



2003

## Digital Architecture as Crime Control

Neal K. Katyal


*Georgetown University Law Center, [katyaln@law.georgetown.edu](mailto:katyaln@law.georgetown.edu)*

This paper can be downloaded free of charge from:  
<https://scholarship.law.georgetown.edu/facpub/1885>  
<https://ssrn.com/abstract=356460>

---

112 Yale L.J. 2261 (2002-2003)

This open-access article is brought to you by the Georgetown Law Library. Posted with permission of the author.  
Follow this and additional works at: <https://scholarship.law.georgetown.edu/facpub>

 Part of the [Computer Law Commons](#), [Criminal Law Commons](#), [Internet Law Commons](#), and the [Other Architecture Commons](#)

# Essays

## Digital Architecture as Crime Control

Neal Kumar Katyal<sup>†</sup>

The first generation of cyberlaw was about *what* regulates cyberspace. Led by Larry Lessig's path-breaking scholarship isolating architecture as a constraint on behavior online,<sup>1</sup> a wide body of work has flourished. In a recent article, I took those insights and reverse-engineered them to show how attention to architecture in realspace (such as our city streets, parks, houses, and other buildings) constrains crime.<sup>2</sup> It is time to begin a new generation of work, one that applies the lessons of realspace study back to the cybernetic realm. The question will not be *what* regulates cyberspace, but *how* to do so given the panoply of architectural, legal, economic, and social constraints.

This Essay details how theories of realspace architecture inform the regulation of one aspect of cyberspace, computer crime. Computer crime causes enormous damage to the United States economy, with even a single virus causing damage in the billions of dollars and with a recent survey finding that ninety percent of corporations detected computer security breaches.<sup>3</sup> Yet despite apparent metaphorical synergy, architects in realspace generally have not talked to those in cyberspace, and vice versa. There is little analysis of digital architecture and its relationship to crime, and the realspace architectural literature on crime prevention is often far too

---

<sup>†</sup> Professor of Law, Georgetown University Law Center.

1. See LAWRENCE LESSIG, CODE 4-14 (1999).

2. Neal Kumar Katyal, *Architecture as Crime Control*, 111 YALE L.J. 1039 (2002).

3. See Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1004 & n.1 (2001) (discussing the "ILOVEYOU" computer worm, which caused approximately \$11 billion in damage); Press Release, Computer Security Institute, Cyber Crime Bleeds U.S. Corporations, Survey Shows (Apr. 7, 2002), at <http://www.gocsi.com/press/20020407.html> (reporting results of an annual survey conducted with the Federal Bureau of Investigation).

"soft" to garner significant readership among computer engineers. However, the architectural methods used to solve crime problems offline can serve as a template to solve them online. This will become increasingly obvious as the divide between realspace and cyberspace erodes. With wireless networking, omnipresent cameras, and ubiquitous access to data, these two realms are heading toward merger. Architectural concepts offer a vantage point from which to view this coming collision.

This brief Essay sketches out design solutions to the problem of security in cyberspace. It begins by introducing four principles of realspace crime prevention through architecture. Offline, design can (1) create opportunities for natural surveillance, meaning visibility and susceptibility to monitoring by residents, neighbors, and bystanders; (2) instill a sense of territoriality so that residents develop proprietary attitudes and outsiders feel deterred from entering private space; (3) build communities; and (4) protect targets of crime.<sup>4</sup>

After introducing these concepts, the Essay discusses analogues to each principle in cyberspace. Naturally, the online and offline realms are not symmetric, but the animating rationales for the four principles can be translated to cyberspace. Some of the outlined modifications to digital architecture are major and will invariably provoke technical and legal concerns; others are more minor and can be implemented quickly to control computer crime. For example, we will see how natural surveillance principles suggest new virtues of open source platforms, such as Linux, and how territoriality outlines a strong case for moving away from digital anonymity toward pseudonymity. The goal of building communities will similarly expose some new advantages for the original, and now eroding, end-to-end architecture of the Internet—a design choice that eschewed barriers between computers and rejected preferences for certain types of content. Principles of community and target protection will illuminate why installing firewalls (which are simply pieces of hardware and software that prevent specified communications<sup>5</sup>) at end points will provide strong protection, why some computer programs subtly cue criminal acts, and why the government should keep some computer crimes secret.

Throughout this Essay, each Section will employ the realspace architect's understanding of *context* to explain why many meta-claims in contemporary cyberlaw are too grand. These claims are proliferating and track the same binary formula: "open sources are more/less secure," "digital anonymity should be encouraged/prohibited," "end-to-end networks are

---

4. Katyal, *supra* note 2, at 1048-71.

5. WILLIAM R. CHESWICK & STEVEN M. BELLOVIN, FIREWALLS AND INTERNET SECURITY: REPELLING THE WILY HACKER 85-118 (1994).

more/less efficient,” “peer-to-peer technologies are a threat/blessing,” etc.<sup>6</sup> Systematic predictions are possible about the benefits of open sources, end-to-end (e2e) networks, and the like, but caution is warranted before applying these predictions across the board. Such caution is a staple of crime prevention in realspace, as the four design principles are often in tension with each other. As this Essay progresses, these tensions will become evident in the cyberspace context as well.

In total, these architectural lessons will help us chart an alternative course to the federal government’s tepid approach to computer crime. In February of this year, after a year and a half of promising a revolutionary approach, the White House released its *National Strategy To Secure Cyberspace*.<sup>7</sup> Unfortunately, the Strategy consists of little beyond an unbridled faith in “the market itself” to prevent cybercrime.<sup>8</sup> By leaving the bulk of crime prevention to market forces, the government will encourage private barricades to develop—the equivalent of digital gated communities—with terrible consequences for the Net in general and interconnectivity in particular. Just as safety on the street depends in part on public police and public architecture, so, too, in cyberspace.

## I. DIGITAL DESIGN PRINCIPLES TO PREVENT CRIME

Today, the damage caused by computer crime runs in the billions of dollars each year, making it one of the most economically damaging forms of crime in human history.<sup>9</sup> Yet the extent of cybercrime today is still constrained by the costs of computers, bandwidth, and attaining computing skill, all of which are likely to diminish over time. As a result of these and other factors, we will soon face the possibility that the Net will become as unsafe as the downtown city street. The city-street analogy is worth thinking about, for some downtown streets effectively control crime. In any number of cities today, people simply avoid the streets at night altogether, making it difficult for them to be attacked. In others, lights or barricades make it more difficult to perpetrate crime. And in still others, police patrols provide a backdrop of safety that scares criminals away and encourages

---

6. See, e.g., *infra* text accompanying notes 14-16, 20, 31-32, 35 (discussing such claims in the context of open sources and anonymity). Compare LAWRENCE LESSIG, *THE FUTURE OF IDEAS* 35-37, 173 (2001) (discussing the benefits of end-to-end (e2e)), with Gerald Faulhaber, Comments at The Policy Implications of End-to-End Workshop (Dec. 1, 2000), at <http://lawschool.stanford.edu/e2e/papers/Fal.pdf>. Faulhaber, then-Chief Economist of the Federal Communications Commission, discussed how e2e “may well be violated for reasons of lower cost and/or higher value to customers.” *Id.*

7. See WHITE HOUSE, *THE NATIONAL STRATEGY TO SECURE CYBERSPACE* (2003), at [http://www.whitehouse.gov/pcipb/cyberspace\\_strategy.pdf](http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf).

8. *Id.* at 15.

9. Katyal, *supra* note 3, at 1003, 1004, 1013-14.

residents to come out of doors. What do these methods of control suggest about cyberspace?

This Part applies four principles of design and crime prevention to explain how changes to digital code can have a dramatic effect on crime rates. In order to ease consideration of these changes, I will be speaking generically about "crime," rather than singling out its particular variants, such as viruses, worms, denial of service attacks, unauthorized access, unauthorized use, and identity theft.<sup>10</sup> This simplification at times will obscure specific architectural solutions, yet the Essay's design is meant to underscore how, in both realspace and cyberspace, architectural changes have the potential to minimize a large number of crimes at once.

### A. *Natural Surveillance*

Natural surveillance refers to the use of architecture to create spaces that are easily viewed by residents, neighbors, and bystanders. The most sophisticated proponent of this approach was Jane Jacobs, who reasoned that "eyes on the street" would control crime.<sup>11</sup> Using Greenwich Village as a model, Jacobs argued that if people could be brought out onto city streets and if the design of city blocks facilitated visibility, the crime rate would drop. Jacobs did not disaggregate types of crime; rather, she felt that much of it could be prevented best by ordinary people, not professional police officers and security guards.<sup>12</sup> Yet a natural, and sometimes self-defeating, impulse is to close space off to prevent crime, rather than to open it up. The gated community is one such modern manifestation.<sup>13</sup>

In cyberspace, however, crime prevention is predominantly a less visible, professional enterprise. Much software today is "closed source," meaning that the programs' underlying computer code is hidden from its users. Just as closure in realspace can increase crime rates, so, too, in cyberspace. Because the underlying code is examined only by professionals

---

10. For a description of the variety of computer crimes, see *id.* at 1013-37 (discussing the types of computer crime in detail). The goal of this Essay is to outline a general framework for computer security that can be used to prevent a large number of types of computer crime; accordingly, some types of crime will not be amenable to this generalized discussion. And some of these activities may be criminalized for no good reason; I am taking as given that society wants to enforce the variety of laws against computer crime and asking how digital architecture can accomplish this efficiently and without doing harm to the Net.

11. JANE JACOBS, *THE DEATH AND LIFE OF GREAT AMERICAN CITIES* 6-40 (1961). For example, contrary to the conventional wisdom, she would argue that a house near a bar is less likely to suffer crime than a house in a remote location. See *id.* at 37.

12. See *id.* at 31-32 ("[T]he public peace—the sidewalk and street peace—of cities is not kept primarily by the police, necessary as police are. It is kept primarily by an intricate, almost unconscious, network of voluntary controls and standards among the people themselves, and enforced by the people themselves.").

13. Studies show, incidentally, that gated communities often do not reduce crime rates, and may even increase them. See Katyal, *supra* note 2, at 1085 & n.172.

(and often only by the firm developing the software), the number of people who can discover its vulnerabilities and repair them is far lower.

Closed source programs, while an understandable reaction to the fear of crime, are often counterproductive. Computer platforms such as Linux (an open source alternative to Microsoft's Windows operating system) will have major security advantages because they can harness the power of natural surveillance in ways that closed platforms, such as Windows, cannot. Because more people can see the code, the likelihood that security vulnerabilities will be quickly discovered and patched rises.<sup>14</sup> President Clinton's Technical Advisory Committee, for example, recognized that "access by developers to source code allows for a thorough examination that decreases the potential for embedded trap doors and/or Trojan horses."<sup>15</sup> Closure of code, like gated communities in realspace, may create a false sense of security.<sup>16</sup> And programmers who work together within a firm may develop groupthink and miss vulnerabilities while having an incentive to hide their mistakes from the outside world if they think they won't get caught.<sup>17</sup> Open source software, by expanding the pool of people who view the code, can harness the benefits of a diverse, far-flung group of minds and eyes to improve security.

