Prepared Testimony and Statement for the Record of

Marc Rotenberg,
President, EPIC

Hearing on

"ICANN and the WHOIS Database: Providing Access to Protect Consumers from Phishing"

Before the

Subcommittee pm Financial Institutions and Consumer Credit.
Committee on Financial Services
United States House of Representatives

July 18, 2006
2128 Rayburn House Office Building
Washington, DC

I. Introduction

Chairman Bachus, Ranking Member Sanders, and Members of the Committee, thank you for the opportunity to testify today on the WHOIS database and the importance of privacy for the Internet. My name is Marc Rotenberg and I am President and Executive Director of the Electronic Privacy Information Center. EPIC is a non-profit research group founded in 1994 to promote privacy and to focus public attention on emerging civil liberties issues. I am also the former chairman of the Public Interest Registry, which manages the .ORG domain, the third-largest generic Top Level Domain.

EPIC has long been involved in the international discussion of WHOIS policy, as a member of the Non-Commercial Users Constituency within the Internet Corporation for Assigned Names and Numbers (ICANN). EPIC has participated in policymaking decisions with ICANN[1] and has contributed to legal and policy discussions of WHOIS through the publication of the *Privacy and Human Rights* reports[2] and in litigation, contributing an amicus brief detailing WHOIS practices across various country-code top level domains (ccTLDs).[3] Our web page on WHOIS privacy is top-ranked on the Internet.[4]

We very much appreciate the opportunity to appear before the Committee today and to discuss the importance of WHOIS privacy for the Internet. With identity theft the number one crime against consumers in the United States, there is understandable concern about the improper disclosure of personal information on the Internet. The WHOIS database performs a critical function by helping to ensure the security and stability of the Internet. But making the data in WHOIS available to anyone without any accountability creates real risks to the privacy and security of Internet users. We are grateful that the Committee has provided an opportunity to explore these issues in more detail.

II. The Importance of Privacy in WHOIS

To understand the WHOIS privacy issue, it is important to understand the purpose of WHOIS. Because of the distributed nature of the Internet, it is often important to be

---

[1] EPIC & Ruchika Agrawal, Privacy Issues Report: The Creation of A New Task Force is Necessary For an Adequate Resolution of the Privacy Issues Associated With WHOIS (2003), *available at* http://www.epic.org/privacy/whois/privacy_issues_report.pdf; Posting by Marc Rotenberg, Executive Director, EPIC, to mailto:whois-comments@icann.org (Feb. 13, 2006, 16:35:42 EST) (http://forum.icann.org/lists/whois-comments/msg00042.html); Marc Rotenberg, Executive Director, EPIC, to gnso-whoisprivacy-cmts@icann.org (Sep. 30, 2005, 17:08:10 EDT) (http://forum.icann.org/lists/gnso-whoisprivacy-cmts/msg00007.html).

[2] EPIC, PRIVACY AND HUMAN RIGHTS: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS 140 (2005).

[3] Brief *Amicus Curiae* of EPIC in Support of Appellant, *Peterson v. Nat. Telecomm.& Info. Admin.*, No. 06-1216 (4th Cir. Apr. 24, 2006).

[4] EPIC, "WHOIS," http://www.epic.org/privacy/whois/. According to Google for a search on "WHOIS privacy," Jul. 17, 2006.

able to locate a person who is responsible for managing a particular web site or a computer server that is attached to the network. Sometimes, there are technical problems that need to be identified and fixed so that the functionality of the network can be maintained. Other times, there are malicious attacks on computers that require system administrators to contact one another, identify the problem, and develop a solution. Administrators take advantage of the WHOIS directory to find other key technical people and help keep the network running.

ICANN, the non-profit, private-sector corporation that was created to determine technical policy for the Internet, formalized the process of collecting contact information for the WHOIS directory when it required that the "registrars," those are the companies that sell Internet domain names, to collect certain information from "registrants," the people who want to register an Internet domain. Any time that a user wants to register a domain name, she must provide her name, address, email address, and telephone and fax numbers, as well as the name, address, email address, phone and fax numbers of the technical and administrative contact persons. The critical question then becomes how much of this information should be made available to others and under what circumstances.

