Competitive Enterprise Institute

Issue Analysis

Cybersecurity and Authentication

The Marketplace Role in Rethinking Anonymity—Before Regulators Intervene

by Clyde Wayne Crews Jr.

November 8, 2004

Advancing Liberty From the Economy to Ecology

2004 No. 2

Cybersecurity and Authentication

The Marketplace Role in Rethinking Anonymity— Before Regulators Intervene

by Clyde Wayne Crews Jr.

Executive Summary

Anonymous speech plays a fundamental role in America's political history. However, that long tradition of anonymous communications faces an image problem in today's age of spam, computer viruses, spyware, denial-of-service attacks on websites, and identity theft. The criminals and hackers who perpetrate these insults on the commercial Internet are, for the most part, anonymous; we simply don't know the identities of these bad guys. Yet the promise of anonymous communications is vital to the preservation of political liberty across the globe. So, how should we regard anonymity in a digital age? And how should we strike the right balance between security and anonymity online?

To begin, we should *not* consider the outlawing of anonymous communications as the answer to today's cybersecurity threats. Commercial sector "regulation" of anonymity, so to speak, can play a significant role in combating these problems. Increasingly, online authentication has become important to both personal security and to cybersecurity in general. Some recent proposals toward bolstering security have included greater authentication of the source of emails to deal with spam, and the requirement that those who conduct transactions online reveal their identities—seeming violations of online culture. Policymakers also want a say in the matter, and as the process unfolds, they might feel increasingly tempted to intervene whenever issues impacting privacy and authentication emerge in debates over telecommunications, intellectual property, biometrics, cybersecurity and more. Regardless, government should not strip us of our anonymity online. Cybersecurity concerns may instead call for the marketplace—not regulators— to deal with the fact that many threats stem from that very lack of authentication. The inclusion of greater authentication standards into online services by private vendors will lead to their working in concert in unprecedented ways that may draw attention from regulatory and antitrust authorities. But these private, experimental efforts have no implications for political liberty—nor are they anticompetitive. Private solutions are the only real hope we have for decreasing cybersecurity threats, given that previous government efforts to regulate the Internet—for example, outlawing spam in 2004—have not lived up to expectations. Political anonymity and commercial anonymity are not the same thing, and the distinction requires better appreciation. Over the coming tumultuous period of dealing with online threats, policymakers should allow the experimentation necessary to cope with today's lack of online authentication to proceed with minimal interference.

Introduction: From Playground to "War Zone"

Viruses, spam, hacks, distributed denial-of-service (DDoS) attacks designed to shut down websites, "phishing" attacks that trick individuals into providing personal data on fraudulent websites, various forms of identity theft, and even potential acts of cyberterrorism, are routinely in the news. If the marketplace fails to solve these mounting cybersecurity problems, the government will undoubtedly intervene. Recent months have brought congressional and Federal Trade Commission hearings and calls for legislation. The marketplace and the public now face key questions in this struggle over the nature of the "online experience."

We have long marveled at how the Internet has allowed us to seek out and contact whomever we want. However, others can do the same, of course, even if we'd prefer otherwise. Brown University's Vice President for Computing and Information Ellen Waite-Franzen lamented that the Internet has "been this nice electronic playground, but you can't help starting to wonder if maybe all this connection is not so great… Now it feels like a war zone."[1]

Although the Internet offers incalculable benefits, it also magnifies security risks inherent in the act of linking corporate networks and personal computers to a shared environment. Viruses, self-propagating worms such as August 2003's "Blaster" and January 2004's MyDoom, and DDoS attacks that grind victimized websites to a halt by overloading them with information requests, now cost billions in lost data and productivity. In January 2004, Trend Micro Inc., a provider of network antivirus and Internet content security software and services, pegged 2003's global costs to business of computer viruses at $55 billion, and predicted that online security problems will worsen.[2]

Who Are The Bad Guys?

We generally don't know *who* is responsible for invasions like spam and cyber attacks, and have few ways of finding out given the Internet's underlying architecture. While a daunting task, the business sector must get its act together to solve these problems, or Washington regulators will step in—regardless of whether they can actually solve the problems we face.

One prominent attack—the January 2003 attacks by the "Sapphire" worm—slowed not only much of the Internet, but also airline ticketing operations and Bank of America ATM networks (ATM networks send encrypted data across the Internet). The experts had no real answers, bemoaning the virtual impossibility of finding the perpetrator: An analyst at online security company iDefense Inc., said, "being able to track down the specific source of this is very unlikely."[3] Similarly, a spokesman for the FBI likened the possibility of searching for the attacker to "kind of like looking at a body of water and determining where a drop of water came from."[4] Even the 2003 arrest of a Minnesota teen allegedly responsible for releasing a modified version of the "Blaster" worm might not help reveal the identity of that worm's original authors.