In two senses, natural surveillance operates differently online than it does offline. First, natural surveillance primarily works offline when the public watches potential offenders and disrupts specific criminal activity. Online, however, it works when professionals and program users eye the code. Their gaze is not directed to any particular offender; rather, it is

---

14. For example, a patch to remove a major security vulnerability, the so-called Ping of Death whereby a remote user could flood a computer and cause it to crash, was posted on Linux within hours of the problem's discovery yet it took far longer for Microsoft to patch it. See TRUSECURE, OPEN SOURCE SECURITY: A LOOK AT THE SECURITY BENEFITS OF SOURCE CODE ACCESS (2001), at [http://www.trusecure.com/cgi-bin/refer.pdf?wp=open\\_source\\_security5.pdf](http://www.trusecure.com/cgi-bin/refer.pdf?wp=open_source_security5.pdf); see also Michael H. Warfield, *Musings on Open Source Security Models*, LINUXWORLD.COM, at <http://www.linuxworld.com/linuxworld/lw-1998-11/lw-11-ramparts.html> (last visited Feb. 27, 2003) (discussing how an open source model quickly solved a problem with the PGP2.6 encryption program).

15. PRESIDENT'S INFO. TECH. ADVISORY COMM., RECOMMENDATIONS OF THE PANEL ON OPEN SOURCE SOFTWARE FOR HIGH END COMPUTING 5 (2000), at [http://www.immagic.com/TOC/elibrary/TOC/meteor/downloads/PITAC\\_000911.pdf](http://www.immagic.com/TOC/elibrary/TOC/meteor/downloads/PITAC_000911.pdf). While empirical data is limited, Microsoft's closed source web server, IIS, was the most frequently targeted web server for hacking attacks in 2001, despite the fact that there are a larger number of open source Apache systems in use. See David A. Wheeler, *Why Open Source Software/Free Software (OSS/FS)? Look at the Numbers!*, at [http://www.dwheeler.com/oss\\_fs\\_why.html](http://www.dwheeler.com/oss_fs_why.html) (last visited Feb. 3, 2003). Indeed, some firms are switching to Apache to avoid the viruses that attack Microsoft server software. See Rutrell Yasin, *So Many Patches, So Little Time*, INTERNETWEEK, Oct. 4, 2001, at <http://www.internetweek.com/newslead01/lead100401.htm> (explaining that after the Code Red virus, the law firm Fenwick & West switched to Apache).

16. Open Source Initiative, Open Source FAQ, at <http://www.opensource.org/advocacy/faq.php> (last visited Feb. 3, 2003) (arguing that closed sources "create a false sense of security").

17. See Neal Kumar Katyal, *Conspiracy Theory*, 112 YALE L.J. 1307, 1323 & n.58 (2003) (discussing groupthink, the phenomenon whereby a group tends to exclude important points of view).

directed at the architecture itself. This shift in gaze reveals an important fact about cyberspace—because code is omnipresent and cheap to alter (compared to bricks and mortar in realspace), it plays a larger role in regulation of behavior online than offline.<sup>18</sup> This is both a blessing and a curse: It can help programs, particularly open source ones, adapt when vulnerabilities are found, but the ease with which architecture is changed can also facilitate exit and network fragmentation. Second, users who examine code for vulnerabilities cannot be equated with realspace bystanders. Only a small fraction of people can read source code, and those who do are most likely to do so when they expect some sort of reward, either an enhanced reputation or improved software product. As such, the pool of people available for natural surveillance online is smaller than it is offline. That fact does not spell the end of open source as a security model, for, as we shall see, sometimes smaller pools can bolster security by facilitating reputational rewards. But, when considered alongside the problem that open source programs make security holes in applications visible to potential cybercriminals,<sup>19</sup> one must pause before proclaiming that one side or the other has won the security debate.

For these reasons, the generic and far too ideological debate in the literature over whether open source is inherently more or less secure than closed source<sup>20</sup> fails to capture the nuances of space and design principles. Any good architect will admit that what works is often a matter of context.<sup>21</sup> Even Jacobs's vaunted natural surveillance, for example, fails in certain settings, which explains why houses in remote locations need

---

18. See Katyal, *supra* note 3, at 1094-111 (explaining how crime in cyberspace is prevented more through third-party strategies than through first-party ones).

19. KENNETH BROWN, OPENING THE OPEN SOURCE DEBATE 8 (2002) (arguing that opening the code teaches hackers how to attack it).

20. Compare, e.g., Warfield, *supra* note 14 ("The closed source camp likes to point out every open source security advisory as evidence that open source is insecure. In doing so, they conveniently ignore the counter examples in their own advisories. They also conveniently overlook the fact that open source problems are often found and fixed before they're widely exploited, while some closed source problem [sic] go unaddressed for months, or longer."), ERIC S. RAYMOND, THE CATHEDRAL AND THE BAZAAR (1999) (making a similar argument for open source security), Nicholas Petreley, *Microsoft's Road to Consumer Trust Is To Open Source Windows*, INFOWORLD, Nov. 13 2000, at <http://www.infoworld.com/articles/op/xml/00/11/13/001113oppetreley.xml> ("If having the source code makes it easy to spot weaknesses, the best way to find and plug security holes is to make the source code as widely available as possible and solicit the input of those who use it."), and BRIAN HATCH ET AL., HACKING LINUX EXPOSED: LINUX SECURITY SECRETS AND SOLUTIONS 8 (2001) (similar, with Rudolf Schreiner, Open Source Software Security, at [http://www.objectsecurity.com/whitepapers/open\\_source/open\\_source\\_security.html](http://www.objectsecurity.com/whitepapers/open_source/open_source_security.html) (last visited Jan. 9, 2003) (arguing that open source models are inherently less secure), and Mathias Strasser, *A New Paradigm in Intellectual Property Law? The Case Against Open Sources*, 2001 STAN. TECH. L. REV. 4, ¶¶ 72-75, at [http://stlr.stanford.edu/STLR/Articles/01\\_STLR\\_4/index.htm](http://stlr.stanford.edu/STLR/Articles/01_STLR_4/index.htm) (criticizing the claim that open source software has fewer bugs).

21. See Katyal, *supra* note 2, at 1049 & n.30 (quoting architects and concluding that "design principles for architecture and crime control cannot be divorced from the context in which they are applied").

fences, dogs, and other mechanisms to prevent trespass. The need for contextualization does not preclude predictions; it simply means that one must understand the conditions necessary for a given design to succeed. If the potential for natural surveillance is low, as it is with the remote house and its cyberspace counterpart, closure will provide a better security model than will openness.<sup>22</sup> With fewer users, moreover, closure may also bolster security because the chance of a malicious individual discovering a vulnerability is lower as well. As the number of users declines, the chance that a vulnerability will be discovered diminishes while the ability to track users increases.<sup>23</sup>

The upshot is that open source operating systems, such as Linux, will have security advantages over their closed competitors, but that more specialized applications with few users (and therefore a low number of eyeballs gazing at the code) may be less secure as open source products than as their closed counterparts.<sup>24</sup> Indeed, the weakness of the Microsoft platform was suggested, in a round-about way, by Microsoft Vice President Jim Allchin, who testified in antitrust proceedings that revealing Microsoft's source code to competitors "could damage national security and even threaten the U.S. war effort in Afghanistan."<sup>25</sup> Security by obscurity is no way to run sensitive systems, particularly in an era where infiltration of Microsoft by rogue employees, hacking, and brute force attacks using distributed computing power are not fanciful.<sup>26</sup>

---

22. I am assuming that security is a dominant concern with the application. Some applications, such as computer games, do not need high security; others may not need it because they do not connect to the outside world.

23. It is possible that larger numbers of users may exacerbate collective action problems. Yet extensive work by Yochai Benkler suggests that such problems do not manifest themselves on the Net in the traditional fashion; indeed, Benkler finds that thousands of people are willing to perform particularly boring tasks, such as looking for craters on maps of Mars. See Yochai Benkler, *Coase's Penguin, or, Linux and The Nature of the Firm*, 112 YALE L.J. 369, 384-85, 429-36 (2002); see also Eric von Hippel, *Horizontal Innovation Networks—by and for Users* (June 2002), at <http://opensource.mit.edu/papers/vonhippel3.pdf> (making a similar point).

24. See TRUSECURE, *supra* note 14, at 6 (stating that more than fifteen million people have touched Linux's code).

25. Caron Carlson, *Allchin: Disclosure May Endanger U.S.*, EWEEK, May 13, 2002, at <http://www.eweek.com/article2/0,3959,5264,00.asp>; see also Direct Testimony of Jim Allchin ¶ 19, *New York v. Microsoft Corp.* (D.D.C. May 3, 2002) (No. 98-1233 (CKK)), at <http://www.microsoft.com/presspass/trial/mswitness/2002/allchin.asp> (testimony of Group Vice President for Platforms, Microsoft Corporation) ("It is no exaggeration to say that the national security is also implicated by the efforts of hackers to break into computing networks. Computers, including many running Windows operating systems, are used throughout the United States Department of Defense and by the Armed Forces of the United States in Afghanistan and elsewhere. It is obviously important that computers being used in military operations be secure from external attack and eavesdropping.").

26. Reports exist that al Qaeda operatives gained employment at Microsoft and attempted to plant trapdoors and bugs in Windows XP. See *Cyber Terrorism: Terrorist Claims al Qaeda Infiltrated Microsoft*, NAT'L J. TECH. DAILY, Dec. 18, 2001; see also John Schwartz, *Experts See Vulnerability as Outsiders Code Software*, N.Y. TIMES, Jan. 6, 2003, at C1, at <http://www.nytimes.com/2003/01/06/technology/06OUTS.html> (documenting concerns about



## B. *Territoriality*

A second realspace crime-prevention technique is to construct landscapes and buildings that evince territoriality, a signal of stewardship of an area.<sup>27</sup> Concerns about territoriality must be balanced against the need for natural surveillance, so that spaces are neither too open nor too closed. If they are too closed, bystanders and residents cannot self-police; if they are too open, intrusion and crime could increase. The goal of territoriality is to ensure that people begin to know each other and develop a sense of caring for an individual place. Compare, for example, a dormitory design that features a single grand entrance with one that uses an entryway system. The entryway students, with fewer students per door, are more likely to know and monitor each other and more likely to intervene in times of trouble.<sup>28</sup>

In cyberspace, the vast numbers of people who traverse individual areas such as websites make it difficult to promote caring through partial closure. Instead, a cyberspace solution must try to capture territoriality's root benefits without doing damage to the Net's principal design innovation—its openness.<sup>29</sup> Territoriality in realspace is principally important because it permits bystanders to recognize intruders and intervene against them. In cyberspace, recognition of intruders, let alone intervention, is hampered by the fact that the Internet Protocol is built not to know a user's identity. Both small and large approaches to digital architecture, however, can help alleviate this problem.