ICANN, currently requires that all of this information, be available to anyone with an Internet connection. This means that both the law enforcement agent with legal authority to investigate crime and a person with the intent to commit crime has the same access to the WHOIS database. This represents a significant privacy and security risk for a domain name registrant. As EPIC found in our comprehensive review of privacy practices around the world, the ICANN WHOIS data policy has "failed to resolve the privacy risks faced by Internet users that result directly from ICANN's own data practices."[5] Even the widely respected Internet Engineering Task Force acknowledged that there were problems with the growing use of the WHOIS database:

> For historic reasons, WHOIS lacks many of the protocol design attributes, for example internationalization and strong security, that would be expected from any recently-designed IETF protocol….WHOIS lacks mechanisms for access control, integrity, and confidentiality….The absence of such security mechanisms means this protocol would not normally be acceptable to the IETF at the time of this writing.[6]

The lack of security in WHOIS reflected the limited uses that its designers envisioned for it. WHOIS was originally intended to allow network operators to contact those responsible for the technical aspects of another domain, so that technical problems could be resolved.[7] This original purpose is still recognized by the Generic Names

---

[5] PRIVACY AND HUMAN RIGHTS, *supra*, at 143.

[6] Leslie Daigle, Internet Engineering Task Force, *WHOIS Protocol Specification* (2004), http://www.rfc-editor.org/rfc/rfc3912.txt.

[7] Statement of the Registry Constituency, Generic Names Supporting Organization, Preliminary Task Force Report on the Purpose of WHOIS and the WHOIS Contacts, Jan. 18, 2006, http://gnso.icann.org/issues/whois-privacy/prelim-tf-rpt-18jan06.htm.

Supporting Organization Council (GNSO), the policy-setting group within ICANN. The GNSO recently recommended that ICANN adopt a formulation for the purpose of WHOIS that maintains this central purpose:

> The purpose of the gTLD Whois service is to provide information sufficient to contact a responsible party for a particular gTLD domain name who can resolve, or reliably pass on data to a party who can resolve, issues related to the configuration of the records associated with the domain name within a DNS nameserver.[8]

This is an approach that is broadly favored by the registrars, Internet users, privacy experts, and the many government representatives who participate in the ICANN decision-making process. The formulation does not ban non-technical uses for WHOIS data. Instead, it reflects the primary purpose and routine uses for the database. In the smaller academic community in which the Internet first gained ground, there were fewer users and uses, and so fewer threats online. The large amount of contact information and ready access to it were built in to the WHOIS system without considering that the system could be used for a wide range of unanticipated purposes, and that there might be a need to protect the sensitive information in a WHOIS entry, or that there would be non-technical reasons (such as law enforcement) for someone to contact a domain name holder.

The formulation of the purpose of WHOIS therefore represents an attempt on ICANN's part to adjust the WHOIS system to reflect the current state of the Internet and the growing need for user privacy. As the Public Interest Registry, which operates the .ORG top-level domain stated:

> As the Internet and the number of its users has grown, the justification for making WHOIS data publicly available is no longer applicable. While business users may have little or no objection to publication of their contact information, individual users have an expectation of reasonable protection of rights of privacy. They are justifiably concerned that far more information is now publicly available than is necessary for any legitimate purpose.[9]

ICANN, in developing the current policy for WHOIS, is primarily concerned with ensuring that the database is accessible to network administrators and providing a reasonable amount of privacy protection for Internet users. But ICANN does not restrict law enforcement access to WHOIS data. At a recent meeting in Marrakech, Paul Twomey, the president and CEO of ICANN, clearly stated that the purpose of the

[8] Generic Names Supporting Organization Council, ICANN, "GNSO Council Motions 12 April 2006," http://gnso.icann.org/mailing-lists/archives/council/msg02393.html.
[9] Public Interest Registry, Policy Statement Regarding the WHOIS Service, Mar. 2, 2005, http://pir.org/PDFs/pdf00000.pdf.