Official Washington adds little to our confidence. Offenders easily cover their digital trail on the Internet. A May 2002 Joint Economic Committee report spotlighted the "anonymous environment" of the Internet and its implications for security, noting the difficulty of apprehending perpetrators of crimes on a global, anonymous Internet.[5] The January 2003 *National Strategy to Secure Cyberspace* also noted the extreme difficulty of tracing an attack's source.[6] Law enforcement has great difficulty tracing the authors of DDoS attacks, despite the ease with which people execute them.[7] If tracking the culprits is impossible, it is also unclear what their capabilities actually are or how to stop the increasingly aggressive attacks. The late-January 2004 MyDoom attack alone cost hundreds of millions of dollars, and caught security firms flat-footed and unsure what to do as the attack's "time release" nature became clear. At the height of the attack, a Thursday, January 29 Reuters story reported on sleep-deprived security experts who were powerless to halt the virus's coordinated attacks, timed to hit Web sites of SCO Group, Inc. on Sunday and then Microsoft on Tuesday.[8]

It is clear that there are some parties who don't make good company in cyberspace. Spammers and virus writers increasingly work together. Meanwhile, hackers create easy-to-use programs or tools to exploit weaknesses and post them on the Internet at the rate of 30 or 40 monthly, making it simple for even novices to mount an attack.[9] The Internet's global nature makes the problem difficult to solve even if we could stop U.S.-based offenders. As Bill Hancock of the non-profit Internet Security Alliance told Congress, many viruses:[10]

> are written with Russian, Chinese and other languages in comments in their code. Some have direct ties to organized crime, especially outside the U.S. Many are propagated from commonly known havens for virus writers where there is no fear of legal prosecution or where the technical skills of the government to prosecute are minimal or non-existent.

Commercial Anonymity vs. Political Anonymity

A commercial, information-based society that depends upon secure online commerce and communications cannot maintain the current state of affairs. Markets must grapple with the possibility that anonymity, in many respects, is not compatible with commerce. Along with better self-protection on the part of computer users—an essential component of cybersecurity—hackers and other miscreants must be prevented from doing their work anonymously. Depending upon the success of other cybersecurity measures, transactions or accounts that are not fully traceable back to an owner may have had their day on the Internet. Endless anonymous security breaches, invasions of privacy, and interruptions of commerce are an unnecessary vulnerability, largely an artifact of the Net's original design, which embodied a built-in trust of the other guy. Lessening online anonymity might make it more difficult (but not impossible) to spread havoc online. However, any pursuit of such a solution that goes beyond application-specific authentication to encompass Internet architecture will inevitably raise fundamental questions about privacy, free speech, and civil liberties in the Internet realm. We face a debate over the principles that undergird the "online experience" itself.

Ongoing developments with implications for anonymity include efforts by governments and oversight bodies to affect changes in underlying Internet routing and control architecture. Their investigations seek to address issues such as the impending shortage of Internet addresses as multitudes of new linkable devices join the network. The newest incarnation of the Internet Protocol (IP version 6), will replace earlier versions, pioneered by the Defense Advanced Research Projects Agency in the 1970s, long before the Internet's usage became widespread. IP version 6 has sparked controversy, however, because it may undermine anonymity by requiring validation for those conducting business online.[11] Unlike the existing protocols by which ISPs assign a different IP address when users go online, IPv6 would include an expanded address that would incorporate a unique serial number for each device's network-connection hardware. Each routed packet of data would carry "electronic fingerprints," a costly plan requiring widespread, coordinated adoption of new Net "plumbing standards"—an idea that might, in the end, not sit well with users concerned about online privacy.[12]

Outlawing Anonymity Not the Answer for Cybersecurity

Such negotiations are not the only source of concern about potential loss of online anonymity. An early draft of the Bush administration's cyberspace security plan raised the alarming idea of limiting the capability for anonymous communications on the Internet: "Allowing completely anonymous communications on a wide-scale basis, with no possibility of determining the source, could shelter criminal, or even terrorist communications."[13] But a move toward deliberately ending anonymous communication, *coming from lawmakers*, would strike an unnecessary blow at the very foundations of the Internet revolution, not to mention fundamental civil liberties.

