

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.

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

Page 2

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.shtml>.

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

Page 3

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

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

Page 4

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.

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

Page 5

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.

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

Page 6

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.*

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

Page 7

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.

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

Page 8

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."

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

Page 9

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

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

Page 10

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.

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

Page 11

Respectfully submitted,

Brad Wiskirchen
Chief Executive Officer
Kount, Inc.

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

Kount, Inc.

Attachment A

Legal Requirements	Utility of Device Fingerprinting, Geolocating or Similar Tracking Features	Potential Impact of "Do Not Track" on Compliance Features
Treasury Department - Office of Foreign Assets Control (OFAC) <u>Country Controls</u>		
Reasons for Country Controls: National Security and Foreign Policy		
Balkans – Prohibition on transactions with designated persons who threaten international stabilization efforts in the Balkans.	Allows merchant to halt transaction if computer or ISP is in the Balkans or other data indicate a strong possibility of diversion to the Balkans.	Negates necessary compliance features
Belarus – Prohibition on transactions with designated persons who committed human rights abuses.	Allows merchant to halt transaction if computer or ISP is in Belarus or other data indicate a strong possibility of diversion to Belarus.	Negates necessary compliance features

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

Page 2

Legal Requirements	Utility of Device Fingerprinting, Geolocating or Similar Tracking Features	Potential Impact of "Do Not Track" on Compliance Features
Burma (Myanmar) – Prohibition on transactions with designated nationals of Burma. Prohibition on engaging in exporting financial services and importing Burmese products.	Allows merchant to halt transaction if computer or ISP is in Burma or other data indicate a strong possibility of diversion to Burma.	Negates necessary compliance features
Cote d'Ivoire (Ivory Coast) – Prohibition on transactions with designated persons who have incited violence, delivered arms or otherwise threatened the peace.	Allows merchant to halt transaction if computer or ISP is in Cote d'Ivoire or other data indicate a strong possibility of diversion to Cote d'Ivoire.	Negates necessary compliance features
Cuba – Embargo. Comprehensive OFAC sanctions. Almost no transactions or exports allowed.	Allows merchant to halt transaction if computer or ISP is in Cuba or other data indicate a strong possibility of diversion to Cuba.	Negates necessary compliance features
Democratic Republic of the Congo – Arms Embargo.	Allows merchant to halt transaction if computer or ISP is in Congo or other data indicate a strong possibility of diversion to Congo.	Negates necessary compliance features
Iran – Embargo. Comprehensive OFAC sanctions. Almost no transactions or exports allowed.	Allows merchant to halt transaction if computer or ISP is in Iran or other data indicate a strong possibility of diversion to Iran.	Negates necessary compliance features
Iraq – Prohibition on transactions with designated persons associated with former Iraqi regime. Prohibition on engaging in transactions involving	Allows merchant to halt transaction if computer or ISP is in Iraq or other data indicate a strong possibility of diversion to	Negates necessary compliance

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

Page 3

Legal Requirements	Utility of Device Fingerprinting, Geolocating or Similar Tracking Features	Potential Impact of "Do Not Track" on Compliance Features
--------------------	--	---

certain Iraqi cultural property.	Iraq.	features
Liberia – Prohibition on transactions with designated persons associated with former Liberian regime; designated narcotics traffickers; weapons of mass destruction proliferators or supporters. Prohibition on importing products produced or provided by persons subject to nonproliferation sanctions.	Allows merchant to halt transaction if computer or ISP is in Liberia or other data indicate a strong possibility of diversion to Liberia.	Negates necessary compliance features
Lebanon – Prohibition on transactions with designated persons associated with undermining the sovereignty of Lebanon.	Allows merchant to halt transaction if computer or ISP is in Lebanon or other data indicate a strong possibility of diversion to Lebanon.	Negates necessary compliance features
North Korea – Near Embargo. Almost no transactions or exports allowed. Prohibition on importing products from North Korea. Prohibitions on receiving certain transfers from the North Korean government including donations.	Allows merchant to halt transaction if computer or ISP is in N. Korea or other data indicate a strong possibility of diversion to N. Korea.	Negates necessary compliance features
Somalia – Prohibition on transactions with designated persons, individuals and entities who have engaged in acts that threaten the peace, security, or stability of Somalia or to have obstructed the delivery of humanitarian assistance.	Allows merchant to halt transaction if computer or ISP is in Somalia or other data indicate a strong possibility of diversion to Somalia.	Negates necessary compliance features
Sudan – Embargo. Prohibition on nearly all transactions and financial	Allows merchant to halt transaction if computer or ISP is	Negates necessary