WHOIS formulation is not to bar law enforcement access. Twomey said, "I cannot see a circumstance where law enforcement agencies will not have access to this information."[10]

Many groups involved in the debate over domain name policy agree on this approach. The Non-Commercial Users Constituency,[11] which represents a wide range of non-commercial domain name holders, highlighted this point in its comments on the WHOIS purpose formulation. After noting that WHOIS was not created with the intention of serving litigants or law enforcement, the group stated:

> Companies with allegations against domain name registrants can seek subpoenas of specific subscriber records through Internet service providers, or learn about a domain name registrant's identity information through requested subpoenas of registrar records.
> …
> Law enforcement agencies can subpoena specific subscriber records through Internet service providers, or learn about a domain name registrant's identity information through subpoenas of registrar records.[12]

The Public Interest Registry also indicated that the purposes of WHOIS are best served by limiting unrestricted and unaccountable access to the database, while still allowing for law enforcement access under appropriate circumstances:

> As a general rule, information available in response to public, anonymous inquiries (whether from registries or registrars) should be limited to domain names, the identity of the registrar and an email address to contact the registrar….[L]aw enforcement agencies with an appropriate legal basis for a request, e.g., a subpoena, should be able to have access to personal information when necessary for law enforcement purposes.[13]

Establishing clear privacy safeguards for the WHOIS database, as ICANN intends to do, is also necessary to reconcile the collection of personal information that ICANN requires for those who register Internet domains with the laws of many countries that explicitly protect the WHOIS data. Peter Schaar, chairman of the leading group of European privacy officials (the Article 29 Working party), recently wrote to the ICANN board of directors, pointing out that, under European privacy law,[14] any data collected and processed must be relevant and not excessive for the purpose for which it was

---

[10] Thomas O'Toole, *ICANN Official Says Government Worries About Loss of Whois Access Are Unfounded*, 11 BNA ELECTRONIC COMMERCE AND LAW REPORT 762, Jul. 12, 2006.
[11] EPIC is a member of the Non-Commercial Users Constituency.
[12] Non-Commercial Users Constituency, *NCUC constituency statement on Whois purpose*, Aug. 9, 2005, http://www.ncdnhc.org/policydocuments/ncuc-whois-purpose-9-Aug-05.pdf
[13] Public Interest Registry, Policy Statement Regarding the WHOIS Service, Mar. 2, 2005, http://pir.org/PDFs/pdf00000.pdf.
[14] Directive 1995/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31.

collected.[15] In the case of WHOIS, collecting and publishing all registrants' contact information and addresses far exceeds the disclosure necessary to resolve technical problems. Even law enforcement purposes can be easily served by a narrower disclosure.[16]

These proposals represent a sensible step towards protecting the sensitive information of domain name holders, protecting a reasonable expectation of privacy in personal information in everyday transactions.

B. Privacy Threats Raised by Unrestricted Disclosure of WHOIS Data

Protecting registrants' addresses, email addresses, and telephone numbers from inappropriate use is a real problem. The personal information available in the WHOIS database can be used for phishing, spamming, stalking, and the suppression of free speech. The problem of identity theft is particularly serious in the United States. According to the Federal Trade Commission, complaints about identity theft topped the list of consumer complaints last year, accounting for 255,000 of more than 686,000 complaints filed with the agency in 2005.[17]

This risk of identity theft combined with the lack of privacy for WHOIS data could affect millions. In the third quarter of 2005 alone, 8.5 million new domain names were registered, bringing the total number of domain names to a record-setting 86.5 million.[18] Registrants include not only large and small businesses, but also individuals, media organizations, non-profit groups, public interest organizations, support groups, and political and religious organizations.[19] ICANN currently requires all of these companies, organizations, and individuals to provide contact information for the WHOIS database. Understandably, there is growing concern about the possible misuse of the data.