Politically, citizens have the right to legitimate, peaceful, anonymous communication. Anonymity occupies a place of honor in our political history—Thomas Paine's *Common Sense* was signed by "An Englishman," and gentlemen calling themselves "Publius" authored *The Federalist Papers*.[14] Today, encryption, which allows the transmission of scrambled material across the Internet, represents an important embodiment of the tradition of speaking freely and of keeping one's private matters private. Legislatively undermining anonymity online effectively abolishes the capability for legitimate political criticism and civil disobedience in the new online medium.

Government ought not undermine or ban anonymity online, whether by interfering with anonymous email or encryption technologies, forcing a particular kind of authenticating technology on the Internet, or other such measure. Maintaining citizens' protections against unreasonable monitoring by the authorities remains crucial; technology and the post-September 11 law enforcement environment potentially makes government surveillance of citizens easier, which could suppress legitimate political speech. In response to a claim by Harvard law professor Alan Dershowitz that no citizens' right to anonymity is "hinted at in the Constitution," Cato Institute scholar Robert Levy noted: "That turns the Constitution on its head. The Ninth Amendment tells us we have an untold number of rights that are not enumerated in the Constitution. The question is not whether we have a right to anonymity, but whether government has the power to take it away."[15]

Indeed, anonymity and pseudononymity are "cornerstones of free speech," consistently held by the Supreme Court as protected by the First Amendment.[16] Particularly in an era in which the Internet can facilitate anonymous speech, and in which businesses continue to develop tools whereby individuals can shop or communicate anonymously, any push to abolish anonymity legislatively is cause for alarm. Although the post-September 11 environment has given rise to calls for national IDs, data mining, and surveillance, Congress should reject federal attempts to undermine anonymity. Curiously enough, given government's proclamations in support of cybersecurity, efforts to restrain anonymity (and in turn, the security anonymity affords) represent contradictory rejections of the government's own proclaimed commitment to privacy and security. That is, sometimes lost in the debate over anonymous communications is the fact that private communication is *itself* one manifestation of cybersecurity. While the Constitution might not guarantee the "right" to anonymity in one's public actions, citizens have the right to legitimate, peaceful communication using their own property and resources—including their computers. The hurdle should be one for government to surmount, not citizens. Indeed, an ethic whereby governments restrict the liberty of criminals and enemies, not that of innocent citizens, would go a long way toward advancing effective cybersecurity policy.

Constant changes in technology do pose challenges to law enforcement, forcing enhancement of surveillance capabilities. Nonetheless, while surveillance can and likely will be enhanced to account for the new realities of instant electronic communications, the Fourth Amendment's protections against unreasonable and warrantless searches need not suffer. Indeed, proliferation of forced identification facilitated by any government-mandated online authentication undermines self-maintained privacy and security, and runs counter to broader cybersecurity goals. Unless engaging in fraud or harming others, maintaining anonymity is legitimate.

Entrepreneurs engaged in facilitating online commerce have struggled for years to enhance privacy for individuals through anonymizing technologies. Washington presumably supports the principle behind such efforts on some level; most notably, legislators have introduced bills during recent congressional sessions to protect online privacy—and, as noted, anonymity is one manifestation of privacy. Marketplace offerings have included anonymity-enabling encrypted services like Hushmail and Freenet, which might record one's identity as a registered user, yet not be able to read one's emails or discern which websites one visited. Yet even here, if government needed to perform a search, it could conceivably do so through appropriate channels by obtaining a court order and installing a "key logger" program on the suspect's computer to intercept communications. Even in the Internet era, government can carry out law enforcement without violating rights and preemptively subverting anonymity and privacy for the innocent.

Private Sector "Regulation" of Anonymity Can Be Critical

So, we have a dilemma. Government shouldn't outlaw anonymity—yet anonymity can lie at the root of cybersecurity problems in the world of commerce. Anonymity is both vital and baneful. While we want to identify the individual (or individuals) who launch malicious viral attacks or unleash spam, we also want to maintain our own privacy and anonymity in legitimate online transactions. The private sector must act to accomplish and reconcile seemingly contradictory ends, as government intervention can complicate matters.

In the post-September 11 world, regulators may fret that anonymizing technologies—like Hushmail or Freenet—might inappropriately cloak the actions of certain clients. The technologies do, however, allow legitimate consumers to feel more secure about their transactions. Unfortunately, some of those very services thought to cloak (legitimately) one's identity turn out to have the occasional unexpected exploitable hole or vulnerability. For example, vulnerabilities uncovered in the dominant Sendmail email transfer application could potentially have allowed intruders to exploit certain vulnerable servers and launch a denial-of-service attack.[17] Freenet, the anonymous communications project, has shown vulnerabilities, as did Napster in its heyday. Even ordinary caching of Web pages by a browser has raised a potential problem uncovered by Princeton researcher Edward W. Felten, in that the possibility existed for outsiders to "probe" someone's browser cache to see if it holds a particular file. If the cache did contain the file, that would indicate that the person has visited a particular Web page, even if that individual surfed the Web using a tool like Anonymizer or SafeWeb.[18] The flaw did not appear to allow reading of the contents of the cache, merely snooping to see if particular pages were there—which is nonetheless alarming and unexpected. And the surge in peer-to-peer file sharing, using technologies such as BitTorrent, raises significant issues since file-sharers often expect anonymity when they do not actually have it,[19] or they expose themselves to viruses.

