



Internet and Computer Crime: System Architecture as Crime Control



INTRODUCTION

New technologies provide new opportunities and new potentials. Technological developments, however, do not determine human fates; rather, they change the constraints within which people act. [FN 1] The global reach of the Internet, the low marginal cost of online activity, and the relative anonymity of users have changed the balance of forces that have previously served to keep in check certain undesirable behaviors in the physical world.

These characteristics of "cyberspace" [FN 2] have lowered the cost of perpetrating undesirable behavior by eliminating certain barriers to entry, lowering transaction costs and reducing the probability of getting caught. [FN 3] In addition, these characteristics make traditional enforcement strategies, particularly identifying and apprehending perpetrators after they commit online crime, both less effective and more expensive. [FN 4]

At the same time, however, other characteristics of cyberspace provide new opportunities to control illegal acts. Unlike in the physical world, in cyberspace certain readily identifiable third parties – Internet service providers ("ISPs") [FN 5] – have exclusive technical control over the infrastructure through which most illegal online behavior is carried out.

1 Robert McClintock and K. A. Taipale, "Educating America for the 21st Century," New York: Institute for Learning Technologies, Columbia University (Circulation Draft, Version 2.1, September 1994).

2 We use "cyberspace" to mean the electronic medium of computer networks, in which online communications takes place, the system of interconnected "switches and pipes" that comprise the digital, packet based communications network. See *Reno v. ACLU*, 521 U.S. 844, 851 (1997):

"All of these methods can be used to transmit text; most can transmit sound, pictures, and moving video images. Taken together, these tools constitute a unique medium—known to its users as "cyberspace"—located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet."

The term "cyberspace" is credited to William Gibson, "Neuromancer", New York: Ace Books, Reissue edition (1995, 1984) p. 51:

"Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts A graphical representation of data abstracted from the banks of every computer in the human system."

3 See Neal Kumar Katyal, "Criminal Law in Cyberspace," 149 U. Penn. L. Rev. 1003, 1006 (2001) and Michael E. O'Neill, "Old Crimes in New Bottles: Sanctioning Cybercrime," 9 George Mason L. Rev. 237, 277 (2000).

4 Katyal, *ibid.*, and O'Neill, *ibid.* at 275.

5 ISPs provide a variety of network related services, for example, network access, hosting services or online content services. For our purposes, unless otherwise stated, we use ISP to include all types of services. For a statutory definition of "service provider", see 17 U.S.C. §512(k) and see ALS Scan

Thus, one strategy for controlling online behavior is to impose some responsibility on such third parties in order to control user misconduct before illegal acts are committed or to help identify and apprehend criminals after the fact. In other cases, the same logic can be applied to second parties – that is, victims of online crime who control the systems on which crime is committed – and legal responsibility to encourage optimal victim behavior can also be employed.

The purpose of this paper is to briefly examine the rationale and opportunity for online crime control through system architecture by imposing certain technical responsibilities on victims and implicated third parties.

In particular, we examine affirmative obligations for ISPs to report criminal activity and retain data, and for victims to employ some minimal level of technical protective measures. In addition, we briefly discuss tort-based mechanisms to encourage both victims and third parties to adopt reasonable technical measures to prevent illegal behavior.



OVERVIEW

Although the Internet has been with us for more than two decades now [FN 6], the threshold question still seems to be [FN 7] whether cyberspace is a "unique and wholly new" thing [FN 8] – so different as to require new laws or doctrine, maybe even its own transnational jurisprudence [FN 9] – or that, although the technology is new, the legal problems are familiar and existing legal doctrine and analysis can easily accommodate the new developments. [FN 10] As with all such questions, neither answer is entirely correct.

Determining where old doctrines can be extended to new circumstance or where new doctrines are required to fill interstitial gaps in old theory requires understanding how, and to what extent,

v. RemarQ Communities, 239 F.3rd 619, 623 (4th Cir. 2001) (the DMCA "defines service provider broadly").

