EPIC Comments on Privacy Issues in 6000_0_8 - ENUM Forum 11-01-02 Unified Document

The Electronic Privacy Information Center (EPIC), a not-for-profit Washington-based research center, submits the following comments to the ENUM Forum on the Unified Document (Contribution # 6000_0_8, November 14, 2002).

EPIC was created in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. In order to protect privacy, EPIC argues for the adoption of Fair Information Practices (FIPs), as interpreted by the Organization for Economic Cooperation and Development (OECD) in 1980. [1] Entities that collect personal information enjoy benefits but also assume responsibilities to safeguard data. FIPs are the most effective method of addressing the responsibilities that come with collection of personal information. [2] Additionally, to supplement FIPs, genuine privacy enhancing technologies (PETs) are necessary to enable anonymity, to securely protect personal information, and to limit the transfer of personal information where possible.

We commend the ENUM Forum for its openness and efforts to consult with privacy groups in the development of this new system. Our comments below summarize the risks that ENUM presents to enrollees, a possible legislative approach to addressing these risks, and specific recommendations to improve privacy protection for enrollees.

ENUM may make personal communication much more convenient. In doing so, however, it presents certain risks to privacy. The primary risk is secondary marketing or profiling use of personal information that is provided for enrollment or provided to populate an ENUM account. These risks are real and growing. In the case of e-mail, for instance, a commentator recently noted that unsolicited commercial messages are so numerous that they threaten to change the open nature of e-mail. As spam now constitutes 30% of all messages, users increasingly are adopting whitelist systems, making e-mail more like a closed system of communication than an open one. [3] Similarly, recent litigation surrounding unsolicited commercial fax messaging has demonstrated that junk faxing can result in economic harm and physical risk. [4] In the area of telemarketing, sales calling has become so frequent that two federal agencies are considering the adoption of national do-not-call lists. Individuals are also reporting increases in unsolicited commercial messages on their SMS or text-based services. [5]

ENUM, as a system that facilitates all of these types of communications, exposes individuals to heightened risk. As explained below in more detail, the ENUM Forum has approached this problem by asking enrollees to assume the risk of privacy violations. For instance, the July 2002 unified ENUM working document reads in part: "...[T]he ultimate form of privacy protection would be to opt-out and choose not to participate in ENUM...Simply put, an ENUM user chooses to load his or her telephone number into the ENUM Golden Tree."

This approach also ignores quality of consent. That is, ENUM may become necessary for participation in modern society. Additionally, many future ENUM users may be required to have an account as a result of corporate policy.

Law enforcement interest in ENUM records and transactional data has also not been addressed.

In the Post-PATRIOT ACT environment, it is safe to assume that law enforcement officers will attempt to collect ENUM enrollment and transactional data. We recommend that the ENUM Forum analyze the possible ways in which law enforcement may gain access to this data. Notice to ENUM enrollees should include an explanation of the legal standards that must be met before law enforcement may gain access to ENUM data.

Because of risks of secondary use of ENUM information, and to speed adoption of the ENUM system, we recommend that the ENUM Forum seek legislation to protect users of the ENUM system. Such legislation should contain the following elements:

- Use limitations that prevent personal information from being employed for unrelated, secondary purposes, such as profiling or spamming. The Fair Credit Reporting Act (FCRA) would serve as a model for this type of protection. [6] FCRA limits the disclosure of credit reports to a series of defined uses. Similarly, legislation for ENUM would prohibit secondary use of registration information or information stored in the NAPTR absent subscriber consent.
- Genuine consent provisions that allow the individual to choose whether or not to enroll, and choice over what data is included in the record.
- Notice of all information collection associated with ENUM, including the information stored in the registrant's account. ENUM service providers should minimize the amount of information collected from users.
- Access and a right to correct personal information collected in the enrollment process and stored in the ENUM database. The Cable Communications Policy Act (CCPA) contains model provisions that could be applied to ENUM. [7]
- Data destruction requirements that guarantee that service providers do not retain information unless it is necessary for operating the service. The Video Privacy Protection Act (VPPA) contains provisions for data destruction that could be incorporated in ENUM. [8]
- A right to withdraw from ENUM, and to have account and usage information expunged. If ENUM portability is fully achieved, the right to withdraw from ENUM becomes especially important.
- Protections against government or law enforcement acquisition of ENUM usage or account information without proper judicial oversight.
- Accountability provisions that give individuals genuine recourse against individuals who misuse their information. The Telephone Consumer Protection Act (TCPA), for instance, allows the FCC, state attorneys general, and individuals to bring actions for violations of the law. [9] A law to protect ENUM registrants would similarly allow these avenues for accountability.