Software vulnerabilities are often unexpected, but the frequency of their exploitation by cloaked perpetrators makes clear that the Internet wasn't originally designed as the mass commercial and consumer communications medium that it is today. Those who exploit unexpected vulnerabilities often have the technological know-how to remain undetectable, while those who legitimately rely on the Internet's presumed anonymity are exploited. It is reasonable to assume that if industry set out to design a commercial network today from the bottom up, using Internet-style technology, but also knowing what we know now about the prevalence of unmannerly behavior by those who can remain undetectable, greater authentication capabilities would have been built in. For example, industry might have initially imposed stricter authentication standards on senders of email, ISP subscribers, and peer-to-peer file sharers, and others. As industry works toward such authentication today—a tall order—government should neither promote nor restrain the evolution.

Wall Street Journal technology columnist Walter S. Mossberg captured some of the popular sentiment regarding the downside of an anonymous Internet in an indignant moment: “Isn’t it finally time for America Online, Microsoft Network, EarthLink and other Internet service providers to re-examine the juvenile practice of allowing customers to hide behind multiple ‘screen names,’ instead of requiring them to conduct themselves online using their identities or email addresses that correspond with their real names? We don’t go around wearing masks in the real world. There, we are responsible—by name—for what we do and say.”[20]

It is not government’s place to interfere with services that continue to offer to us the possibility of anonymity, of course. However, the private sector may well legitimately restrict anonymity on private networks if that’s what overarching goals like network security, “canning spam,” and securing digital copyrights require. If the anonymous Internet commons and the state of its technology are part of the cybersecurity problems we face, rethinking online anonymity may help eliminate some of the “market failures” that otherwise provide rationales for government regulation. Some Internet law experts hold that “code is law,” and that control of Internet architecture affects online freedoms.[21] But the Internet’s roots as an open network are an artifact of governmental defense priorities; it might have evolved quite differently otherwise.[22] Now that the private, commercial sector dominates the Internet, government must continue to allow our anonymity to the extent providers want to offer it to us; it ought not dictate how communications networks evolve. But the private sector, increasingly vulnerable to cyber-vandals, isn’t obligated to provide or support the technology for iron-clad anonymity.

In the cyber-insecure environment in which we operate, mainstream businesses like banks, online merchants, and travel sites have started calling for authentication, hoping to set themselves and their emails to customers apart from the overwhelming torrent of spam. Demands for “caller ID” for the Internet have come from sellers, whose bulk—but wanted—commercial emails encounter impenetrable spam filters, and therefore do not reach the intended recipient.[23] Major hurdles remain. Indeed, spammers, ever opportunistic, now can employ “invisible bulletproof hosting,” as a Polish firm advertising the shady service calls it. The “service” protects the spam-website operator from anti-spam techniques by hiding or “laundering” the spammer’s true website on some unsuspecting computer user’s hacked machine.[24] The arms race continues, with spammers and virus writers now joining forces to make life miserable for others.

As the growing downside of wide-open connectivity becomes ever more apparent, some moves among major service providers—unsurprisingly—would entail drastically limiting online anonymity, and, in turn, the ability to hide one’s online actions or cover tracks. It would appear that the providers hope that those who fail to authenticate themselves may find their online operations increasingly constrained. For example, Novell’s chief technologist told *The Economist*, “I’m kind of a fan of eliminating anonymity if that is the price for security.”[25] In describing the impetus toward greater security, VeriSign CEO Stratton Sclavos said, “It’s not going to be all right not to know who’s on the other end of the wire.”[26] In one high-profile move, the Microsoft Network ended its anonymous worldwide chat room services in September 2003, reporting that they were a haven for spammers and sexual predators. Geoff Sutton, European general manager of Microsoft MSN, put it bluntly: “The straightforward truth of the matter is free, unmoderated chat isn’t safe.”[27] Versions of the service in the U.S., Canada, and Japan will survive, operating on a subscription-only basis, with substantial personal information on users required as condition of participation. Such moves by major vendors may become more common.