Such a massive database of contact information is a treasure trove for spammers and phishers. In 2005, the most prolific spammer in the United Kingdom was found liable for harvesting email addresses from the WHOIS database to use in spam mailings that defrauded domain name holders into giving up financial information.[20] Armed with the personal information of Internet users the phisher was able to pose as a registrar, asking users to renew registrations for a fee. Other fraudsters may use the data to impersonate

---

[15] Letter of Peter Schaar, Chairman of the European Commission's Article 29 Working Group, to Vinton Cerf, Chairman of the Board of Directors, ICANN, Jun. 22, 2006, *available at* http://www.icann.org/correspondence/schaar-to-cerf-22jun06.pdf

[16] Schaar's letter continues by describing a layered approach that would be more proportionate, where "details of the person are known to the ISP that can, in case of problems related to the site, contact the individual or transmit the information to an enforcement authority entitled by law to access this information." *Id.*

[17] Federal Trade Commission, "FTC Releases Top 10 Consumer Fraud Complaint Categories: Identity Theft Again Leads the List," (Jan. 25. 2006), http://www.ftc.gov/opa/2006/01/topten.htm.

[18] VeriSign Domain Name Industry Brief, "The VeriSign Domain Report," November 2005, http://www.verisign.com/static/036316.pdf.

[19] *See* PRIVACY AND HUMAN RIGHTS, *supra*, at 140.

[20] Dinah Greek, *Weasel out of this one*, COMPUTERACTIVE, Feb. 11, 2005, *available at* http://www.vnunet.com/computeractive/news/2012383/weasel.

the domain name registrant to other entities, such as phone companies, retailers, or even financial institutions, gaining access to even more sensitive information.

Even more sinister threats are easy to envision. Individual domain name registrants may have no address to provide other than their home address, and no phone number other than their home or mobile phones. The ready availability of this information on WHOIS puts at risk for stalking or other criminal activity anyone who chooses to register her own domain name. In some situations, a person who would register an Internet web site and provide a useful service to others may choose not to simply because of the lack of privacy safeguards.

Protecting free speech on the Internet also requires protecting the privacy of WHOIS data. A user speaking from his own website, or sending an email from his own domain, currently must surrender his right to speak anonymously. An anonymous speaker in this country, for instance, might find his residence or his telephone numbers subject to harassment for voicing unpopular opinions. In other countries, Internet dissidents face the persecution of oppressive regimes.[21] Someone expressing opinions counter to those of the government may be refused space on local commercial hosts, or may suspect that those hosts would turn his contact information over to authorities.[22]

Already governments are trying to crackdown on human rights groups by extending identification requirements for Internet users.[23] Requiring that a dissident publish his Internet contact information for ready access by government threatens democratic reforms in several countries.[24] The United States should not be on the wrong side of this important twenty-first century human rights issue by opposing privacy safeguards for the WHOIS database.

C. Current Methods Used to Protect Privacy

---

[21] *See generally* REPORTERS WITHOUT BORDERS, *2006 Annual Report on Internet Freedom*, http://www.rsf.org/rubrique.php3?id_rubrique=578 (detailing the arrests, imprisonment, harassment, or torture of Internet speakers in several countries around the world).

[22] Xiao Qiang, *Yahoo helped sentence another cyber dissident up to 8 years - Liu Xiaobo*, CHINA DIGITAL TIMES, Feb. 8, 2006, http://chinadigitaltimes.net/2006/02/yahoo_helped_sentence_another_cyber_dissident_to_8_year_1.php; Hiawatha Bray, *US to Protest Censorship of Internet by Beijing*, BOSTON GLOBE, Feb. 15, 2006 at F1 (noting Yahoo's complicity in identifying two Chinese Internet dissidents); BBC NEWS, *Yahoo "helped jail China writer"*, Sep. 7, 2005, *at* http://news.bbc.co.uk/2/hi/asia-pacific/4221538.stm; Richard Spencer, *Microsoft pulls plug on China protest blog*, THE DAILY TELEGRAPH, Jan. 6, 2005, at 18.

