Testimony and Statement for the Record of

Marc Rotenberg
Executive Director, EPIC
Adjunct Professor, Georgetown University Law Center

"Communications Networks and Consumer Privacy:
Recent Developments"

Marc Rotenberg.
EPIC Executive Director

Before the

House Committee and Energy and Commerce
Subcommittee on Communications,
Technology and the Internet

April 23, 2009
2322 Rayburn House Office Building
Washington, DC

Mr. Chairman and Members of the Committee, thank you for the opportunity to testify today on "Communications Networks and Consumer Privacy: Recent Developments." My name is Marc Rotenberg and I am the Executive Director of the Electronic Privacy Information Center (EPIC) and Adjunct Professor at Georgetown University Law Center where I teach Information Privacy Law.

EPIC is a non-partisan research organization, focused on emerging privacy and civil liberties issues. We have a particular interest in communications networks and consumer privacy. EPIC began with a national campaign -- the first online petition -- to protect the freedom to use encryption, a critical technique for network privacy and security. For the past 15 years, EPIC has pursued many of the critical network privacy issues on behalf of Internet users. We have participated in the work of the ICANN on such technical standards as WHOIS [1] and DNSSEC,[2] and the original IETF review of the RFC for cookie management. [3]

We also support the authority of the FCC to establish enforceable safeguards for consumers. Over the past decade, EPIC has pursued several complaints at the FCC to promote consumer privacy, to improve security, and to reduce the risk that surveillance standards will jeopardize network integrity. [4] And EPIC has filed amicus briefs in the courts on many occasions both to safeguard communications privacy and to protect the rulemaking authority of the FCC. [5] On this last point, I am pleased

---

[1] EPIC, WHOIS, http://epic.org/privacy/whois/ (last visited Apr. 22, 2009).
[2] EPIC, DNSSEC, http://epic.org/privacy/dnssec/ (last visited Apr. 22, 2009).
[3] EPIC, Net Users Urge Standards Group to Protect Privacy, Apr. 7, 1997, *available at* http://epic.org/privacy/internet/cookies/ietf_letter.html.
[4] *See, e.g.* EPIC, NCTA v. FCC: Concerning Privacy of Customer Proprietary Network Information (CPNI), http://epic.org/privacy/nctafcc/; EPIC, Comments of the Electronic Privacy Information Center in the Matter of ACA International Petition for Expedited Clarification, FCC Docket No. 02-278, May 11, 2006, *available at* http://epic.org/privacy/telemarketing/fcc_aca_05-11-06.html.
[5] *See, e.g.* Brief of the Electronic Privacy Information Center, *U.S. West v. Federal Communications Commission*, 182 F.3d 1224 (10th Cir. 1999) (FCC opt-in privacy rule), *available at* http://epic.org/privacy/litigation/uswest/amicus_brief_SRPR.html; Supplemental Brief, *U.S. v. Councilman*, 418 F.3d 67 (1st Cir. 2005) (No. 03-1383) ("intercept" of stored communications), *available at* http://epic.org/privacy/councilman/kerr_amicus.pdf. See also, EPIC. "US West v. FCC -- The Privacy of Telephone Records, http://epic.org/privacy/litigation/uswest/ (last visited Apr. 22, 2009), EPIC,

to report that the D.C. Circuit Court of Appeals recently upheld an opt-in privacy standard to a challenge brought by the cable companies to an agency rule that we helped develop to safeguard consumers against data brokers.[6] EPIC filed an amicus in support of the FCC in that case.[7]

Online Advertising

Today I will focus my remarks on growing concerns about consumer privacy and network advertising. I should say at the outset that we do not object to online advertising. We recognize that advertising plays a critical role in enabling the provision of services and information on the Internet. It supports the sites maintained by bloggers and helps enable the free flow of information. Advertising helped launch and maintain the Internet economy.

At the same time, we believe it is becoming clear that unregulated collection of consumer data is posing an increasing danger to online privacy and maybe even to the economic model itself. A small number of companies and large advertising networks are obtaining an extraordinarily detailed profile of the interests, activities and personal characteristics of Internet users. Users have little idea how much information is gathered, who has access to it, or how it is used. This last point is critical because in the absence of legal rules, companies that are gathering this data will be free to use it for whatever purpose they wish – the data for a targeted ad today could become a detailed personal profile sold to a prospective employer or a government agency tomorrow.