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

Page 4

Legal Requirements	Utility of Device Fingerprinting, Geolocating or Similar Tracking Features	Potential Impact of "Do Not Track" on Compliance Features
dealings.	in Sudan or other data indicate a strong possibility of diversion to Sudan.	compliance features
Syria – Limited Embargo - Prohibition on with designated nationals of Syria and receiving certain transfers from the Syrian government, including donations. Prohibition on engaging in transactions with designated terrorists or terrorist organizations.	Allows merchant to halt transaction if computer or ISP is in Syria or other data indicate a strong possibility of diversion to Syria.	Negates necessary compliance features
Zimbabwe – Prohibition on engaging in transactions with designated persons who undermine democratic processes or institutions in Zimbabwe.	Allows merchant to halt transaction if computer or ISP is in Zimbabwe or other data indicate a strong possibility of diversion to Zimbabwe.	Negates necessary compliance features

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

Page 5

Legal Requirements	Utility of Device Fingerprinting, Geolocating or Similar Tracking Features	Potential Impact of "Do Not Track" on Compliance Features
<p>Department of Commerce - Bureau of Industry and Security (BIS) <u>Country Controls</u></p>		
<p>Reasons for BIS Country Controls: National Security and Foreign Policy</p>		
<p>Burma – License required for all items exported to Burma</p>	<p>Allows merchant to halt transaction if computer or ISP is in Burma or other data indicate a strong possibility of diversion to Burma.</p>	<p>Negates necessary compliance features</p>
<p>Cuba – Embargo on most exports.</p>	<p>Allows merchant to halt transaction if computer or ISP is in Cuba or other data indicate a strong possibility of diversion to Cuba.</p>	<p>Negates necessary compliance features</p>
<p>Iraq – Arms embargo and license required for all other items exported to military end use or user.</p>	<p>Allows merchant to halt transaction if computer or ISP is in Iraq or other data indicate a strong possibility of diversion to Iraq.</p>	<p>Negates necessary compliance features</p>
<p>Iran – Embargo on most exports.</p>	<p>Allows merchant to halt transaction if computer or ISP is in Iran or other data indicate a strong possibility of diversion to</p>	<p>Negates necessary compliance features</p>

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

Page 6

Legal Requirements	Utility of Device Fingerprinting, Geolocating or Similar Tracking Features	Potential Impact of "Do Not Track" on Compliance Features
---------------------------	---	--

	Iran.	
North Korea – General policy of export denial except for items not on control list.	Allows merchant to halt transaction if computer or ISP is in N. Korea or other data indicate a strong possibility of diversion to N. Korea.	Negates necessary compliance features
Rwanda – Arms embargo.	Allows merchant to halt transaction if computer or ISP is in Rwanda or other data indicate a strong possibility of diversion to Rwanda.	Negates necessary compliance features
Syria – General policy of denial on most exports.	Allows merchant to halt transaction if computer or ISP is in Syria or other data indicate a strong possibility of diversion to Syria.	Negates necessary compliance features

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

Page 7

Legal Requirements	Utility of Device Fingerprinting, Geolocating or Similar Tracking Features	Potential Impact of "Do Not Track" on Compliance Features
<p>Department of State – Directorate of Defense Trade Controls (DDTC) <u>Country Controls</u></p>		
<p>Reasons for DDTC Country Controls: National Security and Foreign Policy</p>		
<p>Afghanistan – DDTC denies licenses and other approvals of defense article exports and services.</p>	<p>Allows merchant to halt transaction if computer or ISP is in Afghanistan or other data indicate a strong possibility of diversion to Afghanistan.</p>	<p>Negates necessary compliance features</p>
<p>China – DDTC denies licenses and other approvals of defense article exports and services.</p>	<p>Allows merchant to halt transaction if computer or ISP is in China or other data indicate a strong possibility of diversion to China.</p>	<p>Negates necessary compliance features</p>
<p>Eritrea – DDTC denies licenses and other approvals of defense article exports and services.</p>	<p>Allows merchant to halt transaction if computer or ISP is in Belarus or other data indicate a strong possibility of diversion to Belarus.</p>	<p>Negates necessary compliance features</p>
<p>Cyprus – DDTC denies licenses and other approvals of defense article exports and services except to UN Forces.</p>	<p>Allows merchant to halt transaction if computer or ISP is in Cyprus or other data indicate a strong possibility of diversion</p>	<p>Negates necessary compliance features</p>