[23] Maria Sanminiatelli, *Italian Law Hits Cybercafes*, SAN JOSE MERCURY-NEWS, Dec. 12, 2005, at 4E; REPORTERS WITHOUT BORDERS, *2006 Annual Report on Internet Freedom* (noting identification requirements or special permissions required in Bahrain, Cuba, Syria, and Turkmenistan).

[24] REPORTERS WITHOUT BORDERS, *2006 Annual Report on Internet Freedom* (harassment and censorship of opposition websites in Belarus; arrest of a blogger in Egypt; censorship and arrests of bloggers in Iran; censorship and arrests in Lybia; government intimidation of journalists and bloggers in Malaysia; imprisonment and torture of Internet users in Syria; silencing of critical websites in Thailand; censorship and jailing of dissidents in Tunisia; jailing of dissidents in Vietnam).

Since ICANN makes that the WHOIS data available without any legal process to protect personal information from improper use, domain name registrants have understandably taken steps to protect their personal privacy and security. One such method is simply to enter inaccurate information. This is not surprising. Women, for instance, have often provided just an initial, rather than a complete first name, in the phonebook to protect privacy. Similarly, legitimate Internet users, knowing that others may obtain their address and phone number, will simply enter false data into the system. Here, we can see how the lack of privacy protection undermines the desire for accuracy.

Other users take advantage of a proxy service, either offered by a registrar or a third party, that helps shield the identity of the registrant. These services provide their own contact information for the WHOIS database, passing along any contact or communications to the registrant. In this way, the original purpose of the WHOIS database can be achieved, since messages sent to resolve any problems with the website will still reach the registrant, while preventing the registrant's personal information from being improperly disclosed.

Unfortunately, some registries, such as the United States' country code top-level domain, .US, forbid the use of proxy registration. Such policies further expose registrants under these domains to risk of harm and encourage inaccurate data entry, though fortunately they appear to be the exception to the rule.[25] Still, we believe the current policy of the Department of Commerce for .US is poorly conceived and should be revised.

III. A Model for a Sensible, Effective WHOIS Service

Both of the methods currently available for registrants to protect their data, however, are incomplete solutions. For one, users should not be required to lie to protect their privacy. Furthermore, some users may be unable to afford a proxy registration service, or the service may be banned in their countries. Also, as the Public Interest Registry has pointed out, the Registrar Accreditation Agreement requires proxy providers will be liable for users' actions.[26] Because of this, many users may not be able to use proxy services, if their views are too controversial for proxy providers. This may be a particular problem in countries that do not protect fundamental human rights.

A sensible privacy solution would simply remove the most sensitive data from being viewed by any member of the public. Such solutions have been proposed by registries,[27] registrars,[28] non-commercial users,[29] and others.[30] These proposals would

[25] Brief *Amicus Curiae* of EPIC, *Peterson v. Nat. Telecomm. & Info. Admin.*, No. 06-1216 (4th Cir. Apr. 24, 2006).
[26] Comments of the Public Interest Registry on the Final Report on WHOIS Accuracy and Bulk Access, WHOIS Task Force, Generic Names Supporting Organization, Feb. 17, 2003, http://pir.org/PDFs/pdf00000.pdf
[27] Public Interest Registry, Policy Statement Regarding the WHOIS Service, Mar. 2, 2005, http://pir.org/PDFs/pdf00000.pdf.
[28] Paul Stahura et al. Proposal to Increase Whois Utility and Relevancy: The Operation Point of Contact, Nov. 22, 2005, *available at*

allow the WHOIS database to comply with Fair Information Practices, which require that individuals know, when they disclose personal information about themselves, how that data will be used and who will be able to view it.

Currently, those accessing the Whois database lack these safeguards. This type of disclosure not only violates principles of good information practice and data security, it potentially runs afoul of international laws such as the European data protection directive. As Chairman Schaar pointed out in his letter, the widespread availability of WHOIS data is not proportionate to the problems the database is meant to solve.

