Federal Trade Commission
Title: Federal Trade Commission (Bureau of Consumer Protection) Staff Report
Subject Category: A Preliminary FTC Staff Report on "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers"
Comments Due: February 18, 2011

COMMENTS OF KOUNT INC.

To

THE FEDERAL TRADE COMMISSION

In Response to Questions for Comment on Proposed Framework

I. Introduction

A. Kount Inc.

On behalf of Kount Inc. ("Kount"), I am pleased to submit the following comments. Kount was founded in January 2008 to provide online and catalog merchants with advanced compliance technologies to meet multiple legal and commercial requirements. Kount's technology produces a unique "fingerprint" of devices used to make online purchases to detect if the user of a particular device is attempting identity or other fraud via an anonymous proxy or other schemes.

By combining this fingerprinting feature with a risk-based scoring model and a powerful software platform, Kount's system completes multiple compliance checks to allow merchants and other parties to manage cost-effectively, in real time, and in compliance with legal and other requirements—large volumes of on-line orders.

www.kount.com
917 s. lusk street | boise, idaho 83706

B. FTC Request for Comments

On December 2, 2010, the Federal Trade Commission (the "Commission") published the Preliminary FTC Staff Report entitled "A Proposed Framework for Business and Policymakers" (the "Report"). The Commission invited public response to questions related to the proposed privacy framework in the Report by the Commission (the "Proposed Framework").[1] Central to the Proposed Framework is a proposal that would allow consumers to use a browser-based mechanism to prevent tracking of online activities and transactions ("Do Not Track").

C. Apparent Conflict with Required Compliance Measures

The Report acknowledged that there should be some exceptions to Do Not Track for "commonly accepted practices," including fraud prevention and legal compliance and public purpose. (Report at 53-54). The Report's discussion and reference to these exceptions was narrow and did not fully define or offer a scope of exceptions to Do Not Track. The gist of the proposal, even with exceptions, raises a concern that it may conflict directly with currently required or expected compliance measures. As discussed below, our view is that, without clear and robust exceptions, Do Not Track could inadvertently prohibit measures that are central to

---

[1] Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework For Businesses and Policymakers; Preliminary Staff Report, December 2010*, available at http://www.ftc.gov/opa/2010/12/privacyreport.shtm.

compliance with multiple other federal legal requirements, as well as certain state and industry-specific requirements.

The federal legal requirements at issue address important U.S. national security, foreign policy, anti-terrorism, money laundering and anti-fraud initiatives. Many of these laws are core to U.S. sanctions on countries, such as Iran, Syria and other state supporters of terrorism. These laws are also central to anti-proliferation and money laundering protections.

These comments below elaborate on the apparent significant conflict between compliance measures required to meet these important legal obligations and Do Not Track. Kount is pleased to assist the Commission in identifying these issues for its consideration so that any policy proposed by the Commission is harmonized with these other goals and requirements.

II. Legal Compliance and Device Fingerprinting

A. Device Fingerprinting and Similar Functions Are Essential for Compliance with Federal Laws Supporting National Security, Foreign Policy and Other Significant U.S. Interests.

Kount provides software that allows "device fingerprinting," collection and analysis of as many as 200 points of non-personally identifiable data relating to online transactions. The Kount program is a powerful tool for identifying irregularities in online transactions based on key data points that are captured and analyzed in real time. These data points include browser configuration elements, the location of the device, the location of the Internet service provider

involving the device and any past fraudulent activity involving the same the credit card user, buyer, or device. Additionally, device fingerprinting provides real time data about fraud across multiple merchants, around the world. As a result, device fingerprinting can identify, among other things, velocity data (also known as "fraud runs"), as they happen so that Internet merchants can react swiftly to prevent illegal transactions, circumvention of U.S. sanctions or trade controls and/or losses from other illicit activities.

B. "Do Not Track" Would Conflict with Device Fingerprinting and Other Necessary Compliance Features

Under the Do Not Track proposal, consumers would be offered a mechanism in their Internet browser that would prevent tracking of their activities online. If adopted in a broad manner without comprehensive exceptions, the proposal would prevent the gathering and analysis of even basic information including geo-locating, IP addresses, and Internet browser configuration elements. As a result, merchants and others parties could not gather essential data required for device fingerprinting. In turn, parties seeking to circumvent U.S. controls on sanctioned countries, financial transactions and other illicit conduct would find U.S. companies "blinded" to their Internet activities. This "blinding" of data would remove an essential compliance tool on which U.S. companies rely to demonstrate effective efforts to prevent this sort of illegal conduct.