The harm to consumers is not easy to measure. We know there are serious problems in the United States with identity theft[8] and security breaches,[9] but there

---

"United States v. Councilman," http://epic.org/privacy/councilman/ (last visited Apr. 22, 2009).

[6] *National Cable and Telecommunications Association v. Federal Communications Commission*, No. 07-1312, slip op. (D.C. Cir. Feb. 13, 2009).

[7] Brief for EPIC, Privacy and Consumer Organizations, Technical Experts, and Legal Scholars as Amicus Curiae, *National Cable and Telecommunications Association v. Federal Communications Commission*, 555 F.3d 996 (D.C. Cir. 2009) (No. 07-1312); *available at* http://epic.org/privacy/nctafcc/epic-ncta-050608.pdf.

[8] Federal Trade Commission, 2006 Identity Theft Survey Report, Nov. 2007, *available at* http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf (finding that nearly 4% of surveyed Americans were victimized by identity theft in the previous year, and that the resultant costs topped $15 billion).

[9] *See, e.g.*
In the Matter of The TJX Companies, Inc., FTC Docket No. 072-3055 (FTC 2008)

has not been enough work on the specific link between excessive data gathering and the enormous dangers that consumers face in the networked economy. Still, if the TJX case in Massachusetts provides any indication of the scope of the problem, it is clear that current data collection practices do place consumers at risk.[10] And there is every reason to anticipate that these problems will get worse as long as there is little protection for the data that is gathered.

Significantly also for the economics of the online advertising industry, the profiles that are being developed are increasingly untethered from the editorial content of web sites or the business-customer relations that online consumers have with particular companies. By this I mean that advertisers are learning far more about users than the sites that users actually visit or the businesses they actually interact with. This has profound implications for the future of online advertising and the relationship between users, web publishers, and advertising networks.

For example, Google recently announced that it would move to "Interest-based" advertising, which means that the web-based advertising model will be less dependent on the valuable content of web sites and more dependent simply on what Google know about users. [11] Google is not the only company to do this, and they have tried to create some privacy safeguards, though in my opinion they are not very effective. But the larger development is the increasing transfer from a customer-business relationship to the user profile-advertiser model. Apart from the privacy problems with this model, there are likely to be also substantial antitrust concerns

---

(Complaint), *available at* http://www.ftc.gov/os/caselist/0723055/080327complaint.pdf (data breach involving the improper disclosure of personal information concerning approximately 455,000 consumers, and resulting in tens of millions of dollars in claims for fraudulent credit card charges, as well as the cancellation and reissuance of millions of cards);
In the Matter of Reed Elsevier, Inc. and Seisint, Inc., FTC Docket No. 052-3094 (FTC 2008) (Complaint), *available at* http://www.ftc.gov/os/caselist/0523094/080327complaint.pdf (data breach leading to criminals acquisition of sensitive information about at least 316,000 consumers, and subsequent use to activate credit cards, open new accounts, and make fraudulent purchases.).

[10] U.S. Federal Trade Commission, *Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers' Data*, March 27, 2008, *available at* http://www.ftc.gov/opa/2008/03/datasec.shtm.

[11] Google, Making ads more interesting, Mar. 11, 2009, http://googleblog.blogspot.com/2009/03/making-ads-more-interesting.html (last visited Apr. 22, 2009).

and a real question as to whether this approach will sustain web publishers in the long-term.

EPIC attempted to address these issues in a complaint before the Federal Trade Commission in 2007 regarding the Google-Doubleclick merger. [12] I will not go into that topic this morning other than to say that as the Committee considers the privacy risks that arise from networked-based advertising models, I hope you will consider the full range of threats to consumers and also the long-term structure of this market.

Recent Developments

Last year, Members of this Committee drew attention to a new threat to users when it told an online advertising company, NebuAd, to back off a plan to partner with cable and telephone companies.[13] NebuAd was proposing to use "deep packet inspection" techniques to both profile users based on their Internet activity and to place targeted advertisements. The technology deployed by NebuAd, third-party tracking cookies, was hardly a new technique, but it was more invasive and it took advantage of the ISP's access to network traffic to develop user profiles.

Representative Markey and Representative Barton played a leading role in the effort to stop Charter, a large national cable company, from adopting the NebuAd targeting model. Eventually, the company backed off the plan. Members rightly charged that intercepting network communications ran afoul of the Wiretap Act. [14]

These new threats to online privacy are not limited to the United States. Because of the global nature of the networked economy, policy challenges that are

---

[12] *See* EPIC, Privacy? Proposed Google/DoubleClick Deal, http://epic.org/privacy/ftc/google/ (last visited Apr. 22, 2009).