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

Page 8

Legal Requirements	Utility of Device Fingerprinting, Geolocating or Similar Tracking Features	Potential Impact of "Do Not Track" on Compliance Features
	to Cyprus.	
Haiti – DDTC denies licenses and other approvals of defense article exports and services.	Allows merchant to halt transaction if computer or ISP is in Haiti or other data indicate a strong possibility of diversion to Haiti.	Negates necessary compliance features
Iran – DDTC denies licenses and other approvals of defense article exports and services.	Allows merchant to halt transaction if computer or ISP is in Iran or other data indicate a strong possibility of diversion to Iran.	Negates necessary compliance features
Iraq – Denies licenses, other approvals, exports and defense services, defense articles to the extent specified in U.N. arms embargo.	Allows merchant to halt transaction if computer or ISP is in Iraq or other data indicate a strong possibility of diversion to Iraq.	Negates necessary compliance features
Lebanon – Denies licenses, other approvals, exports and defense services, defense articles to the extent specified in U.N. arms embargo.	Allows merchant to halt transaction if computer or ISP is in Lebanon or other data indicate a strong possibility of diversion to Lebanon.	Negates necessary compliance features
Liberia – Denies licenses, other approvals, exports and defense services, defense articles to the extent specified in U.N. arms embargo.	Allows merchant to halt transaction if computer or ISP is in Liberia or other data indicate a strong possibility of diversion to Liberia.	Negates necessary compliance features
Libya – DDTC denies licenses and other approvals of defense article	Allows merchant to halt transaction if computer or ISP is	Negates necessary

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

Page 9

Legal Requirements	Utility of Device Fingerprinting, Geolocating or Similar Tracking Features	Potential Impact of "Do Not Track" on Compliance Features
exports and services.	in Libya or other data indicate a strong possibility of diversion to Libya.	compliance features
North Korea – Denies licenses, other approvals, exports and defense services, defense articles.	Allows merchant to halt transaction if computer or ISP is in N. Korea or other data indicate a strong possibility of diversion to N. Korea.	Negates necessary compliance features
Rwanda – Denies licenses, other approvals, exports and defense services, defense articles.	Allows merchant to halt transaction if computer or ISP is in Rwanda or other data indicate a strong possibility of diversion to Rwanda.	Negates necessary compliance features
Sierra Leone – Denies licenses, other approvals, exports and defense services, defense articles to the extent specified in U.N. arms embargo.	Allows merchant to halt transaction if computer or ISP is in Sierra Leone or other data indicate a strong possibility of diversion to Sierra Leone.	Negates necessary compliance features
Somalia – Denies licenses, other approvals, exports and defense services, defense articles to the extent specified in U.N. arms embargo.	Allows merchant to halt transaction if computer or ISP is in Somalia or other data indicate a strong possibility of diversion to Somalia.	Negates necessary compliance features
Sudan – Denies licenses, other approvals, exports and defense services, defense articles.	Allows merchant to halt transaction if computer or ISP is in Belarus or other data indicate a strong possibility of diversion to Belarus.	Negates necessary compliance features

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

Page 10

<p>Legal Requirements</p>	<p>Utility of Device Fingerprinting, Geolocating or Similar Tracking Features</p>	<p>Potential Impact of "Do Not Track" on Compliance Features</p>
<p>Sri Lanka – Denies licenses, other approvals, exports and defense services, defense articles.</p>	<p>Allows merchant to halt transaction if computer or ISP is in Sri Lanka or other data indicate a strong possibility of diversion to Sri Lanka.</p>	<p>Negates necessary compliance features</p>
<p>Syria – Denies licenses, other approvals, exports and defense services, defense articles.</p>	<p>Allows merchant to halt transaction if computer or ISP is in Syria or other data indicate a strong possibility of diversion to Syria.</p>	<p>Negates necessary compliance features</p>
<p>Vietnam – Denies licenses, other approvals, exports and defense services, defense articles.</p>	<p>Allows merchant to halt transaction if computer or ISP is in Vietnam or other data indicate a strong possibility of diversion to Vietnam.</p>	<p>Negates necessary compliance features</p>
<p><u>Limited Country Controls</u> Some restrictions on licenses to sell defense articles to:</p>		
<p>Cyprus</p>	<p>Allows merchant to halt transaction if computer or ISP is in Cyprus or other data indicate a strong possibility of diversion to Cyprus.</p>	<p>Negates necessary compliance features</p>
<p>Guinea</p>	<p>Allows merchant to halt transaction if computer or ISP is in Guinea or other data indicate a strong possibility of diversion to Guinea.</p>	<p>Negates necessary compliance features</p>