- 6 Although ARPANET, the predecessor to what we now know as the "Internet" can trace its origins to the 1960s, it was January 1, 1983 when the TCP/IP protocol was adopted as the host protocol for ARPANET. See generally, Internet Society, "All About the Internet: Internet Histories," at <http://www.isoc.org/internet/history/>.
- 7 See, for example, Internet and Computer Crimes Seminar, "Syllabus: Week 1: Introduction to Computer Crime," Columbia Law School (Spring 2003) ("Should federal and state criminal law extend to the bits and bytes of the Internet, or should the Internet be governed by its own rules?").
- 8 "The Internet is a unique and wholly new medium of worldwide human communication." *Reno v. ACLU*, 521 U.S. 844, 850 (1996)
- 9 See, for example, David R. Johnson and David Post, "Law and Borders: The Rise of Law in Cyberspace," 48 *Stanford L. Rev.* 1357 (1996) (stating the case for cyberspace sovereignty). See generally Llewellyn J. Gibbons, "No Regulation, Government Regulation, or Self-regulation: Social Enforcement or Social Contracting for Governance in Cyberspace," 6 *Cornell J. Law and Public Policy* 475 (1997).
- 10 See, for example, Jack L. Goldsmith, "Against Cyberanarchy," 65 *U. Chicago L. Rev.* 1199 (1998) and Christopher M. Kelly, "The Cyberspace Separatism Fallacy: BOOK REVIEW: Curtis Karnow, *Future Codes: Essays in Advanced Computer Technology and the Law*," 34 *Texas Int'l. L. J.* 413 (1999). And see Lawrence Lessig, "The Zones of Cyberspace," 48 *Stanford L. Rev.* 1403, 1407-1410 (1996) (criticizing Johnson and Post, *supra* footnote 9).

the particular characteristics of digital mediation affect opportunity costs for committing, discovering and controlling illegal online behaviors. [FN 11]

Although a full examination of these issues is beyond the scope of this paper, the central features that make cyberspace different for the criminal – in particular the low perpetration costs, difficulty of detection, and ease of escape – also argue strongly for requiring victim precautions and third party participation in controlling online crime.



CYBERCRIME

The United States Department of Justice defines "computer crime" broadly as "any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation or prosecution." [FN 12] Others have focused on those crimes "where knowledge of a computer system is essential to commit the crime" [FN 13], or simply where there is "use of a computer to facilitate or carry out a criminal offense." [FN 14]

For our purposes in discussing system architecture as a method for cybercrime control we adopt a slight variation. Here we are concerned with illegal behavior where the infrastructure that enables the commission of the act is in the direct or indirect control of the victim or a third party. [FN 15] In general, this would include any illegal acts committed "in or through cyberspace" – that is, any criminal act that uses network access or infrastructure.



CRIME CONTROL IN CYBERSPACE

Traditional notions of crime control, particularly among lawyers, is to focus on legal rules proscribing illegal behavior and law enforcement discovering, catching and prosecuting perpetrators after they commit crimes. [FN 16] Crime deterrence under this approach focuses in the main on first party (perpetrator) strategies – raising perpetration costs and legal risks – to discourage criminal acts. [FN 17]

To the extent that cybercrime is more difficult to catch, traditional doctrine would increase sentencing in order to compensate for lower probability in order to maintain the same deterrent

11 See generally O'Neill, *supra* footnote 3.

12 National Institute of Justice, U. S. Dept. of Justice, "Computer Crime: Criminal Justice Manual 1, 2 (1989)

13 Jo-Ann Adams, "Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet," 12 *Computer and High Technology L. J.* 403, 409 (1996).

14 Katyal, *supra* footnote 3, at 1013.

15 This would exclude, for example, the use of a standalone computer as an instrumentality to commit a crime such as counterfeiting currency or production of fraudulent documents.

16 See Neal Kumar Katyal, "Architecture as Crime Control," 111 *Yale L. J.* 1039, 1047 (2002) (Commenting on the traditional approach. Katyal then goes on to discuss the use of physical architecture – structural and space design – as an effective alternative form of crime control. Design mechanisms discussed include: (1) creating opportunities for surveillance, (2) instilling a sense of territoriality, (3) building community and avoiding isolation, and (4) protecting targets.)

