

January 15, 2010

Internet Governance Forum Submission for the Vilnius Agenda

Dear IGF Secretariat:

The Electronic Privacy Information Center (EPIC) submits this letter for inclusion in the record as an input for the February consultation of the Internet Governance Forum, Vilnius Agenda. EPIC is a not-for-profit research center. It was established in 1994 to focus public attention on emerging privacy and civil liberties issues and to promote the Public Voice in decisions concerning the future of the Internet.

EPIC believes that the Internet Governance Forum provides a good opportunity to address the consumer and human rights perspective on Global Governance on privacy and data protection.

2009 was a busy year for privacy. Big Internet firms, such as Facebook and Google, created new challenges for Internet users as personal data became more valuable to advertisers. Many countries around the world considered different privacy bills, though few became law. The New Year promises even more news with biometric identifiers, smart grids, and related emerging privacy challenges.

For the 2010 Internet Governance Forum Agenda, EPIC proposes to discuss the following issues.

1. Global Privacy Standards for a Global World.

The protection of online privacy has quickly emerged as one of the most critical concerns of citizens in the information society. If we understand what the world will look like with real-time matching of facial images, routine identification requirements that rely on biometric data, the collection and matching of health information, family data and personal employment records, we will quickly understand how significant the problem we face is.

Those who are the least powerful politically, especially those groups of society who are most often discriminated against, will feel the loss of privacy first; those people who are excluded from employment, credit and medical care because of personal information contained in a computerized file, and travel across borders.

The roots of the problem are not difficult to understand. Our technological capabilities and our new business practices are racing fast ahead of our established expectations and our legal protections. It is clear that government has an important role to play in the new economy but it is not always clear what should be the best role for government. However, in the area of privacy there is already a well-established tradition of protection in law and through institutions.

The key point we would like to see discussed in the IGF 2010 is the need for legally enforceable global standards for the protection of personal data. Advocates around the world are rallying behind the Madrid Privacy Declaration. The big question at the end of 2010 will be whether there will be more privacy, more surveillance, or more of both.

2. Cloud Computing

What happens to your data when it's in the cloud? That's the issue that policymakers will look at more closely in 2010 around the world, not only because users are moving data to the cloud, but also because government agencies are. Still, the privacy and security risks are real, as well as issues of concentration of power, interoperability and open standards.

3. Green ICT & Smart grid: Will Your Power Meter Be Spying on You?

Standards are still being developed for the Smart Grid, a host of technologies that will modernize the existing electrical grid. The Smart Grid could enable more efficient delivery of electricity and allow consumers to make more informed energy use decisions. At the same time, Smart Grid technologies also raise troubling privacy possibilities that there could be very detailed tracking – and record keeping – of individuals' electric use. EPIC believes that the IGF provides an appropriate opportunity to bring different stakeholders to present their views on this emerging topic.

Conclusion

We believe that the IGF provides a unique opportunity to discuss emerging privacy challenges. The Internet provides an opportunity for growth, employment, development and innovation. But the benefits of the Internet economy cannot come - must not come - in exchange for the personal information of consumers, for the knowledge of the names and ages of their children, the prescription drugs they take, the candidates they support, and the opinions they hold. No economic system should impose such a cost on the privacy of consumers.

Consumers in a global economy share a common interest in the protection of basic rights and freedom. In the information society, one of the fundamental rights of citizen is surely the right to control the collection and use of personal information. The IGF must address these issues.

Respectfully submitted,

Marc Rotenberg
EPIC, Executive Director

Katitza Rodriguez
EPIC, International Privacy Program Director

About EPIC

The Electronic Privacy Information Center (“EPIC”) is a not-for-profit research center focusing on emerging privacy and civil liberties issues. EPIC is also a leading consumer advocate. EPIC was the first to bring the privacy risks of online advertising, to the US Federal Trade Commission’s (FTC) attention.¹

In 2004, EPIC filed a complaint with the FTC regarding the deceptive practices of data broker firm Choicepoint, calling the US Federal Trade Commission’s attention to “data products circumventing the US law, giving businesses, private investigators, and law enforcement access to data that previously had been

¹ In the Matter of DoubleClick, Complaint and Request for Injunction, Request for Investigation and for Other Relief, before the Federal Trade Commission (Feb. 10, 2000), *available at* http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf.