An important distinction can also be drawn between corporate domain name holders and individuals. As with telephone listings, the motivations behind publicizing commercial, or private, contact information differ. As a business that holds itself out to the public and must be accountable for its business dealings, a corporation can reasonably be expected to publish contact information at which it can be reached for questions, complaints, and service of process. Individuals, however, will often use their domains as they would a personal means of communication—such as a cell phone, the number to which they have no public duty to disclose.

But a comprehensive approach to WHOIS cannot rely solely on the distinction between commercial and non-commercial registrants. There should be some point of contact for all who register an Internet site, and there should be clear safeguards to protect personal information from improper disclosure. Under a proposal now being pursued by ICANN – the oPOC or "Operational Point of Contact" – domain name registrants will still provide their name, address, phone, and email contact information when they register, but personal privacy will be protected, since only the operational contact's information will be published.[31]

Large businesses could certainly list themselves, while smaller organizations and individuals would probably list their registrar or ISP – the organizations best equipped to respond to technical problems. Under this arrangement, there would be no change in the collection of registrant data; Individuals and businesses who register Internet sites would still be required to provide contact information that will be accessible to law enforcement and others, subject to due process safeguards.

---

http://code.byte.org/_attachments/1426464/Proposal%20to%20Implement%20oPOC%20-%2011282005.pdf

[29] Non-Commercial Users Constituency, *NCUC constituency statement on Whois purpose*, Aug. 9, 2005, http://www.ncdnhc.org/policydocuments/ncuc-whois-purpose-9-Aug-05.pdf

[30] Letter of Peter Schaar, Chairman of the European Commission's Article 29 Working Group, to Vinton Cerf, Chairman of the Board of Directors, ICANN, Jun. 22, 2006, *available at* http://www.icann.org/correspondence/schaar-to-cerf-22jun06.pdf

[31] "Proposal to Increase Whois Utility and Relevancy: The Operational Point of Contact, Rationalizing the gTLD Whois System and Specific Contact Records,"http://www.dnspolicy.org:4080/index.php?n=Main.OperationalPointOfContact; *original available at* http://code.byte.org/_attachments/1426464/Proposal%20to%20Implement%20oPOC%20-%2011282005.pdf.

An effective model for WHOIS privacy would therefore take into account the limited amount of information necessary to accomplish the technical goals of the database; recognize that law enforcement needs for data should not require widespread disclosure of personal information; and provide a process for releasing, in certain well-defined circumstances, data that is not routinely made available.

That is the approach that ICANN is now pursuing. It is backed by the key stakeholders and the user community. It is a sensible and effective solution that should be supported.

IV. Privacy is Compatible with, and Enhances Accuracy and Accountability

As many have recognized, there are legitimate uses for WHOIS data. If a network administrator notices problems with a connection to another network, for example, he can use the WHOIS information to contact someone at the other network who will be able to resolve the problem. The WHOIS database is a useful tool for network administrators to resolve problems with interconnected networks.

The need for accurate WHOIS information, though, does not mean that privacy must be sacrificed: there is a limited amount of information that needs to be made available, and there are limited classes of people who need access to that information. In most cases, the persons using WHOIS need only a reliable method of contacting the responsible party. That contact information does not need to include all, or even any, of the personal information about the domain name registrant, and it does not even need to be personally identifiable. A registrar or third party proxy can easily pass on communications to the domain name holder without revealing private information to the Internet at large.[32] Where direct contact is necessary, an email address or Post Office Box can suffice. Most of all, though, none of this information needs to be publicly available to anyone on the Internet. Restricting access to network administrators achieves the goals of WHOIS while helping protect the privacy of registrants. The types of information needed and the types of people who need it can be and should be itemized and limited.

In fact, limiting the information made available and the people who can access it promotes the accuracy and therefore the usefulness of the information. One reason users provide false WHOIS information is that they know it will be publicly available for spammers, stalkers, and anyone else on the Internet who wants it. If users know that their information will only be made available to people who actually need it, and that those people will only be getting the information they need, this incentive to provide false information evaporates. The need for accuracy and truthfulness is what underlies the importance we place in doctor-patient confidentiality or attorney-client privilege. When information is protected by medical confidentiality, attorney-client privilege, shield laws, or tighter WHOIS privacy policies, people place themselves at less risk when giving out personal information and are more likely to provide accurate information.