17 See generally Gary S. Becker, "Crime and Punishment: An Economic Approach," 76 *J. Pol. Econ.* 169 (1968).

effect. [FN 18] Thus, increasing statutory sentences as well as sentence enhancements or upward departures under sentencing guidelines would be rational first party strategies for controlling cybercrime under such theories. [FN 19]

An unfortunate side effect of this approach for cybercrime, however, is the severe criminalization of certain behaviors that many feel innocuous, for example, non-malicious systems intrusions. [FN 20] The consequence is a general undermining of the moral authority of law, as these punishments seem out of proportion to the particular illegal act. [FN 21]

Conventional approaches to law enforcement are not the only potential solutions, however, particularly with respect to cybercrime where victims and third parties have significant control over the infrastructure in which the criminal operates. In such cases, private parties can develop and implement technological solutions that make criminal activity more expensive to commit and easier to discover and control. [FN 22] And, in many cases, these parties can do so at much lower overall social cost than relying only on government enforcement. [FN 23]

For example, if a simple anti-virus program can prevent a particular harm, then requiring potential victims to use such preventative software is significantly cheaper than relying on government enforcement of legal sanctions. Likewise, third party monitoring of traffic flows for particular vulnerabilities or suspect behavior can be accomplished at significantly lower overall cost than ex post prosecution.

In such circumstance, the relationship between public and private power is altered and the defining question becomes how and under what circumstances such private power should be used or encouraged to supplement public power in the context of law enforcement. [FN 24] And,

-
- 18 Becker, *supra* footnote 17, at 179-180. See generally, Cesare Beccaria, "On Crimes and Punishments," David Young, trans., Indianapolis: Hackett Pub. Co. (1986, 1764).
- 19 See O'Neill, *supra* footnote 3, at 270-273. And see, for example, United States Sentencing Guidelines Manual ("USSG") §3B1.3 supporting a two-level "special skills" enhancement for computer fraud. See *United States v. Peterson*, 98 F.3d 502, 506-507 (9CA 1996) (holding that computer programming skills were "special skills" subject to enhancement under the guidelines).
- 20 See Catherine T. Clarke, "From CrimINet to Cyber-Perp: Toward an Inclusive Approach to Policing the Evolving Criminal Mens Rea on the Internet," 75 Oregon L. Rev. 191, 207 (1996) ("In this Article, traditional hackers are not considered to be law breakers; their mens rea is presumed innocent."). Cf. Mary M. Calkins, "They Shoot Trojan Horses, Don't They? An Economic Analysis of Anti-Hacking Regulatory Models," 89 Georgetown L. J. 171, 186 (2000) ("However, even benign hackers – those ... without [bad intent] can create [harms] that equal or exceed those created by malicious hackers.").
- 21 See "Chapter Six: Of the Proportion between Crimes and Punishments," in Beccaria, *supra* footnote 16. And, see Catherine T. Clarke, *supra* footnote 18 (critiquing current law enforcement approaches to cybercrime along these lines) and O'Neill, *supra* footnote 3, at 274 ("Significant constraints may affect penalty levels, however. We are unlikely to threaten teenaged hackers with lengthy prison terms for a variety of constitutional, humanitarian, and other political concerns."). Obviously, prosecutorial discretion has significant impact here as well.
- 22 Katyal, *supra* footnote 3, at 1094-1095 and O'Neill, *supra* footnote 3, at 265-288.
- 23 Katyal, *supra* footnote 3, at 1077.
- 24 See Lawrence Lessig, "Code and Other Laws of Cyberspace," New York: Basic Books (1999) at 99 ("... government has a range of tools that it uses to regulate. Cyberspace expands that range. The code of cyberspace is becoming just another tool of state regulation."). And see Katyal, *supra* footnote 3, at 1077-1107 and O'Neill, *supra* footnote 3, at 274-277 and 286.

to the extent that private power is enlisted to achieve public policy objectives, how can it be constrained to provide adequate protections for individuals. [FN 25]

Orthodox notions of law enforcement are premised on an Austinian [FN 26] conception of state power based on an implicit formal triangle of sovereign, citizen and right. However, postmodern theorists, beginning with Michel Foucault, view power through the more subtle informal mechanisms of coercion organized around the concepts of "surveillance and discipline", rather than power-as-sovereign. [FN 27] Foucault and commentators of like mind [FN 28], use this observation to critique the existing power structure, particularly by pointing out how traditional notions of power-as-sovereign are used to conceal the actual procedures (and thus the resulting "violence") of power in society.