Consider, in the small category, Internet Protocol logging (IP logging). Every computer on the Internet has a specific address, designated by a series of numbers, so that the network can route data to it. While some IP addresses are "dynamic" and change with frequency, others are not. IP logging captures the numeric addresses of computers that access a particular website. The address may yield a computer in a fixed location, or

---

how outsourcing of software coding to people outside the United States could permit terrorists to undermine computer security, and discussing a recent FBI raid on a government software contractor that reportedly was infiltrated).

27. See Katyal, *supra* note 2, at 1058-62.

28. *Id.* at 1061. Indeed, a study at Sarah Lawrence College found that students in a dormitory with few students per door had far fewer social problems. *Id.* at 1063-64 (citing OSCAR NEWMAN, DEFENSIBLE SPACE 75 (1972)).

29. Just as territoriality provides an incentive to care for an area in realspace, it could be argued that closure of code will create greater incentives to monitor it. See *Which Is More Secure? Open Source vs. Proprietary*, INTERACTIVE WK., July 17, 2001, at [http://www.linuxsecurity.com/articles/vendors\\_products\\_article-3350.html](http://www.linuxsecurity.com/articles/vendors_products_article-3350.html) (noting such an argument). But because the audience for many open source platforms is so large, even the relatively obscure lines of code are likely to be reviewed by peers. Again, for individual applications that do not enjoy such an audience, a closed source model might prove to be more secure. But unlike realspace, in which crime is prevented by largely unskilled bystanders, the technical skills necessary to find security holes in computer code themselves generate a certain amount of territoriality.

perhaps an address assigned to a domain, such as America Online, in which case a request to the electronic service provider, under the auspices of the Electronic Communications Privacy Act, may be necessary to couple the electronic address to a particular subscriber.<sup>30</sup> IP logging therefore can facilitate after-the-fact tracing, and could deter crime *ex ante*. One of the main reasons why crime is pervasive on the Internet is anonymity. Everything from obscene and threatening speech<sup>31</sup> to copyright infringement, credit card fraud, and hacking is facilitated by anonymity.<sup>32</sup> If websites started to log IP addresses, it would constrain some criminal activity.<sup>33</sup>

IP logging, however, will not detect more sophisticated criminals that “mask” their identity through a variety of techniques.<sup>34</sup> As more of our lives are lived on the Net, stronger solutions will be required. Of course, anonymity often serves useful purposes—consider the whistle-blower who fears retaliation or the survivor of incest who wants to avoid revealing his identity to an online support network.<sup>35</sup> The trick is to develop a strategy that targets the harmful consequences of anonymity without losing the advantages of the positive ones. One possibility, which may become available as biometric identification becomes cheap,<sup>36</sup> is for the government

30. 18 U.S.C. §§ 2701-2711 (2000).

31. *United States v. Alkabbaz*, 104 F.3d 1492 (6th Cir. 1997) (comparing e-mails describing the killing of a fellow University of Michigan student and posting of Usenet pornography to “snuff porn”); *Doe v. 2TheMart.Com, Inc.*, 140 F. Supp. 2d 1088, 1095 (W.D. Wash. 2001) (considering an anonymous chat room discussion that allegedly misrepresented a corporation’s conduct and crippled its stock price).

32. See Edgar Bronfman, Jr., Remarks at Real Conference 2000 (May 26, 2000), at <http://www.mpaa.org/copyright/EBronfman.htm> (“Anonymity, on the other hand, means being able to get away with stealing, or hacking, or disseminating illegal material on the Internet—and presuming the right that nobody should know who you are. There is no such right. This is nothing more than the digital equivalent of putting on a ski mask when you rob a bank.”); Stuart McClure & Joel Scambray, *Tricks of the Trade: Obscure Hacker Tracks and Make Anonymity Easily Attainable*, INFOWORLD, Jan. 18, 1999, at 61 (making a similar point).

33. According to the Carnegie Mellon Software Engineering Institute:

Log files are often the only record of suspicious behavior. Failure to enable the mechanisms to record this information and use them to initiate alert mechanisms will greatly weaken or eliminate your ability to detect intrusion attempts and to determine whether or not they succeeded. Similar problems can result from not having the necessary procedures and tools in place to process and analyze your log files.

See Carnegie Mellon Software Eng’g Inst., *Identify and Enable Web-Server-Specific Logging Mechanisms* (2000), at <http://www.cert.org/security-improvement/practices/p077.html>

34. See McClure & Scambray, *supra* note 32, at 61 (discussing how hackers avoid IP logging). In addition, there are currently some technical measures to help trace offenders. See Ofir Arkin, *Trace-Back: A Concept for Tracing and Profiling Malicious Computer Attackers* (2002), at <http://www.atstake.com/research/reports/acrobat/traceback.pdf>. And, sophisticated commercial intrusion-detection systems have been sold to the public for years. See *Internet Security Systems’ RealSecure Technology Excels*, M2 PRESSWIRE, July 3, 2002.

35. *McIntyre v. Ohio Elections Comm’n*, 514 U.S. 334, 357 (1995) (holding that “[u]nder our Constitution, anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and dissent. Anonymity is a shield from the tyranny of the majority.”).

36. Biometric fingerprint scanners for computers currently cost about \$100 on the retail market, which suggests that the cost to the U.S. government of buying scanners for every resident

to issue unique data identifiers to every individual. Each person would possess a specific digital identity, verified by biometric information such as a fingerprint scan.<sup>37</sup> That identity would not be presented to the outside world in cyberspace—a person could surf the Web using any pseudonym she wishes. But the pseudonym would be coupled to that hidden biometric data identifier, visible to the government only upon a showing of probable cause to a judge in a separate branch of government.<sup>38</sup> The biometric data could be encrypted, with keys held only by trusted parties, or courts themselves, and with each decryption logged and reviewed. Individuals would be free to use as many pseudonyms as they wish on the Net, but all of them would be linked to that unique identifier.

While verifiable pseudonymity would help law enforcement discover the true identity of offenders, it has severe costs. People may fear doing embarrassing things because of the potential for discovery and therefore socially important conduct like whistle-blowing could be chilled. Yet a digital fingerprint scheme, if done openly, might better protect such behavior than the ad hoc status quo. After all, some Internet Service Providers (ISPs) have revealed their customers' true identities in response to inquiries,<sup>39</sup> IP logging is already in use, and commercial intrusion detection systems exist today as well. Privacy online is protected in a haphazard, somewhat accidental fashion. If you buy a book under a particular screenname and e-mail address, you risk having that e-mail and screenname sold to other companies, perhaps with your real name attached

---

will be quite low within a few years. See Rebecca Fairley Rainey, *All It Takes Is a Fingerprint: Unlocking Portable Data*, N.Y. TIMES, Sept. 19, 2002, at G3. But as identification becomes widespread, the error rates may increase as well, leading to additional expenses to improve identification and database technologies. It is likely that standard passwords (and new, picture-based counterparts) can help facilitate biometric identification. See Neal Katyal, Editorial, *How To Fight Computer Crime*, N.Y. TIMES, July 30, 2002, at A19 (discussing such identification schemes).

37. An alternative is to use an identification system to track hardware instead of individuals. See Jonathan Weinberg, *Hardware-Based ID, Rights Management, and Trusted Systems*, 52 STAN. L. REV. 1251, 1253-54, 1263-68 (2000) (explaining how Intel's Processor Serial Numbers could be used to track transmissions from specific computers over the Internet). Either way, the system could accord with standard principles of government data collection. See DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS pt. III (1973), at <http://aspe.os.dhhs.gov/datacncl/1973privacy/tocprefacemembers.htm> (stating five principles: (1) that the existence of the system should not be secret; (2) that there must be a way for a subject to find out the contents of the data and how it is used; (3) that the individual can prevent information obtained for one purpose from being used for another purpose without his consent; (4) that the individual can correct or amend records; and (5) that the organizations that create, maintain, use, or disseminate such data must assure its reliability for intended use and take reasonable precautions).

38. To avoid piercing anonymity for trivial offenses, the range of offenses that trigger a probable cause hearing could be carefully circumscribed, akin to the way the wiretap statute delineates only particular offenses as eligible for wiretap orders. See 18 U.S.C. § 2516 (2000).

39. See, e.g., *McVeigh v. Cohen*, 983 F. Supp. 215 (D.D.C. 1998) (concerning a situation where America Online gave the U.S. Navy the actual identity of "boysrch" upon a simple phone request).

to it. No law prevents such an act. And with thousands of companies that may have access to these data, and little transparency about what they do with the information, the chilling effect of potentially having one's identity revealed exists now, and will increase in the future as data-mining technologies proliferate. In this new world, the powerful and technologically savvy can remain anonymous, by buying (or otherwise creating) new digital identities, but the rest of us cannot. We may therefore have the worst of every world—anonymous cybercriminals and identifiable law-abiders.

Alternatively, the law might go too far in the other direction and overfacilitate the piercing of anonymity. For example, a recent court decision requires the ISP Verizon to reveal the name of one of its subscribers to the Recording Industry Association of America (RIAA) because the RIAA suspects that the subscriber downloaded 600 copyrighted songs within one day.<sup>40</sup> But language in the decision suggests that all providers of Internet services will be required to name those to whom they provide access upon a request by an aggrieved party. The upshot could be to cripple one of the most promising avenues for the Net's future: free wireless broadband. Many individuals and corporations are setting up wireless 802.11b (wi-fi) networks—and permitting outsiders to use the spare bandwidth. The possibility here is dramatic—entire cities could provide free wireless broadband access to the Net by linking users together.<sup>41</sup> But users will not open up their bandwidth if doing so will expose them to legal liability for the acts of others. And individuals more generally will refrain from using anonymity for productive ends, such as whistle-blowing, when they fear that an ISP will be forced to reveal their identity upon a request by a private corporation.