Problems like spam and security breaches ultimately require technological and market fixes rather than legislative ones. The Internet’s governmental origins have left property rights somewhat ill-defined in many online contexts, leading to a general crisis over “who rules?” that goes beyond cybersecurity.[28] A torrent of regulation and legislation would create vast problems and ignite legal wars. But as for private “governance” of what goes on online, it may be that today’s communications system, whereby participants and originators of messages can routinely remain anonymous, will prove inappropriate for the commercial society of tomorrow. Cybersecurity, like commerce itself, sometimes calls for greater authentication—the opposite of anonymity. We all at times need to identify ourselves, and validate the identity of others. In the cyber-environment, with the deluge of spam and viruses and the apparent inability of legislation to stop them, such authentication will likely increase in importance, with the possibility that commercial anonymity may often yield. There are many possible approaches: Along with “caller ID” for sending email or other authentication techniques for transacting online, new ID technologies such as digital certificates or signatures, as well as biometric techniques such as face or hand scanners, may increasingly govern access to critical facilities and networks by rendering them inaccessible all except to authorized personnel. One might increasingly expect future ease-of-movement and access to services online to reflect the extent to which one is willing to prove one’s identity. Shoplifters might still walk into tomorrow’s brick and mortar stores, but online authentication might mean they are kept out of the virtual one. In this respect, computer networks could become increasingly secure.

While government must not outlaw anonymous communications, the restriction of anonymity by online applications and networks may increasingly emerge to cope with the many hazards that plague the Net today. Administrators large and small may prefer recognizable participants, to know who uploads and downloads information or files on a company’s network or a peer-to-peer network.[29] For example, the peer-to-peer networks that thrive in the future may be those that authenticate users and file-sharers (and perhaps the legality of the files they trade), as opposed to the freewheeling ones of today that are bloated with viruses and unwanted files and spyware. Extending such security to Internet architecture itself is a thornier problem; while people might agree to moderated chat rooms, they might not tolerate a “moderated surf.” The precise ways in which society will cope with widespread demands for authentication, and the reduction in anonymity these methods might require, is by no means apparent. But the Internet is a network of largely private networks. And administrators of those components may legitimately limit anonymity of those who partake of their services. In fact, if cybersecurity problems continue to escalate, commercial society may gravitate toward those networks without anonymity rather than anonymous, unfettered ones. Yet the potential loss of commercial anonymity does not mean that government snooping becomes more acceptable.

Regardless of how the Internet evolves, political anonymity, privacy safeguards and Fourth Amendment protections must be preserved.

Cybersecurity Better Served By Private Alliances

A commercial Internet, in some respects, may become increasingly less anonymous, but the direction of its evolution is a question the marketplace and society ought to settle rather than legislators. If matters gravitate in the direction of more authentication and less anonymity, government ought not to prohibit it—for example, thorough antitrust intervention that prohibits agreements among online vendors such as ISPs and software makers. Consolidation or agreements among ISPs could lead to changes in user agreements—such as a requirement for a legitimate name and mailing address—or the adoption of new technological standards that would presumably render the Internet architecture more insulated from cyber attacks.

A key element of enhancing cybersecurity is that alliances might go beyond the mere sharing of information about threats to encompass agreements about new technologies to embed in computers, services, and infrastructure. Parties to such agreements might design them to cope merely with security issues, but signatories might also generate commercial or product market impacts that could attract unwarranted scrutiny from antitrust enforcers. Microsoft's Next Generation Computing Base initiative, for example, is an evolving content control and digital certificate system that would involve working with other major players like Intel. Such initiatives involve no "anticompetitive" motives, but occasionally future partnerships could involve shutting out or "refusing to deal" with certain vendors or customers (e.g., "collusion" with regard to the use of particular software firewalls or other technologies and specifications). For example, one proposal recommends the filtering of viruses at the ISP level, as opposed to the end-user model of today, and for ISPs to share information they uncover about attacks.[30] Such an action would conceivably entail collective action that might make software makers, who feel their downloads may be unfair tagged as potentially viral, nervous. Alternatively, groups of ISPs may determine it's worthwhile to reject customers who fail to purchase and maintain anti-virus and other security software. Or ISPs could decide to promote their own software.[31] Complaints could surface over such collective action, but policymakers should resist the urge to intervene, and allow alliances for purposes of security without fear of antitrust or competitive scrutiny. Inevitably, cooperation will mean some software and other vendors will not be winners, and antitrust complaints are likely. But antitrust law should not upend refusals to do business with certain players; contractual agreements among major players could constitute a critical element of tomorrow's more secure cyber-infrastructure.