We seek here, instead, to appropriate this insight to further underpin ascription of legal responsibility to third party service providers who have exclusive technical control over the mechanisms of identity (cf. surveillance) and access (cf. discipline).



CODE IS LAW

Lawrence Lessig argues that code is law. [FN 29] What Lessig means, of course, is that in cyberspace the opportunities and potentials for behavior (good and bad) are controlled by the software and hardware that determine the characteristics of the environment in which behavior can occur. [FN 30]

In cyberspace, business and technical decisions made by ISPs and victims in designing and implementing their systems [FN 31] determines what behaviors, hence what crimes, can occur and how such acts can be detected and controlled. [FN 32]

25 See Michael Lee, et al., "Electronic Commerce, Hackers, and the Search for Legitimacy: A Regulatory Proposal," 14 Berkeley Tech. L. J. 839, 872-878 (1999) and Lessig, *supra* footnote 24, at 222-230.

26 John Austin, "The Province of Jurisprudence Determined," Amherst, NY: Prometheus Books (2000, 1832). Austin defined "positive law" as that decreed by a sovereign or government.

27 Michel Foucault, "Discipline and Punish: The Birth of the Prison," New York: Vintage Books (1979).

28 See James Boyle, "Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors," 66 U. Cin. L. Rev. 177, 186 (1997).

29 See "Code is Law," pp. 3-8 in Lawrence Lessig, "Code and other Laws of Cyberspace," New York: Basic Books (1999) and p. 89 ("[code] constitute[s] a set of constraints on how you behave. ... The code or ... architecture ... constrain[s] some behavior by making other behavior possible, or impossible.").

30 *Ibid.* Although "code is law" is generally credited to Lessig (see Lessig, *supra* footnote 13, at 6) his work builds upon that of William J. Mitchell who wrote "[o]ut there on the electronic frontier, code is the law." Mitchell, "City of Bits: Space, Place and the Infobahn," Cambridge: MIT Press (1995) at 111. See also, Joel R. Reidenberg, "Lex Informatica: The Formulation of Information Policy Rules Through Technology," 76 Texas L. Rev. 553, 554-555 (1998) and James Boyle, "Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors," 66 U. Cin. L. Rev. 177 (1997). See also Lawrence Lessig, "Reading the Constitution in Cyberspace," 45 Emory L. J. 869, 896-897 (1996).

31 For example, even absent any additional service layer, technical and business decisions for 'simple access' services exert significant control over potential online behavior. Decisions regarding the amount and availability of a/symmetric bandwidth, static versus dynamic IP addressing, and port filtering or other firewall control significantly enable or constrain individual user's ability to engage in

Further, in the case of ISPs, it is the provision of network service itself that gives performative [FN 33] effect to the harmful conduct. Thus, under a constitutive paradigm of responsibility [FN 34], an affirmative duty to control behavior enabled through such service is assignable. [FN 35]

illegal activity. So too, decisions whether and how to use encryption, authentication, access control and logging have significant impact on the cost of perpetration, the difficulty of detection and the ease of escape.

32 The fact that any particular hacker could or could not overcome any technical means to control specific behaviors is not relevant to the general notion of using system architecture to control behavior any more than the observation that "a locksmith can pick any lock" is to the relevance of locks in crime prevention. See Lawrence Lessig, "Constitution in Cyberspace," 45 *Emory L. J.* 869, 896 n. 80 (1996), cited in Lee, *supra* footnote 25, at 843 n. 17.

33 "Performative" is the term used by John L. Austin in "How to Do Things with Words," Cambridge: Harvard University Press (1962) to distinguish speech-acts that do things from those that just say things. See also John R. Searle, "Speech Acts: An Essay in the Philosophy of Language," New York: Cambridge University Press (Reprint edition 1999, 1969)

Summarizing Austin's work here is beyond the scope of this paper, however, for our purposes, the salient points about performative speech-acts are that they are contextual. That is, their ability to perform ("do things") is dependent on the context in which they occur (for example, shouting "fire" in the woods versus shouting it in a crowded theatre is fundamentally different, and is treated differently as a matter of law, because of the performative effect from context).