Cyberspace provides an opportunity to build appropriate privacy safeguards into the system, thereby liberating us from the age-old battle of trying to adapt legal principles to an existing architecture. Instead of haphazard approaches, one possibility is to design the system to permit verifiable and unrestricted pseudonyms, and support that design with legal prohibitions against the unauthorized disclosure of identity by websites, ISPs, and the government. Such a system would minimize, but not erase, fears of improper disclosure, and would therefore still have a chilling effect on socially beneficial communication. But that effect must be weighed

---

40. See *In re Verizon Internet Servs., Inc.*, 240 F. Supp. 2d 24 (D.D.C. 2003).

41. See Todd Wallack, *Grassroots Techies Want To Build a Wireless Internet Network Across the Bay Area*, S.F. CHRON., June 30, 2002, at G3 (describing plans for a free wi-fi network in San Francisco, and stating that “[n]ationwide, countless Internet subscribers are already using their home wireless networks to share their DSL and cable modem access with neighbors”).

alongside the costs of anonymity—in terms of crime and the concomitant loss of trust in the network.<sup>42</sup>

This proposal, which creates pseudonymity and tracing capabilities, suggests one model to which the Net might aspire, apart from “all or nothing” solutions to digital anonymity. The point here is not to offer a magic bullet answer; rather, it is to think about cyberspace the way an architect would—by isolating what structural problems exist and outlining a path for generating design-based solutions to them.

### C. *Building Communities*

The principle of building community stresses architecture that facilitates easy interaction and encourages reciprocity.<sup>43</sup> Some neighborhood plans, for example, situate houses across the street from each other and use centralized parks to encourage people to meet one another and to let linkages between them blossom.<sup>44</sup> Quite obviously, the ability to link to anyone’s content on the World Wide Web is one way to facilitate such interactions online, as the rise of weblogs (blogs) demonstrates so well. But there are less obvious design features that follow this principle, too, such as the original Internet Protocol’s end-to-end communication structure. End-to-end refers to the idea that application-level functions should not be built into the middle of the network, thereby ensuring that the Internet’s routers and switches do not discriminate on the basis of content. As such, the network itself will not refuse to carry your data, whether it happens to be an MP3 music file, a law review article, or a streaming video signal. To the extent there is discrimination, it occurs at the edges of the network, since an individual computer may be configured to prevent any of these types of content from being received or sent. Therefore, e2e reduces the complexity of the core network and means that applications do not have to navigate around its particular programming features and quirks.<sup>45</sup> By refusing to freeze into place preferences for particular content, the Internet

---

42. Again, there are differences between territoriality solutions in realspace and cyberspace. Offline, territoriality facilitates not only the identification of perpetrators after a crime has been committed, but also, like natural surveillance, intervention in ongoing situations. In cyberspace, natural surveillance operates far earlier, well before a crime is committed, whereas territoriality often operates at the other end of the time spectrum. This is because territoriality solutions are predominantly methods that permit after-the-fact tracing, instead of real-time intervention. It is possible that identification may prevent particular ongoing crimes (such as the few that require plenty of unbroken time online), but for the most part, territoriality helps catch criminals after they have acted. Of course, ex post impacts upon ex ante, so that the higher the chance of getting caught, the less likely crime becomes.

43. See Katyal, *supra* note 2, at 1062-67.

44. See *id.* at 1064-65 (discussing such architecture).

45. See Marjory S. Blumenthal & David D. Clark, *Rethinking the Design of the Internet: The End to End Arguments vs. The Brave New World*, ACM TRANSACTIONS ON INTERNET TECH., Aug. 2001, at [http://www.ana.lcs.mit.edu/anaweb/PDF/Rethinking\\_2001.pdf](http://www.ana.lcs.mit.edu/anaweb/PDF/Rethinking_2001.pdf).

has spurred demand for new technologies that supplant the old ways of doing things.<sup>46</sup>

A variety of proposals today seek to modify this fundamental architectural choice. Cisco, for example, has developed routers that prefer specified content and applications.<sup>47</sup> In general, as these protocols get bundled into the routers and network layers, the threat to connectivity increases. Self-sustaining communities require a structure that permits change and decentralized growth. This was the original model of the Internet. In contrast, by moving toward a network that centralizes control, opportunities for advancement are stymied by the design limitations laced into the building plan.

Imagine, for example, that in an attempt to restrict the sharing of copyrighted music files, routers refused to carry traffic from computers with IP addresses that are running the popular KaZaa file-sharing program. This architectural change would undoubtedly reduce file sharing, but it would also threaten the network's ability to use peer-to-peer computing in the future for needs that we may not be able to adequately foresee today. Just as some attempts to reduce crime through street closures have harmed communities,<sup>48</sup> architectural responses to crime in cyberspace can pose serious long-term costs. Generally speaking, both online and offline, open networks for communication and transportation promote growth, opportunity, and interconnectivity. And while digital architecture is easier to modify than realspace architecture—in that digital code can be deleted more easily than buildings can be bulldozed—in neither case will change always be easy. It is already difficult to persuade the corporations and entities that own the routers and other technology that make up the backbone of the Net to make changes for the good of the network more

---

46. LESSIG, *supra* note 6, at 35-36; see also Mark A. Lemley & Lawrence Lessig, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era*, 48 UCLA L. REV. 925 (2001).

47. Lessig notes:

Rather than a neutral, nondiscriminatory Internet, they are deploying technologies to enable the "walled garden" Internet. The network is built to prefer content and applications within the garden; access to content and applications outside the garden is "disfavored." . . . The content favored by the policy becomes the content that flows most easily.

LESSIG, *supra* note 6, at 156. With broadband, cable companies have begun to use technologies that "enable them to give preference to certain kinds of content." Daniel S. Levine, *One on One with Lawrence Lessig*, *Author*, S.F. BUS. TIMES, Dec. 3, 2001, at <http://sanfrancisco.bizjournals.com/sanfrancisco/stories/2001/12/03/newscolumn10.html> (quoting Lawrence Lessig).

48. Katyal, *supra* note 2, at 1049-50 n.31 (discussing the street-closure program in Bridgeport, Connecticut). The recording industry is already exploring code that would implement such measures. See Andrew R. Sorkin, *Software Bullet Is Sought To Kill Music Piracy*, N.Y. TIMES, May 4, 2003, at A1 (discussing how the recording industry is exploring using "interdiction" methods that would "prevent a person from using a network while attempting to download pirated music or offer it to others").

generally. Once they depart from the Net's current nondiscriminatory structure, it will be far more difficult to convince them to rebuild the architecture back in the "traditional," e2e-compliant, style, particularly when its benefits are public, rather than private, goods.

The argument, however, only goes so far. Just as our desire for open space does not translate into a requirement that houses have no doors, so too e2e does not require open access to all computers. Rather, the e2e principle suggests that most gates should be placed at the layer of individual computers, rather than at other layers where they would impede traffic and harm the network. Effective guards for private data are therefore a necessity. Yale University recently learned this lesson the hard way when it discovered that a Princeton University admissions officer had bypassed the simple password protection on the Yale site.<sup>49</sup> Everyone roundly condemned the Princeton official, who was, of course, an intruder acting in an unprofessional manner. But few criticized Yale for using such a weak gate to protect its private data in the first place.<sup>50</sup> Private firewalls must be strong and secure, precisely to encourage institutions to make their data and computers accessible to appropriate individuals. Without them, content providers will refrain from putting material online—whether it be notifications to successful applicants, products to be sold, accessibility to remote networks, or anything else.

Just as the open source debate has been overly ideological, so, too, has the end-to-end one. Sometimes there are needs to break away from e2e principles. In realspace, for example, economies of scale counsel against placing barriers only at end points. For example, it is more efficient to monitor airports and other borders for crop-eating plants and bacteria than it is to employ self-protection by every possible victim. So, too, in cyberspace it is worth thinking about whether the chokepoints to virus protection should reside in the middle of the Net's architecture.<sup>51</sup> Instead of forcing every individual to buy virus protection software and to properly update it, it may be more efficient to bulk scan e-mails and network communications

---

49. Karen W. Arenson, *Princeton Pries into Web Site for Yale Applicants*, N.Y. TIMES, July 26, 2002, at A1.

50. Such private firewalls, however, are an important barrier to crime:

Computer attacks are best prevented not with new criminal penalties, but with common sense and the use of simple digital architecture that enhances security. We use architecture every day in the real world to prevent crime, from driveway gates to streetlights. Because computer criminals are so difficult to prosecute, digital architecture plays an even more important role in fighting crime. The [Princeton] case illustrates this point well: To use a password like a Social Security number is the equivalent of leaving a house key under the doormat.

Katyal, *supra* note 36.

51. See Larry Sobers, *Anti-Virus Architecture: A 4-Layered Approach*, SANS INST., Oct. 31, 2000, at <http://tr.sans.org/malicious/tr/anti-virus.php>.

for viruses. Both Harvard Law School and Hotmail employ such systems today,<sup>52</sup> thereby reducing the need for end users to protect themselves.<sup>53</sup>

One of the unforeseen advances in computer networking has been the emergence of peer-to-peer systems (p2p). In its most popular form—file sharing services such as Napster—p2p permits users to share content with one another without the use of a centralized server. The p2p model has the potential to revolutionize computing. Instead of everyone trying to access the CNN site at the same time, for example, a computer might simply “chain” CNN’s content from another peer computer that has just visited the site. A second example: Search engines could become even more efficient by using the power of multiple computers and aggregated searches.<sup>54</sup> Yet p2p applications require significant trust in one’s peers, and fear of viruses, hacking, and other computer crimes has severely discouraged their use.<sup>55</sup>

Like open source and e2e, p2p is not necessarily good or bad in all contexts. Some have celebrated it explicitly,<sup>56</sup> others implicitly.<sup>57</sup> And some have harshly attacked it.<sup>58</sup> At the application level, one deep question is

---

52. See E-mail from Pete Chvany, UNIX Systems Administrator, Harvard Law School, to Harvard Law School Faculty (Dec. 20, 2002) (on file with author) (stating that Harvard Law School will employ virus scanning of e-mail); Hotmail, at [http://www.hotmail.msn.com/cgi-bin/dasp/ua\\_info.asp?&\\_lang=EN&country=US#q12](http://www.hotmail.msn.com/cgi-bin/dasp/ua_info.asp?&_lang=EN&country=US#q12) (last visited Apr. 1, 2003) (stating that Hotmail uses McAfee Security Service).

53. Bulk scanning of customer e-mail generates positive externalities, in that inoculated computers avoid spreading destructive viruses to others. With enough inoculation, digital viruses can be significantly contained and destroyed, akin to what doctors call “herd immunity” in realspace. Katyal, *supra* note 3, at 1076.

54. MICHAEL MILLER, DISCOVERING P2P 34-35, 194-203 (2001) (discussing search engines that use p2p technology).

55. Security is the Achilles heel of p2p. As even the strongest p2p admirers concede, “security remains the biggest question facing all peer-to-peer applications.” HASSAN M. FATTAH, P2P: HOW PEER-TO-PEER TECHNOLOGY IS REVOLUTIONIZING THE WAY WE DO BUSINESS 180 (2002); see also MILLER, *supra* note 54, at 63-64 (discussing the impact of viruses on the Gnutella network).