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

Page 11

Legal Requirements	Utility of Device Fingerprinting, Geolocating or Similar Tracking Features	Potential Impact of "Do Not Track" on Compliance Features
Indonesia	Allows merchant to halt transaction if computer or ISP is in Indonesia or other data indicate a strong possibility of diversion to Indonesia.	Negates necessary compliance features
Niger	Allows merchant to halt transaction if computer or ISP is in Niger or other data indicate a strong possibility of diversion to Niger.	Negates necessary compliance features
Palestine	Allows merchant to halt transaction if computer or ISP is in Palestine or other data indicate a strong possibility of diversion to Belarus.	Negates necessary compliance features
Yemen	Allows merchant to halt transaction if computer or ISP is in Yemen or other data indicate a strong possibility of diversion to Yemen.	Negates necessary compliance features
Zimbabwe	Allows merchant to halt transaction if computer or ISP is in Zimbabwe or other data indicate a strong possibility of diversion to Zimbabwe.	Negates necessary compliance features

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

Page 12

<p>Legal Requirements</p>	<p>Utility of Device Fingerprinting, Geolocating or Similar Tracking Features</p>	<p>Potential Impact of "Do Not Track" on Compliance Features</p>
<p>Treasury Department – Office of Foreign Asset Controls (OFAC) <u>List-Based Restricted Party Controls</u></p>		
<p>Reasons for OFAC List-Based Controls: National Security, Foreign Policy, Crime Control, and Narcotics Interdiction</p>		
<p>Specially Designated Nationals List Generally listing parties attempting to circumvent country controls, also global terrorists (and their supporters), narcotics traffickers and others. Extensive list of thousands of parties, aliases, supporters and others.</p>	<p>Allows merchant to halt transaction if computer or ISP is in suspect country, if specially designated name or address is present or other data indicate a strong possibility of diversion or illegal activities.</p>	<p>Negates necessary compliance features</p>

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

Page 13

<p>Legal Requirements</p>	<p>Utility of Device Fingerprinting, Geolocating or Similar Tracking Features</p>	<p>Potential Impact of "Do Not Track" on Compliance Features</p>
<p>State Department – Directorate of Defense Trade Controls (DDTC) <u>List-Based Restricted Party Controls</u></p>		
<p>Reasons for DDTC List-Based Controls: National Security and Foreign Policy</p>		
<p>Debarred Parties List Parties barred by the International Traffic in Arms Regulations (ITAR) from directly or indirectly, through financing or otherwise, participating in defense trade under the jurisdiction of the United States.</p>	<p>Allows merchant to halt transaction if debarred party name or address is present or other data indicate a strong possibility of diversion or illegal conduct.</p>	<p>Negates necessary compliance features</p>
<p>Nonproliferation Sanctions Foreign individuals, private entities, and governments that engage in weapons proliferation activities. Examples include:</p> <ul style="list-style-type: none"> • Executive Order 13382 • Executive Order 12938 • Missile Tech Control Regime Sanctions • Chemical and Biological Weapons Sanctions • Sanctions for the Transfer of Lethal Military Equipment 	<p>Allows merchant to halt transaction if computer or ISP is in suspect country, if designated name or address is present or other data indicate a strong possibility of diversion.</p>	<p>Negates necessary compliance features</p>