So, in cyberspace, many illegal behaviors could not occur "but for" the provision of services or infrastructure by third parties (or could be easily detected or traced "but for" certain technical decisions by providers). Thus, society may require some minimal level of responsibility to control illegal acts enabled through the provision of services on the part of the providers of such service.

This is no different than in realspace where we impose certain technical or standards requirements on manufacturers before allowing their products into the stream of commerce or where we put certain duties on third party service providers, for example, certain minimum care standards for professionals. Even in the context of the First Amendment we burden protected speakers, for example, holding newspapers liable for "reckless disregard" of truth in defamation cases involving public figures.

In cyberspace, where almost every business or technical decision defines system architecture (see footnote 31 *supra*) and thus has significant impact on both what behaviors are enabled and the mechanisms of "surveillance and discipline" available (see text accompanying footnotes 26-28 *supra*), imposing a concomitant responsibility to include legitimate law enforcement requirements in such decision making seems appropriate. This is particularly so where, as with victims and ISPs in the context of cybercrime, private action can accomplish control at significantly lower overall costs. (But see the text accompanying footnote 43 *infra* discussing problems of over-deterrence and accountability.).

34 Meir Dan-Cohen, "Harmful Thoughts: Essays on Law, Self and Morality," Princeton: Princeton University Press (2002) at 199-241. It is beyond the scope of this paper to fully summarize Dan-Cohen's work, however, constitutive responsibility for our purposes here can be analogized to the third party responsibility that inures to a tavern owner or bartender for the subsequent actions of a drunk driver. See *ibid.* at 221-224.

35 Others, of course, would argue the contrapose – that merely supplying the infrastructure in which criminal behavior can occur should not be subject to liability or incur any duty of care. This is the "guns don't kill, people do" argument. However much this argument appeals to the libertarians, whether in realspace or cyberspace, it is not reflective of the reality of legal responsibility.

Constitutive responsibility is ascribed throughout the legal system, for example, through the doctrines of vicarious, contributory and negligent liability regimes in tort, and in criminal law through use of the "reckless" standard for certain contributory acts. Further, under the doctrines of conspiracy and

To summarize, in cyberspace code is a primary mechanism of control. Because of technical characteristics of network infrastructure, direct control over code is in the hands of private parties – ISPs, who provide access and control identity, and victims, whose systems are the target of attack. In each case, these private parties are in a position to supplement state action strategies for controlling, detecting and investigating cybercrime, more effectively and at lower cost than relying solely on governmental action. [FN 36]



THIRD PARTY STRATEGIES

Reinier Kraakman identified three primary strategies for third party involvement in law enforcement – monitoring conduct, removing offenders and whistle-blowing. [FN 37] Building on these three strategies, Neal Katyal suggests a fourth and fifth – architecture (code) and investigative support. [FN 38]

Both Katyal and Michael O'Neill suggest that ISPs could monitor web traffic and scan web content for potentially illegal conduct. [FN 39] Obviously, such activity would raise issues regarding online privacy and free expression. Further, they suggest that ISPs could remove "risky" subscribers from the network altogether. This activity may raise issues of due process. In either case – monitoring or "bouncing" – any state involvement, for instance by directly requiring ISPs to engage in such acts, would raise serious constitutional and statutory questions. It is beyond the scope of this paper to address these. [FN 40]

Instead, we suggest that whistle-blowing and investigative support are effective strategies that are already being imposed in certain circumstances and could be expanded without requiring significant system re-architecture or resolution of complex constitutional questions.

Whistle-blowing, that is, the reporting of illegal conduct, is already required in cases of child pornography [FN 41] and could be required more broadly, that is, where the ISP has actual or

accomplice liability, we regularly ascribe criminal liability for the acts of others. It is beyond the scope of this paper to fully develop these arguments. See K. A. Taipale, "Secondary Liability on the Internet: Towards a Performative Standard for Constitutive Responsibility," New York: Center for Advanced Studies in Science and Technology Policy (2003).

36 See O'Neill, *supra* footnote 3, at 274-277.

37 Reinier H. Kraakman, "Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy," 2 J. L. Econ. & Org. 53 (1986). And, see Katyal, *supra* footnote 3, at 1094-1098 and O'Neill, *supra* footnote 3, at 282-285 ("chaperoning, bouncing and whistle-blowing").