56. FATTAH, *supra* note 55, at 12 (explaining how “Napster wasn’t just about sharing music,” but rather “about building empowered communities, about building an empowered workforce, and about mapping your computer systems to better match the behavior and quirks of people”).

57. In a brilliant recent article, Yochai Benkler explains how peer production can provide products that rival traditional centralized models. Benkler, *supra* note 23. While Benkler claims to offer a “purely descriptive account” of peer production, *id.* at 381, the article at various points becomes a normative celebration of it. Consider, as one illustration, the article’s final words: “It is of central importance that we not squelch peer production, but that we create the institutional conditions needed for it to flourish.” *Id.* at 446. There are any number of reasons why one might fear peer production as a general model, reasons suggested by Benkler’s own mention of Napster. *Id.* at 397. Regardless of how one feels about current copyright law, peers can produce all sorts of products, many of which can be harmful, such as viruses, denial-of-service attacks, distributed attacks on encryption algorithms, and the like. These harms might be overwhelmed by the benefits of folding a larger number of people into the productive process, akin to James Madison’s claim in *The Federalist*. See THE FEDERALIST NO. 10, at 79-82 (James Madison) (Clinton Rossiter ed., 1961). But the case here is not an obvious one.

58. See Cory Doctorow, *Hollywood’s Copyright Fight Might Hit Digitally Close to Home*, ORLANDO SENTINEL, Oct. 20, 2002, at G1 (discussing the “Hollywood call for a ban on P2P”); *Education Sector Wants Controllable Broadband*, BROADBAND BUS. REP., Oct. 8, 2002



whether p2p might provide a new security model. Already, p2p security applications are emerging, with companies such as McAfee using p2p to provide quick updates for its anti-virus software, thereby avoiding the peril of having millions of customers crash their servers looking for updates when new viruses hit the Net.<sup>59</sup> In the preceding Section on territoriality, centralized law enforcement was highlighted as a way to control crime. But, as Jacobs might ask, could peers guarantee digital security instead? Unlike natural surveillance (which operates online before a crime is committed) and territoriality (which operates online after the crime has been committed), the use of architecture to enable real-time intervention by peers is difficult. Certain forms of crime might be prevented in this way, such as online harassment and stalking in chat rooms, but a large number of offenses (among them, unauthorized access and disruption, piracy, and child pornography) are not visible at all to peers.

Put differently, today cyberspace is *dark*. One cannot see what other users are doing at any given time. But, as concern about computer crime becomes greater, the architecture could flip—just as it did with the advent of gas lighting and electricity—and shed light on users in cyberspace. Imagine that each ISP customer, on a monthly basis, is randomly aggregated with forty-nine other customers. Each customer, or their pseudonym, would show up as a small avatar on the top right of the other forty-nine users' screens. A right-click at any moment would indicate what that person was doing, and an option would notify the authorities (either public or private) about suspicious activities.<sup>60</sup> This is one possible future to envision, where p2p principles are harnessed to augment security.<sup>61</sup> But there are serious costs, not just in terms of privacy, but also in terms of harm to the network. Realspace architects have found that it is often self-defeating to brightly illuminate areas to reduce crime—the upshot can be to scare users away from the street altogether and make the area look like “a prison yard.”<sup>62</sup>

---

(observing that “Indiana University banned all P2P applications” and that “[m]any other colleges have followed suit”).

59. FATTAH, *supra* note 55, at 135-41. P2P may even offer a reliable strategy to blunt the force of denial of service attacks by dispersing the placement of content across the Net. See IRIS: Infrastructure for Resilient Internet Sys., at <http://iris.lcs.mit.edu> (last visited Feb. 27, 2003).

60. As children taught about wolves and crying quickly learn, if a user falsely blew the whistle too many times, law enforcement would not take their warnings seriously. Conversely, users who give law enforcement helpful information would develop positive reputations around their pseudonyms.

61. As an alternative to gathering ISP customers, the system could randomly group users of a specific site together. When someone signs onto, say, Chase-Manhattan Bank, she could be bundled with fifteen other users, identified by avatar and pseudonym. A right-click would have the same function of revealing activities and enabling reporting to law enforcement.

62. Jackie Spinner, *The Jury's out on Hotel's Lights; Dupont Circle's Bulbs Divide Community*, WASH. POST., Feb. 23, 2001, at E1; see also RRM Design Group, *Are Trees Killing Your Downtown?: Top Ten Tips for Designing a Consumer Friendly Downtown 2*, at

The drive to illuminate cyberspace, and harness the surveillance powers of peers, thus has the potential to scare people away from the Net, instead of encouraging them to use it. As ISPs begin thinking about using such surveillance methods, their actions may generate negative externalities on the community in cyberspace more generally. As such, we should resist any government pressure to illuminate cyberspace because doing so can harm the network as a whole. And we should be developing security solutions that blunt the tendency of providers to overilluminate their space in the name of reducing computer crime. In other words, the threats to anonymity and other (far more significant) forms of freedom on the Net do not simply originate from the state; preventing cybercrime through law and public architecture can forestall attempts to restrict these freedoms by private actors.

Illumination is one of many examples in which subtle cues from the environment can alter crime rates. In recent years, much of the realspace research about such cues has fallen under the rubric of “the broken windows theory” of crime control, which posits that visible disorders should be punished because they breed further crime. The insight of its two original authors, James Q. Wilson and George L. Kelling, was that these disorders are not always the most serious crimes like murder and rape, but instead could be as trivial as loitering and littering.<sup>63</sup> Wilson and Kelling thus inverted the standard thinking about enforcement and suggested that it was more effective to focus on low-level crime. As crimes become more common, the norms that constrain crime erode, and more crimes take place as a result of that erosion. But Wilson and Kelling, in their attempt to stimulate legal reform, wrongly downplayed the role of architecture in solving the problem that they brilliantly identified.<sup>64</sup>

Just as certain realspace architectural choices can facilitate crime, computer programs can be written in ways that cue cybercrime as well. Consider Bearshare, a file-sharing program that operates on the Gnutella p2p network. Unlike many other file-sharing programs, Bearshare’s

---

<http://www.rmdesign.com/news/pdf/designing-downtown.pdf> (last visited Feb. 27, 2003) (discussing the negative effect on “strolling and shopping” when lighting is too bright); Katyal, *supra* note 2, at 1057 (discussing how particular forms of lighting can reduce natural surveillance).

63. See James Q. Wilson & George L. Kelling, *Broken Windows*, ATLANTIC MONTHLY, Mar. 1982, at 29.

64. Wilson and Kelling claimed that high levels of crime were a response to a breakdown in social order, and that the solution to the breakdown was to reform police practices. Yet Wilson and Kelling’s conclusions are somewhat suspect since they were derived from a study of the New Jersey Safe and Clean Neighborhoods Program, a program that not only changed law enforcement, but changed architecture as well. These architectural changes went unmentioned in their article, prompting cities like New York to follow the law-enforcement-centered approach to broken windows. See Katyal, *supra* note 2, at 1078-83 (describing how Wilson and Kelling ignored the New Jersey program’s design-based features and the role of architecture more generally).

"monitor" feature allows a user to see all the requests that are being made of the Gnutella network in real time.<sup>65</sup> Within twenty seconds, a user will glimpse dozens of requests for grotesque pornography, top-forty songs, and the like that flood the system. The user sees only the requests, with no user name or even IP address attached to them. Such visibility can induce crime—suggesting potential files available on the network—and can reduce the psychological barriers to downloading certain forms of content. By creating the perception that downloading such files is common, the architecture of the Bearshare program thus can generate additional crimes.

Computer programs must carefully control the cues that prompt crime, such as this Bearshare monitor feature. In realspace, environmental psychologists have shown that architects can manipulate subtle details to induce massive changes in behavior. The size and shape of tables will predict who talks to whom; the placement of lights in a lobby will make it easy to know where people will stand; the hardness of a chair will force people to get up quickly.<sup>66</sup> Digital architecture has similar properties.<sup>67</sup> Small changes to the way in which programs operate may have significant payoffs because digital architects can manipulate (indeed, already are manipulating) tastes in hidden ways.

Another suggestion follows from the darkness not of users, but of crime itself, in cyberspace. With most computer crimes, there are no broken windows to observe and no loiterers and panhandlers to avoid. While this poses challenges in terms of discovery and tracking down offenders, it also has a significant upside: It makes it harder for one crime to serve as a complement to another. Many corporate victims do not report cybercrime to the police because they fear alerting customers and shareholders to the lack of security.<sup>68</sup> Because only the corporation has knowledge of the crime, no

---

65. See BearShare, BearShare Product Documentation, at <http://www.bearshare.it/help/monitor.htm> (last visited Feb. 27, 2003) (describing the monitor feature).

66. Katyal, *supra* note 2, at 1043-44, 1072-73. As Lawrence Speck, the Dean of the University of Texas School of Architecture, puts it, architecture operates "much more [on the] subconscious than [the] conscious. Architecture is all about subliminal experience. . . . You listen to music, you look at a painting. But you live in architecture, and it affects you whether you're even conscious of it." Avrel Seale, *Architect Lawrence W. Speck and "The Vision Thing,"* TEX. ALCALDE, July-Aug. 1999, at <http://txtell.lib.utexas.edu/stories/s0007-full.html>.

67. To take obvious examples: A link can be placed on the home page, in a prominent font and color, or placed in a space that requires users to scroll down.

68. *Economic Cyber Threats: Hearing Before the Joint Economic Comm.*, 106th Cong., 2000 WL 11068387 (2000) (statement of Vinton G. Cerf, Senior Vice President of Internal Architecture and Technology, MCI Worldcom) ("Companies are concerned that revealing and admitting past mistakes, shortcomings, negative experiences or incidents can open them up for [public] criticism [or potential legal liability]. . . . [C]ompanies are [also] loath to share proprietary or privileged corporate information. Additionally, firms run the risk of eroding consumer, customer, partner and investor confidence."); Huseyin Cavusoglu et al., *The Effect of Internet Security Breach Announcements on Market Value of Breached Firm and Internet Security Developers* (Feb. 2002), at <http://www.utdallas.edu/~huseyin/breach.pdf> (finding that "the announcement of Internet security breach is negatively associated with the market value of the announcing firm," and that

one else is likely to discover it. The broken windows theory of crime control suggests that government might want to keep some forms of crime invisible—not only to encourage victims to come forward, but also to prevent social disorder wrought by complementary crimes and visible disorder. For example, most of the widely reported and publicly known computer crimes, such as Robert Morris's worm and the recent ILoveYou bug, prompted rashes of copycat crimes.<sup>69</sup> The fear that ensues after a reported attack, moreover, can lead to less use of the Net—with pernicious consequences for its growth.