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

Page 14

Legal Requirements	Utility of Device Fingerprinting, Geolocating or Similar Tracking Features	Potential Impact of "Do Not Track" on Compliance Features
<p>Commerce Department – Bureau of Industry and Security (BIS) <u>BIS List-Based Restricted Party Controls</u></p>		
<p>Reasons for Controls: National Security, Foreign Policy, and Crime Control</p>		
<p>Denied Persons List Parties who are denied export privileges or ability to participate in export transactions.</p>	<p>Allows merchant to halt transaction if denied party name or address is present or other data indicate a strong possibility of diversion or illegal activities.</p>	<p>Negates necessary compliance features</p>
<p>Unverified List Parties to a transaction with respect to which BIS could not conduct pre-license or a post-shipment verification. Higher risk of diversion.</p>	<p>Allows merchant to halt transaction if unverified party name or address is present or other data indicate a strong possibility of diversion or other illegal activities.</p>	<p>Negates necessary compliance features</p>
<p>Entity List Individuals and companies subject to specific license requirements due to proliferation concerns.</p>	<p>Allows merchant to halt transaction if entity name or address is present or other data indicate a strong possibility of diversion or illegal conduct.</p>	<p>Negates necessary compliance features</p>

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

Page 15

<p>Legal Requirements</p>	<p>Utility of Device Fingerprinting, Geolocating or Similar Tracking Features</p>	<p>Potential Impact of "Do Not Track" on Compliance Features</p>
<p>Bank Secrecy Act (Departments of Justice and Treasury) Contains core anti-money laundering controls; requires preventive measures or submission of suspicious activity reports (SARs) in certain transactions.</p>		
<p>Reasons for Control: Crime Control, Consumer Protection, and Fraud Prevention.</p>		
<p>Anti-Money Laundering Controls Require financial institutions and other entities to implement effective anti-money laundering systems and programs for identifying suspicious transactions.</p>	<p>Allows covered entities to identify, track, and report illegal conduct or patterns of suspicious behavior.</p>	<p>Negates necessary compliance features</p>
<p>Customer Identification Program Controls Require financial institutions and other entities to implement effective programs for verifying identity, including location, of all parties to a financial transaction.</p>	<p>Allows covered entities to implement and maintain effective Customer Identification Programs and to identify conduct designed to circumvent these controls.</p>	<p>Negates necessary compliance features</p>
<p>Federal Financial Institutions Examination Manual Establishes standards for financial institutions and other entities to comply with the Anti-Money Laundering and Customer Identification Program controls.</p>	<p>Allows covered entities to track effectively Internet Protocol ("IP") address location and geo-location to prevent fraud and money laundering.</p>	<p>Negates necessary compliance features</p>

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

Page 16

<p>Legal Requirements</p>	<p>Utility of Device Fingerprinting, Geolocating or Similar Tracking Features</p>	<p>Potential Impact of "Do Not Track" on Compliance Features</p>
<p>Fair Credit Reporting Act (as amended by the Fair and Accurate Credit Transactions Act) (Federal Trade Commission and State Attorney Generals).</p> <p>Requires users of consumer reports to recognize certain indicia of fraud</p>		
<p>Reasons for Control:</p> <p>Consumer Protection, Identity Theft Prevention, and Fraud Prevention.</p>		
<p>Red Flag Rule</p> <p>Requires any person who extends credit in a consumer transaction to implement procedures to detect certain red flags for fraud.</p>	<p>Allows effective implementation of Identity Theft Prevention Program that is intended to alert merchant to possible discrepancies in consumer information or other indicia of illegal conduct.</p>	<p>Negates necessary compliance features</p>

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

Page 17

<p align="center">Legal Requirements</p>	<p align="center">Utility of Device Fingerprinting, Geolocating or Similar Tracking Features</p>	<p align="center">Potential Impact of "Do Not Track" on Compliance Features</p>
<p>Address Discrepancy Rule Requires users of consumer reports to employ heightened scrutiny whenever the user receives notice of address discrepancy.</p>	<p>Allows effective compliance with requirement to obtain additional identification if there is discrepancy between address associated with application and addresses contained within consumer report; enables report of discrepancy to credit bureaus.</p>	<p>Negates necessary compliance features</p>
<p>Payment Card Industry Data Security Standards (PCI DSS) Require parties accepting credit card payment to protect cardholder data and authenticate identity of the cardholder.</p>		
<p>Reasons for Control: Consumer Protection, Identity Theft Prevention, and Fraud Prevention.</p>		
<p>Requires effective system to achieve PCI Data Security Standards</p>	<p>Allows parties to authenticate effectively identity of cardholder in a "card-not-present transaction," including higher requirements for high-risk internet merchants or transaction points.</p>	<p>Negates necessary compliance features</p>