38 Katyal, *supra* footnote 3, at 1097. And, see Katyal, *supra* footnote 16 (discussing how physical architecture can be used as an alternative crime prevention strategy in realspace).

39 Katyal, *supra* footnote 3, at 1096, and O'Neill, *supra* footnote 3, at 283.

40 It is not our contention, however, that such activities are necessarily unconstitutional. Quite the contrary, we believe that narrowly circumscribed monitoring strategies, particularly traffic analysis, are not only constitutionally permissible, but also socially desirable and will be increasingly employed as the network is further developed. We leave discussion of these issues to a future paper in which we may discuss in greater detail how these strategies could be employed. See also Title III, 18 U.S.C. §2510 et seq. and 18 U.S.C. §3121 et seq. ("wiretap" and "pen/trap" statutes).

41 Under 42 U.S.C. §13032 (Lexis 2003) ISPs currently have a duty to report incidents of child pornography that they become aware of. §130329(c) provides civil immunity to ISPs for good faith reporting under this section, and §13032(e) provides that "monitoring is not required".

imputed knowledge of the illegality they should be under a duty to report such conduct to the appropriate authorities. [FN 42]

Imposition of such a knowledge-contingent standard avoids certain problems of over-deterrence [FN 43], however, such standards tend to encourage ISPs to ignore user misconduct. [FN 44] Thus, some commentators have argued that knowledge-contingent standards should only be introduced in conjunction with monitoring regulations. [FN 45] Under monitoring regulations, lawmakers set the optimal level of monitoring that is required by ISPs. [FN 46]

However, in addition to the constitutional questions raised above, any such monitoring-regulation regime is likely to suffer from (i) inflexibility in that such a regime imposes a uniform standard on performance regardless of particular conditions, costs or relative benefits in a particular situation (or for a specific service), (ii) a tendency to establish a floor (or ceiling) for performance and "lock in" a set level of performance, and (iii) discouragement of technical innovation (no incentive to innovate beyond existing standards). [FN 47]

For these reasons, legislative standard setting for monitoring online conduct is particularly inappropriate in areas of rapid technical innovation. Any standard for compliance is likely to be obsolete when enacted since it will not take into account innovations in services, monitoring technologies, or user behaviors. [FN 48]

Investigative support is also required in some circumstances, including certain technical infrastructure requirements. For example, under the Communications Assistance for Law Enforcement Act of 1994 ("CALEA") [FN 49] telecommunications carriers are specifically required to enable their infrastructure to support court-ordered government wiretaps. [FN 50] A decision

42 As a start, § 230 of the Communications Decency Act, 47 U.S.C. §230 (2003), should be repealed or amended to overrule *Zeran v. AOL*, 129 F.3d 327 (4CA 1997) (extending immunity to ISPs for defamation even with knowledge). See Paul Ehrlich, "Cyberlaw: Communications Decency Act §230, 17 Berkeley Tech. L. J. 401 (2002). Potential liability for defamation would encourage preventative strategies as discussed below under Tort-based Regimes.

43 Over-deterrence occurs when there is "incentive divergence" between the ISP bearing the cost of enforcement and the user reaping the gain of any conduct. ISPs will tend to eliminate more conduct than optimal if required to monitor or if held responsible for user misconduct. See Assaf Hamdani, "Who's Liable for Cyberwrongs?" 87 Cornell L. Rev. 901, 905 (2002).

44 So-called "willful blindness".

45 Hamdani, *supra* footnote 43, at 936.

46 *Ibid.*, at 933-934. Compare 42 U.S.C. §13032(e), *supra* footnote 41 ("monitoring is not required") and the procedural standards in the Digital Millennium Copyright Act, 17 U.S.C. §512 (LEXIS 2003) (monitoring is not required but once notice is given ISPs must follow DMCA procedures).

47 Any system of legislated technical standards is subject to the same criticisms that are leveled at the current "command-and-control" standard setting regime employed in environmental regulation. See generally the text accompanying footnotes 45-54 in K. A. Taipale, "Information Technology as Agent of Change in Environmental Policy," New York: Center for Advanced Studies in Science and Technology Policy (2002).