Collective marketplace action is not new, of course. ISPs have long blocked known spammers listed in directories such as the Mail Abuse Prevention System's "Realtime Blackhole List."[32] Blacklisting can lead to problems, such as the inadvertent blockage of non-spammers, but remains a legitimate exercise of market-based, rather than regulatory, problem solving. Some bulk mailers regard blacklisting as vigilante behavior, and disputes often arise. ISPs may overreach at times; but at least the blacklist process is subject to market pressures and discipline. Poorly conceived legislation, or unwarranted interference, could prove more difficult to work around.

In coping with the spam deluge, ISPs have experimented with giving users a less polluted inbox by such means as limiting the number of outgoing messages per subscriber account. Indeed, companies may offer tiered pricing for email and bandwidth, since today's flat fees aren't a fact of nature or a natural right. Some envision a future in which ISPs are no longer all trusting, and inadvertently complicit in the spread of viruses and spam, and may require that anyone sending an email will need a unique identifier, a "license" of sorts.[33] Such identifiers or "seals" for trusted commercial e-mail could help tomorrow's ISPs block unwanted e-mail, but they would require major reworking of Internet protocols, and unprecedented industry coordination. As noted, to set up such wide-scale systems, ISPs and technology providers would likely need to "collude" in novel ways; for example, one recently formed consortium including America Online, Microsoft, and Yahoo explored the idea of certified email. Ultimately, some tout email "postage" or protocols that allow users or ISPs to charge fractions of a cent for receiving unsolicited email as ways of ending spam once and for all.[34] Entrepreneurs have already created bonded sender programs, anticipating such a sea change. But, again, such major reforms would require vast improvements in authentication to work properly.

Another example of a joint effort is an international industry coalition of telecommunications firms, software makers, and ISPs that has developed a "Neighborhood Watch" program seeking to eradicate spam though information sharing, cooperation, and technical changes at the network level rather than standard filtering.[35] Like other campaigns, their aim is to prevent "spoofing" and hiding behind fake email headers via a caller ID technique for email. One could compare such major overhauls of the Net architecture to widening all the nation's roads six inches; it would constitute a monumental undertaking. But if lack of authentication is at the root of scourges like viruses and spam, legislation and regulation do not directly address the problems. Indeed, the federal anti-spam law that became effective in January 2004 has had no discernable effect. For such reasons, the cooperation among service providers and other vendors we have seen—and will surely see more of—is necessary. While it will generate controversies and invite hearings and scrutiny from Congress and antitrust enforcers, legislators should leave the marketplace free to address cybersecurity issues. The very real costs imposed by cybersecurity vulnerabilities outweigh any imagined antitrust ramifications.

Conclusion

Of course, technologies to create and secure networks exist now—and they do not always require the latest advances like biometrics. User vigilance—such as learning how to practice good security and locking down servers to withstand attacks—remain important to cybersecurity. While authentication may represent the ultimate in cybersecurity, it will still make many nervous; some view such changes as fundamentally threatening the openness and anonymity of the Internet. However, if private network operators and other vendors increasingly require authentication, it has no implications for *political* liberty and is within the rights of network owners. People still retain the right to use any legal means to protect their anonymity, and can always resort to those online services and networks that continue to provide it. The task we face—that of protecting political anonymity while also protecting the ability to experiment with authentication technologies—simply requires that the government leave the Internet alone.

Notes

[1] Amy Harmon, "Digital Vandalism Spurs a Call for Oversight," *New York Times*, September 1, 2003. p. A1.

[2] Jennifer Tan, "Firm Says 2003 Viruses Caused $55B Damage," *Washingtonpost.com*, January 16, 2004, Available from Tecrime Website, http://www.tecrime.com/llartV10.htm.

[3] Ted Bridis, "FBI Skeptical on Internet Attack Source," Associated Press, January 29, 2003. Available from Information Security News Website, http://seclists.org/lists/isn/2003/Jan/0154.html. See also Katie Hafner and John Biggs, "In Net Attacks, Defining the Right to Know," *New York Times*, January 30, 2003. p. G1. http://www.nytimes.com/2003/01/30/technology/circuits/30secu.html..

[4] Quoted in Robert O'Harrow Jr. and Ariana Eunjung Cha, "Internet Worm Unearths New Holes," *Washington Post*, January 29, 2003, p. A1.

[5] *Security in the Information Age: New Challenges, New Strategies*, United States Congress, Joint Economic Committee, May 2002. p. 63. http://www.house.gov/jec/security.pdf.

[6] "Revised Cybersecurity Plan Issued," Associated Press, January 7, 2003. http://www.wired.com/news/conflict/0,2100,57109,00.html.