Therefore, for specialized attacks that are unlikely to be replicated and for which countermeasures are easily developed, government might provide assurances to victims that these crimes will remain secret to the extent possible.<sup>70</sup> Of course, when the vulnerability is a more generalized one, such secrecy cannot be maintained, both for reasons of natural surveillance as well as the need to minimize damage through protecting targets.

#### D. *Target Protection*

The architectural approach to crime reduction begins by emphasizing that law alone cannot solve crime, for police officers can't be everywhere. Instead, society relies on citizens to prevent the bulk of crime. But some private action will be ineffective, and perhaps even harmful. After all, private actors try to prevent crime with whatever makeshift measures they have available, such as iron bars on windows or avoiding the streets altogether.<sup>71</sup> But these forms of target protection can have serious negative externalities, particularly in their crippling of interconnectivity and their destruction of reciprocity. Bars on windows and other target hardening scare people away, fragmenting the community and the development of an ethos that promotes order. Thus, instead of decreasing crime, these acts of self-help can actually increase it.<sup>72</sup>

---

"[c]ompromised firms, on average, lose approximately 2.1% of their market values within two days," which "translates into \$1.65 billion average loss in market capitalization per incident").

69. See *Internet Integrity and Critical Infrastructure Protection Act: Hearing Before the Senate Comm. on the Judiciary*, 106th Cong., 2000 WL 23832308 (2000) (statement of Assistant Attorney Gen. James K. Robinson, Criminal Division, Department of Justice) ("Frighteningly, the 'I Love You' virus was followed almost immediately by copycat variants. [Among the] almost 30 . . . variants that . . . followed . . . [was] the New Love virus, a virus that self-replicated, mutated in name and size, and destroyed the computer systems affected by it.").

70. Since these crimes may only affect individual entities (putting to one side situations in which viruses replicate and spread to other computers), prosecution of these cases should be a lower priority because they do not create harmful complementarity. Building on the experience of victims, the government could occasionally release reports about how to maintain effective computer security. Therefore, government should create mechanisms to permit victims of crime to inform law enforcement of security breaches while providing for appropriate secrecy.

71. See Katyal, *supra* note 2, at 1067-71.

72. *Id.* at 1084-86.

One underappreciated function of public law enforcement, which might be called a liberal argument for crime control, is to cultivate and protect public networks. In cyberspace, the network concerns are omnipresent: For example, a virus will scare computer users into restricting their computer connections (particularly their e-mail and p2p networking), fear of interception leads many to fear using e-mail, and the possibility of credit card theft prompts many not to make online purchases.<sup>73</sup> Assurances about security are necessary to promote the Internet's growth, just as they are necessary in realspace for vibrant and dynamic cities. In economic terms, the Net takes advantage of network effects. A network effect occurs when the utility of a good increases with the number of other agents who are consuming the same good.<sup>74</sup> The Internet's value lies, at least in part, in exploiting these network effects. As more people come online and share more of their lives, the Internet's value increases.<sup>75</sup> Vigorous enforcement of computer crime prohibitions can help ensure that the network's potential is realized.

Without a strong public law enforcement presence on the Net, the Net risks balkanization into a series of separate systems. When people fear computer crime, they may only connect with other "trusted" computers, stifling one of the greatest communication innovations in our lifetime—the ability to connect directly with, and learn from, people with whom we lack any prior experience.<sup>76</sup> Some today are even proposing a division of the

---

73. See *Many Worry Net Is Not Safe, Study Finds*, CNN.COM, Oct. 16, 2002, at <http://www.cnn.com/2002/TECH/internet/10/16/internet.report/index.html>.

74. Michael L. Katz & Carl Shapiro, *Network Externalities, Competition, and Compatibility*, 75 AM. ECON. REV. 424, 424 (1985); see also Michael L. Katz & Carl Shapiro, *Systems Competition and Network Effects*, J. ECON. PERSP., Spring 1994, at 93, 94 ("Because the value of membership [in a network] to one user is positively affected when another user joins and enlarges the network, such markets are said to exhibit 'network effects,' or 'network externalities.'"); S.J. Liebowitz & Stephen E. Margolis, *Network Externality: An Uncommon Tragedy*, J. ECON. PERSP., Spring 1994, at 133 (refining and limiting the Katz and Shapiro concept).

75. The standard phrase to capture this is "Metcalfe's Law"—that the value of participation on a computer network grows exponentially with the size of the network. George Gilder, *Metcalfe's Law and Legacy*, FORBES ASAP, Sept. 13, 1993, at 158, 160; see also Mark A. Lemley & David McGowan, *Legal Implications of Network Economic Effects*, 86 CAL. L. REV. 479, 483-84, 484 n.9 (1998). While this is no doubt an exaggeration, the larger the number of people online, in general, the greater the advantages there are. See generally ALBERT-LÁSZLÓ BARABÁSI, *LINKED: THE NEW SCIENCE OF NETWORKS* (2002) (outlining payoffs to larger networks).

76. For example, at the time when the Supreme Court was hearing its first major Internet case, a constitutional challenge to an act of Congress that regulated online pornography, the entire Court had only two computers with Internet access due to security fears. See Martha Woodall, *First Computerized Brief Filed with Supreme Court*, PHILA. INQUIRER, Feb. 21, 1997, at A1 (quoting the Supreme Court's public information officer as saying at the time that "[f]or security reasons . . . the computers in the court are part of an internal network that prevents the justices from surfing the Web or exchanging e-mail with outsiders," that "the court has two stand-alone computers with Internet access," and that it is doubtful whether "any of the nine Supreme Court justices had an Internet account at home").

Internet into two networks to bolster its security.<sup>77</sup> In other words, we should fear the response to cybercrime—private architectures of control—nearly as much as the crimes themselves. Because computer crime will become easier to perpetrate as a result of increasing automation, bandwidth, and skills, private developers will have reason to put these architectures in place, with grave consequences for the network and freedom. When not carried out appropriately, target protection, like its cousins natural surveillance and territoriality, risks harm to the network by enabling destructive private precautions.

The social costs of private precautions are not typically given much weight in legal discourse. Consider the famous Learned Hand test in torts, that negligence depends on whether the expense of private precautions (*b*) exceeds the probability of an accident (*p*) multiplied by the harm of that injury (*l*). In the case that gave rise to the test, a ship had broken away from its tow and smashed into a tanker. The ship owner sued the towing company, but the towing company said that the ship owner was contributorily negligent for not having an attendant on board. Hand sided with the towing company, reasoning that the ship owner could have avoided the accident with an attendant.<sup>78</sup> Hand, however, focused only on the cost of precautions to the ship owner. While perhaps appropriate on those facts, this formula treats all forms of prevention as equal and unfortunately fails to consider the negative externalities of private precaution.

It is from this vantage point, that a key cost of crime lies in the private reactions of potential victims, that one should assess the effectiveness of any computer security plan. Take, for example, the new cybersecurity initiative by the White House. Far from being a breakthrough document, the Strategy is a hodgepodge of concepts and consulting talk, devoid of a serious agenda.<sup>79</sup> Both simple and complicated solutions to cybercrime

---

77. See RICHARD O. HUNDLEY ET AL., RAND NAT'L DEF. RESEARCH INST., THE FUTURE OF THE INFORMATION REVOLUTION IN EUROPE 48 (2001), at <http://www.rand.org/publications/CF/CF172>. Apart from balkanization, assurances about trust are necessary to exploit positive network effects. Consider a search engine, which requires two levels of trust: the trust between the engine and the sites it indexes, and the trust between the individual user and the particular target websites identified by the engine. Both of these levels can be compromised by fears about computer security. Owners of sites may not give search engines sufficient access to their content to adequately index it, and they may forbid unknown users from entering the site at all.

78. *United States v. Carroll Towing Co.*, 159 F.2d 169, 173 (2d Cir. 1947).

79. The White House released a draft of its proposal in September 2002 that received much criticism along these lines. See FOURTH ANNUAL REPORT TO THE PRESIDENT AND THE CONGRESS OF THE ADVISORY PANEL TO ASSESS DOMESTIC RESPONSE CAPABILITIES FOR TERRORISM INVOLVING WEAPONS OF MASS DESTRUCTION 81-82 (2002), at <http://www.rand.org/nsrd/terrpanel/> [hereinafter *FOURTH ANNUAL REPORT*] (stating that the White House draft proposes “voluntary, tactical responses to an inherently strategic problem of national importance” and “largely failed to exercise any of its powers besides persuasion” and that there “are essentially little or no consequences for Federal government agencies and officials who do not take prudent steps to improve cyber security”); Mark D. Rasch, *What About Our Cyber-Security?*, WASH. POST, Sept. 26, 2002, at A32 (stating that “[i]f security is in the national

were obscured by an antiregulatory, antigovernment bias that infected the Strategy's outlook and thinking from the start. In its single-minded focus on computer security, moreover, the White House did not pause to think about what values the Net serves. These failures are yoked together: The White House wants private industry to do the work of securing cyberspace, but the most obvious private sector response is to diminish connectivity. And if, as some have suggested, the burden for crime prevention is placed on ISPs, so that they are responsible for the criminal acts of their subscribers, the result will be harm to the Net and its users as ISPs purge their subscriber base of customers who arouse the faintest whiff of suspicion.<sup>80</sup> There is a different path, one that situates the government as an active protector of the Net and its users, just as government protects city streets and their users.

The Strategy announces that "[t]he federal government should . . . not intrude into homes and small businesses, into universities, or state and local agencies and departments to create secure computer networks."<sup>81</sup> While government intrusion is not typically something to be preferred, a careful discussion necessarily must examine the costs of failing to intrude. Yet all the Strategy gives us is some weak guidance in this regard<sup>82</sup> coupled with proclamations about the power of the market such as "federal regulation will not become a primary means of securing cyberspace" and "the market itself is expected to provide the major impetus to improve cybersecurity."<sup>83</sup>

---

interest, the government must, through the purse and the sword, force itself and the private sector into compliance" and that the White House strategy "specifies no sanctions" for the failure to adhere to any of the government's recommendations for minimizing the risk of cyberattacks); *Critics: National Cybersecurity Plan Too Weak*, CAPITAL TIMES, Sept. 19, 2002, at 4E (quoting a computer security expert as stating that the "voluntary security plan" is analogous to "asking ordinary citizens to erect a nuclear shield when it's obviously the government's job to organize those things"); Marcus J. Ranum, *Federal Cybersecurity: Get a Backbone*, TISC INSIGHT, Sept. 24, 2002, at <http://www.tisc2002.com/newsletters/414.html> (making a similar criticism); Press Release, CSIS, *Cybersecurity: Current Challenges Larger than National Strategy Response* (Sept. 18, 2002), at [http://www.csis.org/press/pr02\\_43.htm](http://www.csis.org/press/pr02_43.htm) (quoting James Lewis, Director, CSIS Council on Technology and Public Policy, as saying that "[c]ompanies will only change their behavior when there are both market forces and legislation that cover security failures. Until the U.S. has more than just voluntary solutions, we'll continue to see slow progress in improving cybersecurity."). It is worth noting, however, that the final Strategy did propose a few significant changes that may augment cybersecurity, such as a National Response System and some use of the procurement power. See WHITE HOUSE, *supra* note 7, at 21 (discussing the response system); *infra* note 96 (discussing the procurement power).