48 Not only will new innovation outpace legislative standard setting, but technological innovation will be directed specifically at circumventing such standards much like the development of second generation peer-to-peer networks such as Morpheus and Kazaa were developed to circumvent the "standards" for liability set forth in *Napster*.

49 47 U.S.C. §1001 et seq. (LEXIS 2003).

50 47 U.S.C. §1002(a) (LEXIS 2003).

by the Federal Communications Commission in 1999 [FN 51] adopting technical standards for the implementation of CALEA extended these requirements to include location determination for cell phones. [FN 52]

In addition, federal law currently permits the government to request (by issuing a "data preservation letter") that an ISP take "all necessary steps to preserve records and other evidence in its possession pending issuance of a court order or other process." [FN 53] However, there is no standard for log data or general retention requirement. Thus, law enforcement is subject to the vagaries of individual ISP policies.

However, government could require mandatory data retention for particular kinds of information, for example, traffic logs, for a specified period of time. [FN 54] Any such law requiring ISPs to log and retain data, although anathema to cyber- and civil-libertarians, would seek only to preserve data for lawful use. Law enforcement access to such data or use of such data in a criminal investigation or for other purposes would still have to satisfy constitutional requirements under the Fourth Amendment. In addition, additional mandatory security and privacy protections could be built into any legislation requiring data retention, for example, significant criminal and civil penalties for misuse or unauthorized access. [FN 55]

51 CC Docket No. 97-213, adopted August 31, 1999.

52 In addition, ISPs are required to enable FBI access to their network for Carnivore, an FBI developed "sniffer" program said to be able to discriminate among electronic traffic and capture only that subject to court-ordered wiretap authority. See <http://www.fbi.gov/hq/lab/carnivore/carnivore2.htm>. The USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001) extends pen register and wiretap to Internet communications. The Act revises "line" to encompass a "line or other facility", which could include a cell telephone number or Internet user account or email. See US DOJ, Field Guidance on New Authorities (2001). See generally, Stephen W. Tountas, "Carnivore: Is the Regulation of Wireless Technology a Legally Viable Option to Curtail the Growth of Cybercrime?" 11 Washington Univ. J. L. & Policy 351 (2003).

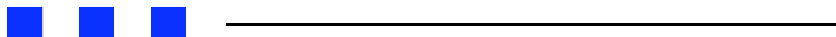
53 18 U.S.C. §2703(f) (2003) (records must be kept for 90 days with a provision for an additional 90 day renewal).

54 See, for example, the European Union Directive on data retention, (Directive 2002/58/EC), permitting each member state to adopt its own data retention policy:

On June 25, 2002 the European Union Council adopted the new Directive on Privacy and Electronic Communications. Under the terms of the new Directive, member states may now pass laws mandating the retention of the traffic and location data of all communications taking place over mobile phones, SMS, landline telephones, faxes, e-mails, chat rooms, the Internet, or any other electronic communication device. The new Directive reverses the 1997 Telecommunications Privacy Directive by explicitly allowing EU countries to compel Internet service providers and telecommunications companies to record, index, and store their subscribers' communications data (Art. 15 (1) of Dir. 2002/58/EC). The data that can be retained includes all data generated by the conveyance of communications on an electronic communications network ("traffic data") as well as data indicating the geographic position of a mobile phone user ("location data") (Art. 2 (b) and (c) of Dir. 2002/58/EC). The contents of communications are not covered by the data retention measures. These requirements can be implemented for purposes varying from national security to criminal investigations and prevention, and prosecution of criminal offences, all without specific judicial authorization.

Initial proposals under the EU directive called for retaining telecommunications traffic data for 12 to 24 months.

55 See, for example, the Electronic Communications Privacy Act of 1986, 18 U.S.C. §2510 et seq. (LEXIS 2003).



SECOND PARTY STRATEGIES – OPTIMIZING VICTIM BEHAVIOR

For some kinds of cybercrime, requiring victim precaution is a socially efficient strategy because the cost of government action to identify, investigate and prosecute the misconduct is too great and the cost of prophylactic action by the victim is quite small. [FN 56] For example, as stated earlier, where simple anti-virus programs could prevent the harm it may be more efficient to require that potential victims adopt such preventative software than to rely on ex post government enforcement of legal sanctions.

