Working Draft: This is our effort to compile the previous discussions and proposed text with regard to security and fraud prevention within the Tracking Protection Group. We apologize for any missed text or viewpoints or for including any issues unrelated to security and fraud prevention.

Security and Fraud Prevention

Tracking Compliance and Scope March, 6, 2013

http://www.w3.org/2011/tracking-protection/drafts/tracking-compliance.html#security

6.2.2.6 Security and Fraud Prevention

Information may be collected, retained and used to the extent reasonably necessary for detecting security risks and fraudulent or malicious activity. This includes data reasonably necessary for enabling authentication/verification, detecting hostile and invalid transactions and attacks, providing fraud prevention, and maintaining system integrity. In this example specifically, this information may be used to alter the user's experience in order to reasonably keep a service secure or prevent fraud. Graduated response is preferred when feasible.

There has been an unresolved discussion on whether "graduated response" should be in the normative text, defined, addressed through non-normative examples, or not included at all.

Tracking Compliance and Scope Oct. 2, 2012

http://www.w3.org/TR/tracking-compliance/#security

6.1.1.6 Security and Fraud Prevention

Regardless of DNT signal, information may be collected, retained and used for detecting security risks and fraudulent activity, defending from attacks and fraud, and maintaining integrity of the service. This includes data reasonably necessary for enabling authentication/verification, detecting hostile transactions and attacks, providing fraud prevention, and maintaining system integrity. In this example specifically, this information may be used to alter the user's experience in order to reasonably keep a service secure or prevent fraud.

NOTE

The more likely options at this point may be represented in Nick Doty's proposed:

To the extent reasonably necessary for protection of computers and networks and to detect ad or other fraud, third parties may engage in tracking. Use of graduated response is preferred.

or David Wainberg's proposed:

Parties may collect and use data in any way to the extent reasonably necessary for the detection and prevention of malicious or illegitimate activity.

ISSUE-24: Possible exemption for fraud detection and defense

http://www.w3.org/2011/tracking-protection/track/issues/24

ACTION-293: Draft non-normative examples illustrating graduated response

http://www.w3.org/2011/tracking-protection/track/actions/293

John Mayer's proposal March 13, 2012:
http://lists.w3.org/Archives/Public/public-tracking/2012Mar/0268.html
I. Fraud Prevention

A. Operative Text

"A third party may receive and use protocol information for the detection and prevention of security breaches and fraudulent activity, subject to a six-month retention period and the restrictions imposed in the subsequent sections on security and fraud prevention."

B. Non-Normative Discussion

When a user meaningfully interacts with third-party content (e.g. clicking an ad), the third party can collect, retain, and use information for fraud prevention. Third parties can also use protocol logs for fraud prevention. This exception provides an additional capability to, in certain circumstances, track impressions for fraud prevention.

II. Security

A. Operative Text

A third party may collect, retain, and use data about a particular user or user agent for the purpose of ensuring its security, provided that there are reasonable grounds to believe the user or user agent is presently attempting to breach the party's security.

B. Non-Normative Discussion

This exception grants third parties (e.g. advertising networks) some latitude to mitigate security risks. Websites that users store sensitive personal information on (e.g. financial services and webmail) are all first-party; they are able to collect, retain, and use information about all users for security purposes.

Roy Fielding and Shane Wiley Response:

http://lists.w3.org/Archives/Public/public-tracking/2012Mar/0269.html

http://lists.w3.org/Archives/Public/public-tracking/2012Mar/0290.html

Amsterdam Face to Face Oct. 4, 2012

http://www.w3.org/2012/10/04-dnt-minutes

ACTION-279: Write an explanation of graduated response and a list of explanatory use cases

http://www.w3.org/2011/tracking-protection/track/actions/279

Ian Fette proposal Oct. 24, 2012:

http://lists.w3.org/Archives/Public/public-tracking/2012Oct/0506.html

Graduated Response

A graduated response a methodology where the action taken is Proportional to the size of the problem or risk that is trying to be mitigated. In the context of this document, the term is used to describe an increase in the collection of data about a user or transaction in response to a specific

problem that a party has become aware of, such as an increase in fraudulent activity originating from a particular network or IP address range resulting in increased logging of data relating to transactions from that specific range of IP addresses as opposed to increased logging for all users in general.

Shane Wiley:

http://lists.w3.org/Archives/Public/public-tracking/2012Oct/0655.html

Would it be possible to look at "graduated response" in the opposite direction as an element of data minimization? Collect more data up-front (security, debugging, frequency capping) and move to less data where possible as a "graduated response". As I stated in Amsterdam, attempting to operational-ize a technical "graduated response" in the less->more sense is not a trivial matter (if at all really possible in most circumstances), whereas the opposite is much more doable.

ACTION-339: Propose a refinement to debugging permitted use

http://www.w3.org/2011/tracking-protection/track/actions/339

Walter Van Hoist proposal Dec. 5, 2012:

My suggestion would be not to use the term graduated response but 'proportionate response' and that:

A proportionate response to concrete indications that fraudulent and/or other malicious HTTP requests are being made is one that proportional to the size and impact of the percieved problem or the risk that is being mitigated. In the context of this document, the term is used to describe the collection of data about users, devices and network adresses in response to a specific problem that a party has become aware of, such as an increase in fraudulent activitiy from a particular network or IP address range. Such increased data collection MUST be as specific and brief as possible and MAY only result in increased logging for all users in general in extreme cases.

Related Issue:

ISSUE-31: Minimization -- to what extent will minimization be required for use of a particular exemption? (conditional exemptions)

http://www.w3.org/2011/tracking-protection/track/issues/31