80. This is because the marginal benefits to the ISP of having an additional subscriber are outweighed by the risk of an adverse judgment against it. See Katyal, *supra* note 3, at 1086-88 (discussing the asymmetric incentive problem, and providing an example of how prohibitions of hostile environments in the workplace can often result in firing employees under minor suspicion).

81. WHITE HOUSE, *supra* note 7, at 11.

82. *E.g.*, *id.* at ix (stating that the "federal role in these and other cases is only justified when the benefits of intervention outweigh the associated costs").

83. *Id.* at 15; see also *id.* at xiii ("The federal government alone cannot sufficiently defend America's cyberspace. Our traditions of federalism and limited government require that organizations outside the federal government take the lead in many of these efforts."); Jennifer Lee, *White House Scales Back Cyberspace Plan*, N.Y. TIMES, Feb. 15, 2003, at A14, at

But, throughout its sixty-page report, the White House never really stopped to consider the harm caused by private ordering to prevent computer crime. This isn't merely an oversight.<sup>84</sup> The "market itself" can help minimize cybercrime, but often at a cost that is too dangerous to bear.

Like the White House, prominent academics have also not considered all the implications of this point. Consider two of Larry Lessig's major arguments in *Code*: (1) private ordering can pose dangers as severe as those levied by the state, and (2) architecture is a tool of control.<sup>85</sup> Lessig's second claim leads him to fear government regulation of architecture because it may lack transparency.<sup>86</sup> But, when considered in conjunction with the first, the second argument explains why the government should regulate architecture, and why such regulation is not as dire a solution as Lessig portrays.<sup>87</sup> After all, when Congress regulates architecture, it does so

---

<http://www.nytimes.com/2003/02/15/technology/15CYBE.html> (explaining how the Strategy backs away from government regulation in favor of market approaches); Jonathan Krim, *Cyber-Security Strategy Depends on Power of Suggestion*, WASH. POST, Feb 15, 2003, at E1 (similar). Even the draft Strategy released in September was criticized for its belief in the market. See Brian Krebs, *Cybersecurity Draft Plan Soft on Business, Observers Say*, WASHINGTONPOST.COM, Sept. 19, 2002, at <http://www.washingtonpost.com/ac2/wp-dyn/A35812-2002Sep18?> (stating that "intense lobbying from the high-tech industry has pulled nearly all the teeth from the plan when it comes to steps the technology industry should take," and quoting Bruce Schneier as stating that the plan will have "absolutely zero effect"); Paul Magnusson, *Commentary: Is Business Cheaping Out on Homeland Security?*, BUS. WK., Sept. 30, 2002, at [http://www.businessweek.com/magazine/content/02\\_39/b3801063.htm](http://www.businessweek.com/magazine/content/02_39/b3801063.htm) ("Thanks to heavy lobbying by the tech sector, The National Strategy to Secure Cyberspace Report, released Sept. 18 by the White House, substitutes weak suggestions for tough directives. Gone from previous versions: a special government-and-industry-fed fund to be used to upgrade network security; requirements for Internet service providers to boost customer protection; and mandatory moves to enhance wireless-network security. Cybersecurity 'is an area that cries out for government regulation, but the response has been 'Yawn, ho hum' . . . . That, many experts fear, could set the stage for future security lapses." (quoting Russ Cooper, TrueSecure Corporation)).

84. In a few places, the White House does mention law enforcement. E.g., WHITE HOUSE, *supra* note 7, at 28-29. Far from containing a single new idea, the Strategy does not even explain what the need for law enforcement is, let alone provide a blueprint for how to achieve it. Again, this flaw is attributable to the Strategy not being tethered to an understanding of cybercrime's harm. The White House knows that cybercrime can cause billions of dollars in damage. See *id.* at 5-8 (discussing financial repercussions of computer crime). But the key isn't to focus on the harm of cybercrime; it is to zero in on the social cost of the precautions private actors, left to their own devices, will take to avoid being victims.

85. See, e.g., LESSIG, *supra* note 1, at 128-38 (discussing harm from private control over intellectual property); *id.* at 6-8 (arguing that code regulates in ways similar to law).

86. See, e.g., *id.* at 98 ("The state has no right to hide its agenda. In a constitutional democracy its regulations should be public. And thus, one issue raised by the practice of indirect regulation is the general issue of publicity. Should the state be permitted to use non-transparent means when transparent means are available?"); see also *id.* at 7, 18, 44; Lawrence Lessig, *The Law of the Horse: What CyberLaw Might Teach*, 113 HARV. L. REV. 501, 541-43 (1999) (contending that secret regulation of code would diminish political accountability and enable the government to "avoid the political consequences of its choices").

87. Throughout his book, Lessig states that he is not averse to some forms of regulation and that he is not "against government." LESSIG, *supra* note 1, at 208. But his fear of government regulation of code, that it will lack transparency without some modularity and openness of the source code, *id.* at 224-25, is somewhat overstated. Government regulation of code will on balance expose more code to the public eye than will private ordering.



against a backdrop of sunshine laws and practices—from the Freedom of Information Act (FOIA) to open congressional hearings. Private code labors under no such constraint.

Once it becomes clear that the White House proposal has not changed computer security in any concrete way, three options will emerge. Option one is for the executive branch to develop private agreements with industry. Certain benefits, whether financial or regulatory, might be promised in exchange for commitments by engineers to develop products that protect certain digital rights, or commitments by ISPs to facilitate law enforcement operations through tracking and monitoring of customers. Such agreements are done without publicity and without the benefit of open laws and meetings. These forms of coercive nonregulation permit the partially invisible hand of the executive branch's national security apparatus to clasp the fully invisible hand of the market, with dangerous consequences for transparency.

Option two is for private industry to develop architectures of control on its own. These design choices can be hidden from public view in their entirety due to closure of the code. In the modern age, private architectures of control pose just as much, if not more, of a threat to transparency and individual freedom than public ones. Major conglomerates, whether they be Microsoft, AOL-Time Warner, or Cisco, can dramatically alter human behavior online with little need to be open and forthcoming in the process. If Microsoft fears viruses that attack its Outlook program, it can develop sophisticated ways to trace such criminals and embed these features in the code. If Hollywood fears the theft of copyrighted motion pictures, it can develop code that notifies the studio when someone is playing a movie without apparent authority. Some of these features might successfully be hidden from the public. And those that are discovered may not be resistible; because of massive market power and bundling of products, customers may not be able to exercise the choice to switch platforms or software.<sup>88</sup>

The final option, direct government regulation, is the best solution, but also the one least likely to be implemented today given the Administration's stated philosophy. This is a mistake. Government regulation of code is far more transparent than the two other alternatives, and can generate effective architecture that provides security and builds

---

88. If discovered, of course, market pressures could force the removal of technical measures. See, e.g., Anick Jesdanun, *Privacy Protection Jumps to Fore at Doubleclick; Tries To Restore Image After Lapses*, CHI. TRIB., Apr. 23, 2001, § 2, at 5 (describing the public outcry against one company for measures that failed to adequately protect privacy). A similar pressure would be brought to bear on government regulation of code, and, due to FOIA and other sunshine features of our democratic system, that pressure is likely to occur earlier than it would under private ordering.

community.<sup>89</sup> After all, the libertarian impulse in cyberspace ultimately will prove ineffectual because it depends on protocols of trust. When cybercriminals erode that trust, the openness that has characterized the Net will come under attack. The result will be greater amounts of private control over the Net, and a concomitant reduction in connectivity. Just as laws against street crime provide a baseline of safety, so too do laws against computer crime. Public enforcement of these laws is necessary to encourage people to use the Net and to reveal private information in a secure setting, and thereby unleash the positive force of network effects.<sup>90</sup>

Accordingly, the American government must not shy away from regulating code out of transparency concerns. If open source platforms are more secure, the government should be encouraging their development through government procurement strategies (instead of continuing to prop up the closed Microsoft system through its purchases).<sup>91</sup> If digital anonymity is a serious contributor to crime, government should be thinking about modifications to the architecture of the Net to minimize it. What it should not do is simply pretend that the market will solve the cybercrime problem. The market doesn't solve our realspace crime problems; after all, in many of those areas left to market forces, crime spirals out of control and the social network frays as individuals barricade themselves inside their residences.<sup>92</sup>

---

89. Members of Congress could cut secret deals with industry as well, but two facts suggest that this method will be more transparent than will private agreements between the White House and industry. First, congressional hearings by default are open, whereas White House meetings by default are closed. Second, the structure of Congress, containing a large number of individuals each with a different constituency to please, makes it unlikely that a secret can be kept in that body. See Saikrishna B. Prakash & Michael D. Ramsey, *The Executive Power over Foreign Affairs*, 111 YALE L.J. 231, 278 & n.206 (2001).

90. As a Cornell Commission Report on a worm famously launched by one of its students states, a "community of scholars should not have to build walls as high as the sky to protect a reasonable expectation of privacy, particularly when such walls will equally impede the free flow of information." Ted Eisenberg et al., *The Cornell Commission: On Morris and the Worm*, in *COMPUTERS UNDER ATTACK* 253, 258 (Peter J. Denning ed., 1990).

91. The National Security Agency developed a version of secure Linux but has recently decided not to continue working on the project. See Robert Lemos, *Linux Makes a Run for Government*, CNET NEWS.COM, Aug. 16, 2002, at <http://news.com.com/2100-1001-950083.html>. A recent report prepared for the Defense Department similarly suggests that the government will become increasingly reliant on open source software. See MITRE CORP., *USE OF FREE SOURCE AND OPEN-SOURCE SOFTWARE (FOSS) IN THE U.S. DEPARTMENT OF DEFENSE* (2003), at <http://www.egovos.org/pdf/dodfoss.pdf>.