Requiring victim precaution is not a novel concept. The common law of burglary provided a direct incentive for property owners to take precautions and to use preventative technologies. [FN 57] For example, it was not considered burglary if the thief entered through an open window or door. According to Blackstone "if a person leaves his door or window open, it is his own folly and negligence; and if a man enters therein, it is no burglary." [FN 58]

The same analysis could be applied to cybercrime, requiring victims to adopt some minimum standards of self-protection. Obviously, determining by regulatory fiat what standard of prevention is mandated and what consequences arise for not meeting the standard entails the same difficulties expressed earlier regarding mandated monitoring requirements. [FN 59]

Among the methods suggested by Katyal for encouraging victim precautions would be to prioritize prosecution where adequate protections were employed. Another method would be to adopt a rule that permitted law enforcement to only open criminal cases in situations where the victim had taken appropriate precautions. This approach is intended to incentivize "police departments [to] behave more like fire departments (focusing more on warning and prevention and less on chasing suspected perpetrators after they commit crimes)." [FN 60]



TORT-BASED REGIME

Some commentators have suggested that a more promising regulatory scheme than public law solutions could be based on tort negligence theory. [FN 61] Tort law provides an efficient means to provide incentives for Internet participants to increase security, deter hacking and provide financial remedy to victims. [FN 62] This approach has been criticized, however, as likely to lead to over-regulation because of the incentive divergence discussed above. [FN 63]

56 See Katyal, *supra* footnote 3, at 1077.

57 See Katyal, *supra* footnote 16, at 1124-1125.

58 Sir William Blackstone, 4 Commentaries on the Laws of England 226 (1765).

59 See text accompanying footnotes 43 through 48 *supra*.

60 Katyal, *supra* footnote 3, at 1007.

61 See David L. Gripman, "The Doors are Locked but the Thieves and Vandals are Still Getting In: A Proposal in Tort to Alleviate Corporate America's Cyber-Crime Problem," 16 J. Marshall J. Comp. & Info. L. 167, 169-170 (1997), cited in Lee, *supra* footnote 25, at 874 n. 152.

62 See Lee, *supra* footnote 25, at 874-877.

63 See Hamdami, *supra* footnote 43, at 905 and Lee, *supra* footnote 25, at 878.

It is beyond the scope of this paper to discuss tort-based regimes in detail [FN 64], however, the following aspect of tort schemes is worth comment. One way that tort liability could potentially bring preventative precautions to cyberspace concerns insurance companies.

Insurance companies profit by exploiting the downward cost curve. They insure against a condition that has some likelihood of occurring and calculate the premium on that basis. They then educate the customer about ways to reduce the likelihood of the insured event occurring, which benefits the potential victim by providing information to avoid loss and benefits the insurer but reducing payouts. [FN 65]

A good example of this result is fire prevention. Fire prevention has largely succeeded because insurance companies stepped in to become fire-prevention educators for building owners, architects and designers. In addition they developed and then lobbied for adoption of fire safety codes and other fire prevention regulation. A similar result might be induced by applying tort liability to cybercrime victims and third party ISPs. [FN 66]



CONCLUSION

This paper has briefly examined the rationale and opportunity for using certain aspects of systems architecture to help control cybercrime. In particular, we have examined several victim and third party strategies for situations in which the potential victim and implicated third parties control the underlying infrastructure through which the crime is enabled. Although the opportunity exists to enlist much more aggressive third party and victim participation, this paper only suggests adoption of incremental expansion of existing approaches to require third parties to report crime and improve data retention, and for victims to adopt minimal protective measures. [FN 67]

This paper should be considered a preliminary research agenda rather than as a definitive statement on these issues.

64 However, see generally, Taipale, *supra* footnote 35.

65 See Katyal, *supra* footnote 15, at 1114.

66 *Ibid.*

67 More aggressive strategies might include affirmative duties for third parties to monitor and prevent behavior, and for victims to engage in certain "vigilante" self-help strategies. See O'Neill, *supra* footnote 3, at 278-281 suggesting that retaliatory countermeasures by victims should be encouraged.