subjected to Fair Information Practices.”² As a result of the EPIC complaint, the FTC fined Choicepoint \$15 million.³

EPIC initiated a complaint to the FTC regarding Microsoft Passport.⁴ The Commission subsequently required Microsoft to implement a comprehensive information security program for Passport and similar services.⁵

EPIC also filed a complaint with the FTC regarding the marketing of amateur spyware,⁶ which resulted in the issuance of a permanent injunction barring sales of CyberSpy’s “stalker spyware,” over-the-counter surveillance technology sold for individuals to spy on other individuals.⁷

In 2009, EPIC filed a complaint with the Federal Trade Commission (FTC), urging the Commission to open an investigation into Google's Cloud Computing Services -- including Gmail, Google Docs, and Picasa -- to determine "the adequacy of the privacy and security safeguards." The complaint follows the recent report of a breach of Google Docs. EPIC cited the growing dependence of American consumers, businesses, and federal agencies on cloud computing services, and urged the Commission to take "such measures as are necessary" to ensure the safety and security of information submitted to Google.⁸

In 2009-2010, EPIC and nine other privacy and consumer organizations, has filed a complaint with the Federal Trade Commission, urging the FTC to open an investigation into Facebook’s revised privacy settings. The EPIC complaint states that the "changes violate user expectations, diminish user privacy, and

² In the Matter of Choicepoint, Request for Investigation and for Other Relief, before the Federal Trade Commission (Dec. 16, 2004), available at <http://epic.org/privacy/choicepoint/fcraltr12.16.04.html>

³ Federal Trade Commission, ChoicePoint Settles Data Security Breach Charges; to Pay \$10 Million in Civil Penalties, \$5 Million for Consumer Redress, <http://www.ftc.gov/opa/2006/01/choicepoint.shtm> (last visited Dec. 13, 2009).

⁴ In the Matter of Microsoft Corporation, Complaint and Request for Injunction, Request for Investigation and for Other Relief, before the Federal Trade Commission (July 26, 2001), available at http://epic.org/privacy/consumer/MS_complaint.pdf.

⁵ In the Matter of Microsoft Corporation, File No. 012 3240, Docket No. C-4069 (Aug. 2002), available at <http://www.ftc.gov/os/caselist/0123240/0123240.shtm>. See also Fed. Trade Comm’n, “Microsoft Settles FTC Charges Alleging False Security and Privacy Promises” (Aug. 2002) (“The proposed consent order prohibits any misrepresentation of information practices in connection with Passport and other similar services. It also requires Microsoft to implement and maintain a comprehensive information security program. In addition, Microsoft must have its security program certified as meeting or exceeding the standards in the consent order by an independent professional every two years.”), available at <http://www.ftc.gov/opa/2002/08/microst.shtm>.

⁶ In the *Matter of Awarenessstech.com*, et al., Complaint and Request for Injunction, Request for Investigation and for Other relief, before the Federal Trade Commission, available at http://epic.org/privacy/dv/spy_software.pdf

⁷ *FTC v. Cyberspy Software*, No. 6:08-cv-1872 (D. Fla. Nov. 6, 2008) (unpublished order), available at <http://ftc.gov/os/caselist/0823160/081106cyberspytro.pdf>.

⁸ In the Matter of Google, Request for Investigation and for Other Relief, before the Federal Trade Commission (2009), available at <http://epic.org/privacy/cloudcomputing/google/>

contradict Facebook's own representations." EPIC cites widespread opposition from Facebook users, security experts, bloggers, and news organizations.⁹

EPIC edits the publication *Privacy & Human Rights: An International Survey of Privacy Laws and Developments*, which is the most authoritative reference on privacy regulations and developments in 78 countries.¹⁰ The report outlines legal protections, new challenges, and important issues and events relating to privacy.

⁹ In the Matter of Facebook, Request for Investigation and for Other Relief, before the Federal Trade Commission (2009-2010), *available at* <<http://www.epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf>>.

¹⁰ EPIC, Privacy International. *Privacy and Human Rights Report. An International survey of privacy laws and developments, 2007*, *available at* <<http://privacyinternational.org/phr>>.