data used for security is aggregated, parceling the data for a particular individual may be expensive, and impossible. To the extent providing the data is possible, it should be done at the consumer's expense.

Companies should increase the transparency of their data practices – Material changes

Transparency of data collection and use practices can interfere with fraud detection efforts. As mentioned above, disclosure of information collection and use for cyber security can provide information enabling a fraudster to circumvent security mechanisms. Fraud detection requires substantial flexibility to successfully detect and disable fraud perpetration technology, and changing the manner in which data is used is critical to preventing online fraud. Cyber security companies' ability to rapidly develop new techniques for detection in response to new fraud perpetration technologies may be impaired if they are required to disclose any changes they make to the manner in which they use collected data. The Proposed Framework should be modified to state affirmatively that detailed disclosures as to changes in data use for fraud detection should not be required.

Respectfully submitted,

Bert Rankin
Vice President of Marketing
ThreatMetrix Inc.
5150 El Camino Real, Suite D-30
Los Altos, CA 94022