IAB/W3C/ISOC/MIT
Internet Privacy Workshop
Position Paper
November 5, 2010

J. Fox
B. McDowell
PayPal

Protection-by-Design: Enhancing ecosystem capabilities to protect personal information

1. Background and Premise

In the IETF#77 plenary talk Balachander Krishnamurthy explained the status of data sharing for advertising purposes and suggested actions by the technical community in the IETF. Since this workshop is, at least in part, a response to that call for action it is worth noting that in the introduction of that presentation [1] Krishnamurthy posits:

* Security is about keeping unwanted traffic from entering our network
* Privacy is about keeping wanted information from leaving our network -- Privacy is thus the dual of security

Though we agree that Privacy and Security are bound, we disagree with this particular binding. We suggest the following:

* Security is about protecting systems and data from Abuse
* Abuse is about unauthorized exploitation of a system or its data
* Privacy is about the authorized use and access to personal information.
-- Good privacy practices are thus an outcome of applying good data management and security to enforce good policy.

Krishnamurthy goes on to focus exclusively on the “leakage” of PII through data sharing for advertising purposes, due primarily to various tracking techniques such as cookies. Though Internet Privacy architectures and technologies should help the community avoid unintended and unauthorized data sharing/”leakage”, if we focus exclusively on these advertising-oriented use cases and develop rigid anti-sharing/anti-tracking architectures, our solutions will actually be counter-productive to securing networked systems from the most prevalent forms of abuse we see today [2] and therefore will reduce our ability to ensure an environment that enables the authorized use and access of personal information, i.e. we will have undermined Internet Privacy, not improved it.

2. Security Considerations for Internet Privacy

We have posited that good privacy is the outcome of applying good data management and security to enforce good policy governing the collection, storage, and use of personal information. Therefore, we suggest a friendly amendment to the fundamental question being posed as the central organizing theme for this workshop:

“How can we ensure that architectures and technologies for the Internet, including the World Wide Web, are developed in a way that respects users’ privacy and enhances the capability of the ecosystem to better protect personal information from predators?”

We offer an answer to that question: The Use-and-Obligations Framework [3] developed by the Business Forum for Consumer Privacy. This framework provides operational clarity regarding how to evaluate policy-to-technology binding that other regimes such as the OECD Fair Information Practices [4] and the Privacy-by-Design 7 Foundational Principles [5] have only touched on in the past. We suggest that the Use-and-Obligations framework could be a useful requirements guideline for the next generation of Internet Privacy architectures and technologies.

In preparation for the workshop, we also offer the following two use cases where data sharing and user profiling techniques are used to improve privacy through enhanced security of personal information. We hope to illustrate that “technology doesn’t abuse privacy, people abuse privacy” by detailing these use cases at the workshop.

3. Protection-by-Design Use Case 1: Anti-Abuse Data Sharing

At PayPal, we have deployed email authentication [6] technologies and privacy policy compliant data sharing techniques to protect customers from being phished for their personal information and system credentials. Now when a message comes in that reports to be from us, but cannot be cryptographically verified as being from us, the mailbox provider (a) no longer delivers that message and (b) forwards a PII redacted copy of that message to us. We then take the contents of that message, investigate if it was sent by someone trying to phish information, and if so, we initiate a site takedown. The net result of this program is the blocking of approximately 175,000 phishing attacks and numerous phishing site takedowns every day.

This is an example of how data sharing works to enhance security and privacy, yet when viewed through the prism of certain privacy regimes even this data exchange has been called into question as a privacy risk. We believe this is due primarily to communication gap between what has traditionally be referred to as “the security community” and “the privacy community”. Closing that gap should be a strategic goal we all share so that we begin to recognize the truth, that we are all collectively “the Internet community”.

4. Protection-by-Design Use Case 2: Anti-Abuse Profiling

At PayPal, we use first-party cookies and other techniques to collect and profile information about the environment our users are in when they access our secured applications. Without these techniques, we would not be able to perform anti-fraud risk management analysis which is mission critical to the operation of our service and the protection of our customers’ personal information.

This is another example of technologies that are normally the ire of “the privacy community,” yet when deployed correctly by “the security community,” it actually improve the privacy of Internet users.

We look forward to exploring these issues with other members of “the Internet community” at the workshop.

References

[1]http://www.ietf.org/proceedings/77/slides/plenaryt-5.pdf
[2]Phishing & Malware (http://stopbadware.org/home/badware)
[3]http://www.huntonfiles.com/files/webupload/CIPL_Use_and_Obligations_White_Paper.pdf
[4]http://www.privacyrights.org/ar/fairinfo.htm
[5]http://www.privacybydesign.ca/about/principles
[6]https://otalliance.org/events/2010Forum/Presentations/OTA%20Auth%20Academy%20FINAL.pdf

Acknowledgments

This document greatly benefited from comments by Jeff Hodges, Laksh Raghavan, and Andy Steingruebl.

Author's Addresses

Jonathan Fox
eBay, Inc.
2145 Hamilton Ave.
San Jose, CA 95125

Email: jfox@ebay.com

Brett McDowell
PayPal, Inc.
2211 North First Street
San Jose, CA 95131

Email: bmcdowell@paypal-inc.com