C. Device Fingerprinting Is an Essential Compliance Tool to Meet Legal Requirements Addressing National Security and Foreign Policy Concerns

Numerous federal laws prohibit U.S. businesses from engaging in transactions, providing products, services or information to countries, companies and individuals who are subject to trade sanctions ("Restricted Parties"). Device fingerprinting is a state-of-the-art tool used by many U.S. companies to identify Restricted Parties and report attempted circumvention of U.S. trade sanctions. Confronted with thousands of transactions happening all at once, many U.S. companies have adopted device fingerprinting or analogous technologies to flag transactions or parties. Proving the need for these systems to be dynamic and work in real-time, Restricted Parties are constantly engaged in efforts to circumvent U.S. controls, enter into prohibited transactions or acquire funds or technologies in contravention of U.S. law.

In this context, the adoption of Do Not Track -- without a broad and effective carve-out for fraud prevention and legal compliance-- would neutralize this important compliance element.

Generally, U.S. regulators measure the effectiveness of a compliance program on a scale that reflects the sophistication and resources of the company under review. Whether a company would be expected to have state-of-the-art control features, such as device fingerprinting, will depend on circumstances. For large companies with global operations, the standard is high and it would be expected that the global company would have a compliance feature that includes Kount or a similar offering.

As recently as December 2010, the U.S. Treasury Department - Office of Foreign Asset Control ("OFAC") settled an enforcement action against Wells Fargo Bank N.A. that underscored this obligation. OFAC found that "Wells Fargo exported financial services to Iran by performing financial services in the United States on behalf of an account holder while the account holder was located in Iran."[2] As part of the settlement, OFAC *required* Wells Fargo to "create and implement a risk-based OFAC compliance program, which includes the use of Internet Protocol addresses to identify registered users located in Iran."[3] Such programs are offered by Kount and other companies and involve tracking methodologies. Indeed, companies are more likely to meet federal compliance expectations if they employ robust tools such as device fingerprinting, as opposed to simple geo-location tools. Restricted Parties frequently use tools such as IP proxies and "spoofed" addresses to try and mask their identities so they can circumvent these sanctions. Device fingerprinting is designed to defeat such evasion without the use of personally identifiable information.

Attachment A is a chart summarizing the specific regulatory obligations related to U.S. trade sanctions and the effect on related compliance features if Do Not Track prohibits device fingerprinting or similar technologies. This chart also addresses other legal requirements discussed below.

---

[2] Enforcement Action pursuant to 31 C.F.R. § 501.805(d)(1)(i), U.S. Treasury, *available at* http://www.treasury.gov/resource-center/sanctions/CivPen/Documents/12212010.pdf.

[3] *Id.*

D. Device Fingerprinting Is an Essential Compliance Tool to Prevent Money Laundering and Meet Related Requirements

Device fingerprinting is also a key compliance tool to meet requirements of the Federal Financial Institution Examination Council, Customer Identification Program and Anti-Money Laundering provisions of The Bank Secrecy Act of 1970 ("BSA").[4] The BSA requires that banks and other financial institutions track certain transactions and report to law enforcement conduct that might indicate fraud, tax evasion, money laundering or other criminal activity. Given the prevalence of online banking, device fingerprinting is a vital tool to help banks comply with these obligations. Device fingerprinting helps banks confirm the location of their customers, whether the computer used by the customer has been involved in a suspicious number or type of transaction and other indicators of possible unlawful conduct.

Attachment A includes reference to applicable anti-money laundering obligations and the compliance features that would be impacted by Do Not Track.

E. Device Fingerprinting Is an Effective Anti-Fraud Measure that Benefits All Consumers

The Payment Card Industry Data Security Council ("PCI DSC") requires merchants to authenticate cardholder identities. Card associations uniformly categorize on-line transactions as a "high risk." Using Kount and other fraud prevention services reduces this risk by using geo-

---

[4] *See* Fed'l Financial Institutions Examination Manual, p. 208-209, *available at* http://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2010.pdf.

locating and other tracking technologies to identify transactions that indicate possible fraud. An essential part of Kount's evaluation is browser configuration, which can provide essential data to compare with other information to identify potentially fraudulent transactions.[5]

Such evaluations are consistent with the Commission's own "Red Flag Rule" and "Address Discrepancy Rule" which require businesses to detect evidence of fraud and address discrepancies.[6] A Do Not Track requirement that prohibits device fingerprinting would significantly undermine the ability of retailers to identify red flags or discrepancies and would defeat the purpose of these rules, themselves designed to protect consumers from fraud.