[32] Carl Bialik, *New Services Are Making It Easier to Hide Who Is Behind Web Sites*, Wall Street Journal, Sept. 30, 2004, at A1.

V. Unrestricted Access to WHOIS is an Ineffective Approach to the Phishing Problem

Phishing involves three steps: setting up a web site to collect information, getting people to go to the site (usually via spam), and collecting the information. A phisher sets up a web site generally by copying the design of a login page for a bank or other trusted web site. This page is then set up on a free or fraudulently obtained web site, a hacked web site, or a hacked personal computer. Once it is operational, the phisher sends out emails that appear to be official notices asking users to visit the site and enter their financial information. When the information is submitted, the phisher stores it and uses it to commit fraud or theft. In some cases, phishers have even set up the site to check the validity of the information and prompt the user if it is not correct.[33]

There are many victims of this kind of fraud in addition to the person whose financial information is used. A computer is hacked to host the web site, or someone else's financial information is used to fraudulently pay for hosting, and hacked computers are often used to send out the spam messages luring users to the site. Because of this setup, the identity of the actual phisher, who is often even outside of the United States, is hidden. Instead, only the hosting and spamming computers are known.

Once a hosting web site has been identified, WHOIS may be useful in shutting the site down. Because the phishing sites are usually short-lived, the spam announcements generally refer to them by IP address rather than domain name, so the WHOIS IP database is used to find the administrator for the network. That is, WHOIS is used as a technical means of finding the person who controls the hosting computer's network access. In many cases, the WHOIS database of domain name registrants is not even used.

However, in finding the perpetrator himself, the WHOIS database may be less useful. Since the computers used to send the spam or host the fraudulent website are often hacked, or the domain names registered under stolen account information, the results of a simple WHOIS search will not lead law enforcement to the fraudster.

In fact, open access to the WHOIS database may contribute to phishing and spam. Phishers and spammers must build a list of email addresses to which they can send their messages, and the WHOIS database contains an email address for the owner of every domain name. Spammers can "harvest" this database to quickly build a list of recipient addresses. Because spam's success depends on the miniscule cost of sending each message, bulk "harvesting" of email addresses from WHOIS can be hindered by even a moderately successful method of limiting access to domain registrants' information to people who have legitimate needs for it. In addition, as described above, users will be more willing to give accurate contact information when they know it will not be used by spammers and phishers.

---

[33] Brian Krebs, *Citibank Phish Spoofs 2-Factor Authentication*, Jul. 10, 2006, http://blog.washingtonpost.com/securityfix/2006/07/citibank_phish_spoofs_2factor_1.html (last visited July 14, 2006).

VI. Conclusion

The public availability of WHOIS information has resulted in harassment and criminal acts, some of which the Committee today is working to prevent. Rather than mandating more disclosure of this information, though, the Committee should both protect domain name holders' privacy and increase the usefulness of information in the WHOIS database by limiting access. When registrants feel that their personal information will remain safe and will only be used for legitimate purposes, they will be more willing to provide accurate information. As long as the personal information is published and available for anyone on the Internet, including spammers, stalkers, hackers, and phishers, registrants will be hesitant to give correct information. A private, accurate database is no less useful for resolving technical problems and for legal investigations than the current database, but it would protect the privacy of millions of domain name holders.

ICANN has made significant progress addressing the twin concerns of online fraud and privacy protection. The WHOIS proposal currently under consideration will still permit law enforcement access to WHOIS data under appropriate circumstances, but will limit the possibility that personal information will be improperly disclosed to spammers, phishers, stalkers, and governments intent on stopping democratic reform.

We appreciate the Committee's interest in this important issue and hope that Members agree that privacy protection remains a central concern for Internet users and the future of Internet-based services.