[13] Letter from Re. Edward J. Markey and Rep. Joe Barton to Mr. Neil Smit (May 16,2008) ("We are writing with respect to recent media reports that Charter Communications has announced plans to begin collecting information about websites that subscribers visit and then disclsoing such data to a firm called NebuAd.") http://markey.house.gov/index.php?option=content&task=view&id=3401&Itemid=125

[14] The Wiretap Act provides for civil liability and criminal penalties against any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any … electronic communication [except pursuant to a statutory exception]." 18 U.S.C. § 2511(1)(a) (2009).

arising in the United States are also faced in many countries around the world. In the United Kingdom, the debate over deep packet inspection continues. A company called Phorm has pursued a business model similar to NebuAd. The UK Information Commissioner's Office, somewhat surprisingly, took the position that Phorm's monitoring of user activity did not violate user privacy as long as users had opted-in. That decision did not sit well with UK users, UK online companies, or the European Commission.

Earlier this month, European Commissioner Viviane Redding began legal proceedings against the UK government for violating EU law by allowing Phorm to go forward with its controversial Internet monitoring plan. Commissioner Redding has alleged violations of both the 1995 EU Directive concerning data protection[15] as well as the 2002 EU Directive concerning electronic communication.[16] If the Commission is successful in this challenge, which appears likely, the UK government will be required to change its privacy law so as to ensure that Phorm, and other companies engaged in similar practices, cannot continue to monitor the private activities of Internet users in the UK. In a statement, Commissioner Redding said, "Technologies like Internet behavioral advertising can be useful for businesses and consumers but they must be used in a way that complies with EU rules. These rules are there to protect the privacy of citizens and must be rigorously enforced by all member states."

Several UK firms, including Wikipedia and Amazon, have also announced that they do not want to be included in the Phorm advertising service.[17] While it is good to see these organizations take steps to protect privacy, the opt-out scheme currently in place in the UK is unworkable and will leave users without a clear indication of whether their network traffic is being monitored. That is the reason that a clear legal prohibition must be maintained.

---

[15] European Commission, "Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data," *available at* http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=Directive&an_doc=1995&nu_doc=46.

[16] European Commission, "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector," *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML.

[17] Wikimedia Technical Blog, "Wikimedia Foundation opting out of Phorm," (Apr. 16 2009), http://techblog.wikimedia.org/2009/04/wikimedia-opting-out-of-phorm/ (last visited Apr. 22, 2009); BBC, "Amazon blocks Phorm adverts scan," (Apr. 15, 2009), http://news.bbc.co.uk/2/hi/technology/7999635.stm.

Policy Analysis

Companies such as NebuAd and Phorm claim that their techniques protect privacy because they do not necessarily require the collection of personally identifiable information, a traditional trigger for the application of a privacy law. But this observation is not correct with respect to the privacy safeguards required for communication service providers. In the communications context, service providers and their businesses partners also have an obligation not to intercept the content of a communication except for the purpose of providing the service, to comply with a court order or other similar legal obligation. [18]

It is possible that the techniques being developed by these firms may help in some ways to safeguard privacy if they are robust, scalable and shown to provably prevent the identification of Internet users. But the essential problem is that they simply do not have the right to access communications traffic for this purpose. Also, I would not recommend that you alter current law or enable consent schemes to make this permissible.

First, companies have not demonstrated the viability of the non-PII model. It is simply too easy to reconstruct actual identity from network traffic. While we remain hopeful that advertising models based on non-personally identifiable information can be made, there are still too many instances where companies, particularly where there is no regulation, fail to fulfill their responsibilities.

Second, even if these privacy techniques are shown to be reliable, it will still be necessary to enact legislation to place the burden on the advertising company to prevent the reconstruction of user identity. Without this statutory obligation, there would be no practical consequence if a company inadvertently disclosed personal information or simply changed its business model to true user-based profiling. In fact, this is exactly what happened in the early days of online advertising when the company Doubleclick moved from an anonymous advertising model that was widely supported to a true user-based targeting scheme.

Third, the long-term consequences of encouraging network-based advertising will likely degrade network security and privacy. For example, it may become more difficult to adopt good network security standards, such as IPsec (Internet Protocol security), [19] if ISPs have a vested interest in access to their

---

[18] *See* 18 U.S.C. § 2511(1)(a) (2009); 18 U.S.C. § 2511(1)(c)-(d) (2009); 18 U.S.C. § 2511(3)(a) (2009).