92. Similarly, we do not leave airplane security to the demands of the market and say that the federal government should trust individual airlines, with all of their economic variability, to do the job adequately. The government should ensure the security of the Net, both through policing and through robust free security software, because doing so will help the network expand its value to everyone. While the White House Strategy does mention some forms of digital architecture that may improve cybersecurity, such as Internet Protocol 6, it offers no plan on how to create and implement such changes, apart from simply convening a Department of Commerce "task force." WHITE HOUSE, *supra* note 7, at 30.

Instead of a tepid government approach to a major security problem, there is a different path. Obviously, part of such a strategy includes vibrant law enforcement, and law enforcement targeted not only at cyberterrorism, but also at identity theft, corporate hacking, privacy violations, credit card fraud, cyberstalking, and the gamut of crimes that scare people from using the Net. But in addition, it includes methods that encourage the development of better private and public architectural solutions. In my realspace architecture work, I detailed systems of regulation that could bring about such crime control through design. Consider five of them: (1) using building codes to mandate crime-prevention methods, (2) modifying default rules in contract (such as those between landlord and tenant) to penalize those who are in a better position to make design improvements but fail to do so, (3) employing tax expenditures to subsidize architectural investments, (4) requiring "Crime Impact Statements" when developers build housing or other significant projects, and (5) coupling tort liability for poor design with safe harbors for designing more secure products.<sup>93</sup>

Similar methods are available in cyberspace. For example, the federal government could use the equivalent of building codes to require proper design and performance standards for software. Performance standards, which do not specify a particular way of preventing crime, might prove particularly helpful given the context-dependent properties of digital architecture. The government could alter default rules for warranties in contract in order to provide incentives for software manufacturers to pay greater attention to cybersecurity.<sup>94</sup> It could also use tax expenditures and government-subsidized research to study cybersecurity, and could even contemplate a "Center for Digital Disease Control," based on the realspace CDC model. It could use its procurement power—estimated at more than \$50 billion a year on information technology<sup>95</sup>—to influence marketplace development of security products.<sup>96</sup> Indeed, when President Clinton

---

93. See Katyal, *supra* note 2, at 1102-08 (discussing building codes); *id.* at 1116-19 (discussing contractual regulation); *id.* at 1098-100 (discussing tax expenditures and procurement); *id.* at 1101-02 (discussing Crime Impact Statements); *id.* at 1112-16 (discussing tort suits).

94. By contrast, the Uniform Computer Information Transactions Act (UCITA) would permit software companies to disclaim liability for shoddy products. See UNIFORM COMPUTER INFORMATION TRANSACTIONS ACT: DRAFT (1999), at <http://www.law.upenn.edu/blil/ulc/ucita/citaam99.htm>; see also Barbara Simons, *Inside Risks: Shrink-Wrapping Our Rights*, 43 COMM. ACM 122 (2000), at <http://www.acm.org/usacm/copyright/ucita.cacm.htm> ("UCITA will remove any legal incentives to develop trustworthy software, because there need be no liability.").

95. OFFICE OF INFO. & REGULATORY AFFAIRS, OFFICE OF MGMT. & BUDGET, REPORT ON INFORMATION TECHNOLOGY SPENDING FOR THE FEDERAL GOVERNMENT FOR FISCAL YEARS 2000, 2001, AND 2002 (2001), at <http://www.whitehouse.gov/omb/inforeg/final53.xls> (giving estimated figures for 2002).

96. Ranum notes:

Rather than standardizing on a single enterprise firewall product, anti-virus product, and desktop firewall, federal computing is a mish-mash of incompatible solutions. If the feds wanted to make the single greatest impact possible on CyberSecurity they'd do

mandated that federal computers meet Energy Star requirements, it helped usher in an era of environment-friendly computing.<sup>97</sup>

The Crime Impact Statement, modeled after the Environmental Impact Statement required under federal law, is a realspace device that encourages developers to think about the consequences of their design on crime rates. In cyberspace, government could require companies that release major products, such as software platforms, to provide a similar impact statement, perhaps on a confidential basis. Statements could discuss some of the key security features of the software, such as its encryption and password protocols, certify that the trapdoors that programmers use to quickly make changes to the program have been removed, and explain how the program should be configured to prevent attack. Requiring statements alone will make it more likely that developers will ship their software in secure default modes. Because the impact statement does not mandate any particular form of architectural design, it couples the flexibility of a market-based solution with the government's ability to serve as a catalyst for reform.

Another mechanism that harnesses the benefits of the market concerns insurance companies. In realspace, insurance companies profit through exploiting downward cost curves. They calculate premiums on the chance that a particular calamity will occur, such as robbery, and then educate their customers about methods that reduce the likelihood of the calamity occurring. This education gives the customer valuable information and simultaneously reduces the insurance company's expected payouts.<sup>98</sup> Yet again, the parallels with digital code are striking, for government could use techniques to spur the use of insurance companies as educators and evaluators of cybersecurity practices.<sup>99</sup> Insurance companies are already

---

what *any* FORTUNE 500 company does: standardize on a few good products and then use their status as an important customer (more precisely, a large source of revenue) to demand the features it wants and needs.

Ranum, *supra* note 79. The White House Strategy does, fortunately, mention the use of this power. See WHITE HOUSE, *supra* note 7, at 43 ("The federal government's procurement practices will be used to help promote cybersecurity. For example, federal agencies should become early adopters of new, more secure systems and protocols where appropriate."). But the Strategy backed away from any security requirements on procurement, and "[w]ithout that requirement in the cybersecurity plan, critics questioned how the government could truly lead by example." Aaron Davis, *Internet Security Strategy Released*, MERCURY NEWS, Feb. 15, 2003, at <http://www.bayarea.com/mlid/mercurynews/business/5189215.htm>; see also Lee, *supra* note 83 (observing that the Strategy "falls short of using its [government] buying power to nudge businesses to improve their security standards").

97. See CLIMATE PROT. DIV., U.S. ENVTL. PROT. AGENCY, THE POWER TO MAKE A DIFFERENCE: ENERGY STAR AND OTHER PARTNERSHIP PROGRAMS 12 tbl.3 (2000), at <http://www.epa.gov/appdstar/pdf/cpdann99.pdf>.

98. See Katyal, *supra* note 2, at 1091, 1114 (discussing the power of insurance companies as educators).

99. See FOURTH ANNUAL REPORT, *supra* note 79, at 82 (discussing how insurance changes and auditing practices to "reward good security practices" can serve to increase the market value of security). One insurance company, J.S. Wurzlcr, charges a higher premium to companies using Windows NT than to those using Unix or Linux because of the higher risk of loss and payouts.

providing "hacker insurance," and some of them have asked the government to set cybersecurity benchmark standards.<sup>100</sup> Either such standards or the adoption of modest common-law tort liability for poor design can induce insurance companies to play an educational role.<sup>101</sup> If the price of using a proprietary web server doubled due to hacker insurance, for example, businesses would quickly switch products. And apart from the price, when insurance companies issue such policies, it will prompt those companies to teach their clients about good cybersecurity practices. Exploiting the educational power of insurance companies is one way to bolster computer security without the heavy hand of government design codes. But it, like so many other solutions, has been ignored due to a preconceived faith in the market as the solution to the cybercrime problem.

## II. CONCLUSION

Crime of any sort, whether a mugging, terrorist incident, or computer hacking, prompts not only legal but architectural responses as well. Yet we as Americans think far too much about the law, and not enough about design.<sup>102</sup> This Essay has continued my argument that to prevent crime, governments and citizens must devote far more attention to the positive and negative consequences of architecture. We should carefully avoid reflexive responses to crime like gated communities and their digital equivalents, for they often do little to prevent criminal acts and spur an atmosphere of fear. Unfortunately, the government today has adopted a stunted view of law enforcement in cyberspace, a view that threatens so much of what is valuable about the Net by encouraging private closure. By reverse-engineering the realspace analysis of architecture back to cyberspace, a better appreciation for how to regulate cyberspace is gained and new strategies for government regulation emerge.

---

See Erich Luenig, *Windows Users Pay for Hacker Insurance*, CNET NEWS.COM, May 29, 2001, at <http://news.com.com/2100-1001-258392.html>; NIC PEELING & JULIAN SATCHELL, ANALYSIS OF THE IMPACT OF OPEN SOURCE SOFTWARE § 2.11 (2001), at [http://www.govtalk.gov.uk/documents/QinetiQ\\_OSS\\_rep.pdf](http://www.govtalk.gov.uk/documents/QinetiQ_OSS_rep.pdf) (stating that Wurzler charges a twenty-five percent higher premium for companies using Microsoft Windows).

100. Interview by Brian Krebs with Alan Paller, Director of Research for the SANS Institute (Sept. 18, 2002), at [http://www.washingtonpost.com/wp-srv/liveline/02/special/sp\\_technews\\_paller091802.htm](http://www.washingtonpost.com/wp-srv/liveline/02/special/sp_technews_paller091802.htm) (reporting requests by the insurance industry to the government, and stating that "[i]ndustry is thirsty for benchmarks. Just delivering them will have a profound effect. And very soon after they are delivered insurance companies and consumers will simply say no to organizations that do not meet minimum standards of care reflected in the benchmarks.").

101. See Katyal, *supra* note 3, at 1092-94 (discussing conditions under which tort liability coupled with safe harbors is better than government-issued benchmark standards).

102. But see Lawrence Lessig & Paul Resnick, *Zoning Speech on the Internet: A Legal and Technical Model*, 98 MICH. L. REV. 395 (1999) (outlining architectural mechanisms to prevent pornography and spam on the Net).

Besides the dangers of private architectural solutions, an understanding of realspace design informs other aspects of cyberspace. We have seen, for instance, how an architect treats context as central. For this reason, the emergence of computer crime as a major variable can invert some of the thinking by leading law professors. To take just three examples, Larry Lessig has argued powerfully in favor of e2e, Yochai Benkler in favor of open source software and peers, and Julie Cohen in favor of anonymity.<sup>103</sup> But, respectively, inoculation against viruses might be best accomplished through scanning at levels higher than end points, some types of open source software are particularly vulnerable to hacking because they cannot harness natural surveillance, and anonymity can be a dangerous inducement to commit crimes on the Net.

In each of these areas, there are trade-offs to be made. But without some serious government attention to these problems and a strong recognition of the need for contextual solutions, the overall security and utility of the Net will be compromised. No matter how vigorous the law enforcement, or how robust the inducement for public architecture, the public sector alone will, of course, not solve the crime problem. But, through careful planning and incentives that leverage the power of the market, it can help develop the types of digital bricks and mortar that can both reduce crime and build community.

---

103. See *supra* notes 6, 46-47 (discussing Lessig's e2e claims); *supra* note 57 (discussing Benkler's views on peer production); Julie E. Cohen, *A Right To Read Anonymously*, 28 CONN. L. REV. 981 (1996).

\*\*\*