Section 9.1 Registrant Choice with ENUM. *Choice, as an FIP, relates to secondary use of personal information. The ENUM Forum should rework the Registrant Choice section to reflect that individuals can choose to use ENUM without assuming the risk of secondary use of their personal information.*

The current ENUM Forum approach to privacy in regards to "choice" is flawed. Choice is a Fair Information Practice that recognizes that individuals should have some say over the use of their personal information, once they have enrolled in a service or purchased a product. The working group has confused the risks inherent in adopting a new technology with the choices that a person makes with regards to personal information once that technology is adopted.

This principle is more simply explained through examples of other technologies and "choice." If

an individual chooses to use a phone, that person does not assume the risk that the conversation will be intercepted and used by other persons. Rather, after choosing to use the phone, the individual must make another affirmative choice to allow interception of the communication. Choice does not relate to adopting a technology—it relates to the secondary use of personal information once a technology has been adopted.

We think that adoption of ENUM will be retarded by the absence of affirmative privacy protections, and an approach that requires users to assume new privacy risks. If we were to take the same approach with cable television, for instance, those who subscribed to cable would assume the risk that the cable operator was tracking viewing habits. Those who rented videocassettes would assume the risk of marketing use of their title rental information. Those who checked out books from the library would assume the risk of having the circulation records disclosed to third parties. In all of these scenarios, choice is treated differently than the approach that the ENUM Forum has currently taken. In each of these scenarios, individuals can enjoy the benefits of technology without having their personal information used for secondary marketing purposes.

The ENUM Forum should rework the Registrant Choice section to reflect that individuals can choose to use ENUM without assuming the risk of secondary use of their personal information.

Section 9.3 Open Disclosure of the Registrant's Information in the Public DNS.

We applaud the ENUM Forum for cautioning registrants against using URIs that would directly identify the account holder.

Section 9.4 ENUM Registration and Initial Provisioning.

The Registrar portion of this section suffers from the same weaknesses described in Section 9.1 above. Registrants cannot be assumed to have consented to all uses and disclosure of their personal information by merely enrolling in the system.

Section 9.5 Third Party Diagnostic Capability – ContactInfo.

We applaud the ENUM Forum for including privacy-enhancing policies with respect to ContactInfo services. It is important that if ContactInfo or WHOIS-like services are adopted that they not reveal personal information of ENUM registrants.

Section 9.6 Recommended Privacy Practices. *The ENUM Forum should recommend opt-in requirements before service providers use personal information for secondary purposes.*

We applaud the ENUM Forum for adopting a framework of FIPs.

We urge the ENUM Forum to specify that secondary use of registrant data receive opt-in consent protections rather than the "choice" provision currently in the unified working document. An opt-in framework would better protect individuals' rights, and is consistent with most United States privacy laws. For instance, the Family Educational Rights and Privacy Act, Cable Communications Policy Act, Electronic Communications Privacy Act, the Video Privacy Protection Act, the Driver's Privacy Protection Act, and the Children's Online Privacy Protection Act all empower the individual by specifying that affirmative consent is needed before information is shared. [10]

Further, public opinion clearly supports an opt-in system for information collection and sharing.

A study conducted by the American Society of Newspaper Editors (ASNE) and the First Amendment Center (FAC) in April 2001 illustrated strong support for privacy and specifically for opt-in systems. [11] In that study, the respondents indicated that personal privacy was an issue as important as crime, access to health care, and the future of the Social Security system.

In other information collection contexts, individuals regularly indicate that opt-in is preferable to opt-out. The ASNE/FAC study shows that 76% of individuals support opt-in as a standard for sharing of driver's license information. A study conducted by Forrester Research found that 90% of Internet users want the right to control how their personal information is used after it is collected. [12] A study conducted by the Pew Internet and American Life Project found that 86% of Internet users favor opt-in privacy policies. [13] And, a BusinessWeek/Harris poll found that 86% favored opt-in over opt-out. The same poll showed that if given a choice, 90% of Internet users would either always or sometimes opt out of information collection. [14]

Opt-in is more effective than opt-out because it encourages companies to explain the benefits of information sharing, and to eliminate barriers to exercising choice. Experience with opt-out has shown that companies tend to obfuscate the process of exercising choice, or that exemptions are created to make opt-out impossible. For instance, the Gramm-Leach-Bliley Act required opt-out notices to be sent to customers of banks, brokerage houses, and insurance companies. [15] These notices were confusing and in fact incomprehensible to many Americans. [16] Opting out often required the consumer to send a separate letter to the company. Even if a consumer did opt out under the law, a company that wished to share consumer data could simply create a joint marketing agreement with another company to fall within an exemption to the prohibition on information sharing. [17]

In other contexts, phone companies have thwarted opt-out processes by demanding excessive authentication for opting-out. For instance, the opt-out process for Customer Proprietary Network Information (CPNI) data sharing established by Verizon was confusing, and placed the burden on individuals to navigate a five-step process in order to opt-out. [18]

Section 9.7 Conclusion - Recommendations.