[19] Wikipedia, IPsec, http://en.wikipedia.org/wiki/IPsec (last visited Apr. 22, 2009) (describing IPsec as "a suite of protocols for securing Internet Protocol (IP)

customers' network traffic for commercial benefit. Sealing the envelope will make it more difficult to inspect its contents.

There are technical measures that may allow some users to avoid the risks of deep packet inspection. For example, a Secure VPN uses cryptographic tunneling protocols to enable private communications over unsecure networks. There are both proprietary and open standards for Secure VPN. Significantly, the long-delayed Internet Protocol standard IPv6 would include IPsec as a standard.

Congress needs to keep a long-term view of the growth of the Internet. If the claims of Internet advertisers that they must have the unrestricted ability to monetize user traffic goes unchallenged, users will face new privacy risks, web publishers will find that their content is less valuable, and the technical standards that are necessary for the integrity of the Internet will be further delayed. Once down this road, it will be difficult to turn back.

Conclusion

From the user perspective, the threats to privacy online are increasing. Unregulated data collection continues. Privacy policies are opaque and ineffective. Users are unable to exercise any meaningful control over the personal information that is obtained by firms when they visit sites, purchase online, or participate in the rapidly growing world of social networking.

Some have simply given up and said that reduced privacy is the cost of new technology. But even that approach may not work. The Federal Trade Commission reports that identity theft and the related problem of security breaches continue to grow. To give up a privacy protection would allow identity theft and security breaches to escalate even further.

The Committee's oversight on the Deep Packet Inspection matter is commendable, but more needs to be done. There should be greater oversight of practices in the online advertising industry and a greater willingness to distinguish between sensible business practices and those that should not be permitted. Regarding many of these new challenges, I recommend in particular the work of the Center for Digital Democracy. Mr. Jeff Chester has brought attention to fundamental

---

communications by authenticating and encrypting each IP packet of a data stream. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.")

changes in online advertising that are generally not well understood by the American public and that pose a real threat to the open evolution of the Internet

We also look forward to the development of the FCC's National Broadband Plan. The Commission and the Acting Chair have identified privacy as a top concern in the development of this important initiative. We agree and believe that consumers across the country want the assurance that when they use new technology their personal information will be protected and they will not be profiled and tracked by secretive companies, hiding in the shadows of the Internet.

Thank you again for the opportunity to appear before the Committee today. I will be pleased to answer your question.

ADDITIONAL REFERENCES

EPIC, “NCTA v. FCC: Concerning Privacy of Customer Proprietary Network Information (CPNI))”(“ Federal Appeals Court Upholds Opt-In Privacy Rule for Telephone Services.” Feb. 13, 2009)
http://epic.org/privacy/nctafcc/

EPIC, “Deep Packet Inspection and Privacy”
http://epic.org/privacy/dpi/

EPIC, “FCC Approval of FBI Wiretap Standards Threaten Communications Privacy,” (Aug. 27, 1999)
http://www.epic.org/privacy/wiretap/calea/comments_12_98.html

EPIC Letter to FCC Chairman Martin, May 17, 2006 ("If telecommunication carriers disclosed customer information to the NSA in the manner described in press reports, then violations of section 222 of the Communications Act have occurred.")
http://www.epic.org/privacy/wiretap/epic-fcc-nsa.pdf

FCC, Report and Order and Further Notice of Proposed Rulemaking, Adopted: March 13, 2007 - Released April 2, 2007: "Our Order is directly responsive to the actions of data brokers, or pretexters, to obtain unauthorized access to CPNI. As the Electronic Privacy Information Center (EPIC) pointed out in its petition that led to this rulemaking proceeding, numerous websites advertise the sale of personal telephone records for a price. These data brokers have been able to obtain private and personal information, including what calls were made to and/or from a particular telephone number and the duration of such calls. In many cases, the data brokers claim to be able to provide this information within fairly quick time frames, ranging from a few hours to a few days. The additional privacy safeguards we adopt today will sharply limit pretexters’ ability to obtain unauthorized access to this type of personal customer information from carriers we regulate. We also adopt a Further Notice of Proposed Rulemaking seeking comment on what steps the Commission should take, if any, to secure further the privacy of customer information."
http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-22A1.doc