[7] For example, see Louis Trager, "Multiple Agencies Expected to Investigate Internet Attack," *Washington Internet Daily*, October 24, 2002, p. 1.

[8] "MyDoom Worm Spreads as Attack Countdown Begins," *CNN.com*. January 29, 2004. http://www.cnn.com/2004/TECH/internet/01/29/mydoom.future.reut/index.html. Quoted in the story was Paul Wood, chief information analyst for British-based e-mail security firm MessageLabs: "It's very difficult for anti-virus firms to react in these scenarios. We're always going to be on the back foot,"

[9] Noted in *Effective Patch Management is Critical to Mitigating Software Vulnerabilities* (GAO-03-1138T), Statement of Robert F. Dacey, Director, Information Security Issues, United States General Accounting Office, Before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, House Committee on Government Reform, September 10, 2003. http://www.iwar.org.uk/comsec/resources/worm-virus-defense/GAO-final-testimony.pdf.

[10] Testimony of Dr. Bill Hancock, Chief Executive Officer, Internet Security Alliance, "Computer Viruses: The Disease, the Detection, and the Prescription for Protection," Subcommittee on Telecommunications and the Internet, Committee on Energy and Commerce. November 6, 2003. http://energycommerce.house.gov/108/Hearings/11062003hearing1124/Hancock1786print.htm.

[11] For one overview see Alex Salkever, "Needed: A Security Blanket for the Net," *BusinessWeek Online*, September 16, 2003. http://www.businessweek.com/technology/content/sep2003/tc20030916_6815_tc129.htm.

[12] "Stop Signs On the Web," *The Economist*, January 11, 2001. Available at http://www.economist.com/printedition/displayStory.cfm?Story_ID=471742.

[13] Quoted in Declan McCullagh, "White House Preps Cybersecurity Plan," *CNET News.com*, September 16, 2002. http://news.com.com/2102-1023-958159.html.

[14] Jonathan D. Wallace, "Nameless In Cyberspace: Anonymity on the Internet," *Cato Institute Briefing Paper No. 54*, December 8, 1999. http://www.cato.org/pubs/briefs/bp54.pdf.

[15] Robert A. Levy, "The ID Idea," National Review Online, October 24, 2001. www.nationalreview.com/comment/comment-levy102401.shtml.

[16] Wallace, 1999. pp. 2-3. http://www.cato.org/pubs/briefs/bp-054es.html. Wallace cites *McIntyre v. Ohio Campaign Commission*, 514 U.S. 334, 115 S.Ct. 1511 (1995), noting that "the Court invalidated an Ohio ordinance requiring the authors of campaign leaflets to identify themselves." Also, in 2002, the Court struck down an ordinance requiring Jehovah's Witnesses and other door-to-door canvassers to carry written

identification permits. *Watchtower Bible and Tract Society of New York, Inc. v. Village of Stratton*, 122 S.Ct. 2080 (2002).

[17] See Robert Lemos, "Sendmail Flaw Tests Homeland Security," *CNET News.com*, March 3, 2003. http://news.com.com/2102-1009-990879.html, as well as "Second Major Vulnerability Discovered in Sendmail this Month," *Internetweek.com*. March 31, 2003. http://www.internetweek.com/security02/showArticle.jhtml?articleID=8100186.

[18] Ian Austen, "Study Finds That Caching By Browsers Creates a Threat to Surfers' Privacy," *New York Times*, December 14, 2000. http://www.nytimes.com/2000/12/14/technology/14PRIV.html.

[19] Seth Schiesel, "File Sharing's New Face," *New York Times*, February 12, 2004. http://tech2.nytimes.com/mem/technology/techreview.html?res=9805E2DE133AF931A25751C0A9629C8B63.

[20] Walter S. Mossberg, "In Wake of Terrorism, It's Time for the Internet to Face the Real World," *Wall Street Journal*, October 4, 2001. p. B1.

[21] For example, see Lawrence Lessig, *Code and Other Laws of Cyberspace*, Basic Books: New York. June 2000.

[22] See Bruce M. Owen and Gregory L. Rosston, "Local Broadband Access: Primum Non Nocere or Primum Processi? A Property Rights Approach" (paper prepared for Progress and Freedom Foundation conference on Net Neutrality, June 27, 2003), p. 22, http://siepr.stanford.edu/papers/pdf/02-37.pdf.

[23] See Saul Hansell, "Anti-Spam Focus Shifts to Legitimate Mail; System Would Be Like Caller ID for the Inbox," *SFGate.com*, October 7, 2003. http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2003/10/07/BUGSQ26H7I1.DTL&type=printable.