We recommend against a contractual approach alone to secure individuals' privacy rights. Academic scholarship has recognized that collective action problems, information asymmetry, and differences in bargaining power limit individuals' ability to protect their privacy through contract. [19] Additionally, we note that some of the participants in developing ENUM have not always been sensitive to privacy issues. [20] There is no reason to assume they will be sensitive to privacy issues with respect to ENUM.

Section 10.5 Data Elements For ENUM Registration. *The ENUM Forum should allow anonymous registration of ENUMs.*

It is foreseeable that individuals may wish to use an ENUM account without sharing any personal information. Anonymous speech is an important right protected by the Constitution. Individuals should be able to exercise the option to enroll in ENUM anonymously (provided that there is contact information for a technical administrator on the account).

---

[1] Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), at http://www1.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM.

[2] Marc Rotenberg, Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get), 2001 Stan. Tech. L. Rev. 1 (2001) at http://stlr.stanford.edu/STLR/Working_Papers/00_rotenberg_1/index.htm.

[3] Kevin Werbach, Death by Spam: The e-mail you know and love is about to vanish, Slate, Nov. 18, 2002, at http://slate.msn.com/?id=2074042.

[4] In the complaint, the Plaintiffs allege that a junk faxer "war dialed" a hospital, causing over 1,000 calls to be made to University of Washington Medical Center. *Lawsuits Seek $2.2 Trillion Over Junk Faxes*, New York Times, Aug. 22, 2002.

[5] *The New Frontier of Mobilespam*, Wired, Aug. 5, 2002.

[6] 15 U.S.C. § 1681.

[7] 47 U.S.C. § 551(d).

[8] 18 U.S.C. § 2710(e).

[9] 47 U.S.C. § 227.

[10] Respectively, at 20 U.S.C. § 1232 g, 47 U.S.C. § 551, 18 U.S.C. § 2510 et. seq., 18 U.S.C. § 2710, 18 U.S.C. § 2721, and 15 U.S.C. § 6501.

[11] Anders Gyllenhaal & Ken Paulson, *Freedom of Information in the Digital Age*, April 2001, at http://www.freedomforum.org/.

[12] *The Privacy Best Practice*, Forrester Research, Sept. 1999.

[13] Susannah Fox, *Trust and Privacy Online: Why Americans Want to Rewrite the Rules*, the Pew Internet & American Life Project, Aug. 20, 2000.

[14] *Business Week/Harris Poll: A Growing Threat*, BusinessWeek, Mar. 20, 2000, at http://www.businessweek.com:/2000/00_12/b3673010.htm.

[15] 15 U.S.C. § 6801.

[16] Mark Hochhauser, *Lost in the Fine Print: Readability of Financial Privacy Notices*, July 2001, at http://www.privacyrights.org/ar/GLB-Reading.htm.

[17] 15 U.S.C. § 6802 (b)(2).

[18] *See* Letter from Marc Rotenberg, Executive Director, Electronic Privacy Information Center, to Ivan Seidenberg, President and co-CEO, Verizon (Feb. 7, 2002), at http://www.epic.org/privacy/cpni/verizonletter.html.

[19] Shaun B. Spencer, Reasonable Expectations and the Erosion of Privacy, 39 San Diego L. Rev. 843 (Summer, 2002); Paul Schwartz & Ted Janger, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 Minn. L. Rev. 1219 (2002), at http://www.paulschwartz.net/minn-final.pdf; Arthur R. Miller, (1971).

[20] Verisign has sold DNS records to direct marketers. Thomas Weber, *Domain database sale--*

marketers delight, privacy nightmare?, Wall Street Journal, Feb. 15, 2001, at http://zdnet.com.com/2100-11-528257.html?legacy=zdnn. Verizon charges a monthly fee to individuals who wish to have a non-published number or unlisted number, the company has followed an opt-out model for CPNI affiliate sharing, and the company's CPNI notice is confusing and does not even mention privacy (http://www.epic.org/privacy/cpni/verizon_optout.jpg).

ENUM FORUM CONTRIBUTION:
Contribution #: SEC0056R0