Further, robust device fingerprinting can serve to reduce identify theft and increase consumer privacy. As recognized by the Commission, brick and mortar retailers can check drivers' licenses at the point of purchase, and on-line retailers need a way to perform similar checks in an on-line fashion.[7] In fact, gathering of that sort of data – on-line – only increases risks of identity theft. Identity theft is a major concern for 87% of consumers who have made a

---

[5] For example, a device's browser history would reveal that a credit card belonging to a consumer living in Atlanta was being used by a person in Syria. Further, when evaluating the risk score of a purchase of a flat screen television, it would use velocity data to reveal that the same device and card was used to buy 10 other high priced electronics in the previous hour. The transaction would be flagged as likely involving fraud and the purchase would be denied.

[6] 16 C.F.R. §681.2.; 16 C.F.R. § 681.1(c).

[7] *See* Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework For Businesses and Policymakers; Preliminary Staff Report, December 2010*, Section V.C.1, (page 54): "Offline retailers check drivers' licenses when consumers pay by check to monitor against fraud. Online businesses also employ fraud detection services to prevent fraudulent transactions."

purchase or bank transaction on-line.[8] Device fingerprinting enables retailers to minimize or even avoid collection of personal information, such as drivers' license numbers, without increasing the risk of fraud or incurring the additional costs of ensuring data security. As stated by the Electronic Privacy Information Center ("EPIC") "the best long-term approach to the problem of identity theft is to minimize the collection of personal information."[9] Device fingerprinting provides a safe and efficient alternative by using data other than personal information to prevent fraud.

Location information used in device fingerprinting is one of the most effective non-personally identifiable indicators for fraud. According to a ClearCommerce® survey, 12 international locations account for the majority of online fraud: Ukraine, Indonesia, Yugoslavia, Lithuania, Egypt, Romania, Bulgaria, Turkey, Russia, Pakistan, Malaysia, and Israel.[10] Geo-location information alerts retailers when an order originates from one of these high risk countries. Accordingly, the use of location data in for device fingerprinting is an essential, generally accepted practice for which prior consent must not be required.

---

[8] August 2010, Identity Theft Resource Center, ITRC Consumer Internet Transaction Concerns Survey, *available at http://www.idtheftcenter.org/artman2/uploads/1/Consumer_Concerns_Survey_20100813.pdf*

[9] EPIC, *Comments to the Federal Identity Theft Task Force, P065410* (Jan. 19, 2007), *available at* http://www.epic.org/privacy/idtheft/EPIC_FTC_ID_Theft_Comments.pdf.

[10] ClearCommerce, Inc., White Paper: Fraud Prevention Guide, *available at* http://www.atg.com/repositories/ContentCatalogRepository_en/products/clearcommerce_fraud_protection.pdf

Finally, if Do Not Track creates obstacles to device fingerprinting, predictably, there will be an increase in on-line fraud. As a result, merchant banks may be obliged to increase the fees they charge to businesses conducting sales over the internet. Ultimately, that cost will be passed on to consumers.

Attachment A provides a reference to these consumer protection laws and related compliance features that would be impacted by Do Not Track.

III. Conclusion

Kount appreciates the privacy concerns at the core of the Do Not Track proposal. Any resultant recommendations or regulations, however, must accommodate the need for essential compliance features discussed above. The Commission should not contemplate having businesses compromise compliance features that are designed to meet national security, foreign policy, money laundering and consumer protection concerns. Similarly, no consumer should have to pay higher costs for online purchases due to increased – but avoidable – on-line fraud.

It appears, therefore, that the Commission should review the proposal with this in mind, perhaps to broaden the scope of the proposed exemptions for fraud prevention and legal compliance to permit unambiguously compliance tools, such as device fingerprinting.

Respectfully submitted,

Brad Wiskirchen
Chief Executive Officer
Kount, Inc.