[24] Brian McWilliams, "Cloaking Device Made for Spammers," *Wired News*, October 9, 2003, http://www.wired.com/news/business/0,1367,60747,00.html.

[25] Ibid, *The Economist*, November 27, 2003.

[26] Quoted in Steven Levy, "A Net of Control," *MSNBC News*. http://msnbc.msn.com/id/3606168.

[27] "Microsoft to Shut Down Chat Rooms," Reuters, September 23, 2003. http://www.wired.com/news/culture/0,1284,60567,00.html.

[28] See Adam Thierer and Clyde Wayne Crews Jr., *Who Rules the Net? Internet Governance and Jurisdiction*, Cato Institute: Washington, D.C. 2003.

[29] See Steve Peacock, "Bill to Hold Chief Information Officers Accountable for Security Seen," *Washington Internet Daily*, October 30, 2002. p. 2.

[30] Larry Seltzer, "Put Antivirus Protection Where it Belongs—On the ISP," *eWeek Enterprise News and Reviews*, July 25, 2003. http://www.eweek.com/article2/0,1759,1490782,00.asp.

[31] Noted in Salkever, "Needed: A Security Blanket for the Net," September 16, 2003.

[32] See http://www.mail-abuse.com.

[33] Michelle Finley, "Other Ways to Fry Spam," *Wired News*, April 24, 2000. http://www.wired.com/news/print/0,1294,35776,00.html.

[34] In January 2004, Bill Gates embraced the long-standing idea. Jonathan Krim, "Gates Wants to Give Email Users Anti-Spam Weapons," *Washington Post*, January 28, 2004. p. E1. http://www.detnews.com/2004/technology/0401/28/technology-47750.htm.

[35] Stefanie Olsen, "Telecoms, ISPs partner in spam fight," *CNET News.com*, January 13, 2003. http://news.com.com/2100-1024_3-5140556.html.

About The Author

Wayne Crews is Vice President for Policy and Director of Technology Studies at the Competitive Enterprise Institute. His work includes regulatory reform, antitrust and competition policy, safety and environmental issues, and various information-age concerns such as e-commerce, privacy, "spam," broadband, and intellectual property. He is the author of the annual report, *Ten Thousand Commandments: An Annual Snapshot of the Federal Regulatory State*.

Wayne has published in outlets such as the *Wall Street Journal, Chicago Tribune*, *Forbes, Atlanta Journal-Constitution*, *Communications Lawyer*, and the *Electricity Journal*. He has made various TV appearances on Fox, CNN, ABC and others, and his regulatory reform ideas have been featured prominently in such publications as the *Washington Post*, *Forbes* and *Investor's Business Daily*. He is frequently invited to speak, and has testified before several congressional committees.

Wayne is co-editor of the books *Who Rules the Net: Internet Governance and Jurisdiction* (2003) and *Copy Fights: The Future of Intellectual Property In the Information Age* (2002). He is co-author of *What's Yours Is Mine: Open Access and the Rise of Infrastructure Socialism* (2003), and a contributing author to others.

$8.00

The Competitive Enterprise Institute is a non-profit public policy organization dedicated to the principles of free enterprise and limited government. We believe that consumers are best helped not by government regulation but by being allowed to make their own choices in a free marketplace. Since its founding in 1984, CEI has grown into an influential Washington institution.

We are nationally recognized as a leading voice on a broad range of regulatory issues ranging from environmental laws to antitrust policy to regulatory risk. CEI is not a traditional "think tank." We frequently produce groundbreaking research on regulatory issues, but our work does not stop there. It is not enough to simply identify and articulate solutions to public policy problems; it is also necessary to defend and promote those solutions. For that reason, we are actively engaged in many phases of the public policy debate.

We reach out to the public and the media to ensure that our ideas are heard, work with policymakers to ensure that they are implemented and, when necessary, take our arguments to court to ensure the law is upheld. This "full service approach" to public policy makes us an effective and powerful force for economic freedom.

CEI
Competitive
Enterprise
Institute

1001 Connecticut Avenue, NW
Suite 1250
Washington, DC 20036
202-331-1010
Fax 202-331-0640
www.cei.org

Issue Analysis is a series of policy studies published by the Competitive Enterprise Institute. Nothing in *Issue Analysis* should be construed as necessarily reflecting the views of CEI or as an attempt to aid or hinder the passage of any bill before Congress. Contact CEI for reprint permission. Additional copies of *Issue Analysis* may be purchased through CEI's publications department (pubs@cei.org or 202-331-1010).