NO COP ON THE BEAT: UNDERENFORCEMENT IN E-COMMERCE AND CYBERCRIME

PETER SWIRE*

INTRODUCTION

This essay emerges from my ongoing research about how computers and the Internet change the nature of consumer protection law.[1] The

* C. William O'Neill Professor of Law, Moritz College of Law of The Ohio State University, and Senior Fellow, Center for American Progress. My thanks to Brian Beauchamp and Joseph Buoni for their research assistance. My thanks as well to comments by Scott Charney and other participants at the Silicon Flatirons Conference.

1. PETER P. SWIRE, CTR. FOR AM. PROGRESS, THE INTERNET AND THE FUTURE OF CONSUMER PROTECTION (2006), http://www.americanprogress.org/kf/swire_consumer_protection_report.pdf; Peter P. Swire, *Consumers as Producers* (forthcoming 2009), *available at* http://ssrn.com/abstract=1137486; Peter P. Swire, *Elephants and Mice Revisited: Law and Choice of Law on the Internet*, 153 U. PA. L. REV. 1975 (2005) [hereinafter *Elephants and Mice Revisited*]; Peter P. Swire, *Trustwrap: The Importance of Legal Rules for Electronic Commerce and Internet Privacy*, 54 HASTINGS L.J. 847 (2003) [hereinafter *Trustwrap*]; Peter P. Swire, *Of Elephants, Mice, and Privacy: International Choice of Law and the Internet*, 32 INT'L LAW. 991 (1998) [hereinafter *Of Elephants, Mice, and Privacy*]. For information on a conference I hosted in the summer of 2006

essay has developed into a more general theory about why we should expect underenforcement for e-commerce, cybercrime, and Internet harms more broadly. It also recommends a strategy for addressing that underenforcement, focusing on more federal or federated enforcement.

This essay stresses an "information" problem and a "commons" problem that have largely been overlooked to date. In brief, the information problem arises because only a tiny fraction of complaints and knowledge about an online fraudster or criminal comes from each jurisdiction. Enforcers thus lack the informational basis for telling "good guys" from "bad guys." Priority bad guys are thus less likely to become the targets for enforcement.

This information problem is compounded by a commons problem. A local enforcer might say: "Why should I spend my scarce prosecutorial resources on a case when most of the victims are outside of my jurisdiction?" In light of the incentives facing enforcement agencies, priority will typically go to cases where many or all of the victims are local. No one will have the incentive to give priority to harms that occur across borders. This is a classic commons problem, because cross-border harms will be left to "someone else." In short, no one will own these problems, and there will be underenforcement.

These information and commons problems exacerbate the underenforcement problem that has been the focus of the greatest legal attention to date. What might be called the "forensic" problem is the recognition that it is often technically and legally difficult to gather evidence where the perpetrator is physically distant from the victim. The analysis in this essay shows why addressing the forensic problem will not be enough to solve underenforcement for e-commerce, cybercrime, and Internet harms generally.

The basic response should be to shift toward more federal or federated enforcement. Federal enforcement means a greater role, compared to offline activity, for the Federal Trade Commission (FTC) in consumer protection and the Department of Justice for cybercrime. Federated enforcement means building new structures, compared to offline activity, to share information among local enforcers and to encourage local enforcers to bring more enforcement actions even when the perpetrator and many of the victims are outside of their jurisdiction.

Part I of the essay explains the information, commons, and forensic problems in greater depth, and explores policy and legal responses to those problems. Part II responds to five possible critiques, which I call:

---

that dealt with these matters, see Ctr. For Am. Progress, The Internet and the Future of Consumer Protection, http://www.americanprogress.org/events/2006/7/b593305ct2758595.html.

(1) "The Internet hasn't really changed anything"; (2) "Enforcement works better on the Internet"; (3) "We don't want enforcement for what's done on the Internet"; (4) "States need to be the laboratories of experimentation"; and (5) "The Feds don't do small potatoes."

I. REASONS FOR UNDERENFORCEMENT IN E-COMMERCE AND CYBERCRIME

Part I defines "underenforcement," and then analyzes the information, commons, and forensic problems that face cyberspace enforcers.

A. Defining Underenforcement

I will briefly define what I mean by "underenforcement" before examining in more detail the information, commons, and forensic problems that bedevil cyberspace enforcement. A recent article by Alexandra Natapoff has studied the general phenomenon of underenforcement.[2] Professor Natapoff's article responds to criminal law debates about over-criminalization. Her article effectively shows problems from too much laxity, and explains why "underenforcement can be a form of deprivation, tracking familiar categories of race, gender, class, and political powerlessness."[3] Beginning with this focus on serious physical crimes, and predictable negative effects on powerless groups, Professor Natapoff seeks to distinguish generally between "good" and "bad" underenforcement.[4]

My goal is narrower. The focus here is on online fraud, malicious software, and other harms that are carried out through the Internet. This essay highlights the information and commons problems that have not been the subject of clear attention to date. As discussed below, these problems are primarily institutional – the capabilities and incentives of enforcers are likely to work less well in the shift from offline harms to online harms. My proposed responses are also institutional, designed to address the specific problems that arise online.

This essay, therefore, does not attempt to decide on some optimal level of enforcement against fraud or other online harms. Instead, "underenforcement" here refers to a comparative analysis, the way that enforcement against a category of harm is likely to be less effective online than offline. In light of my starting point with consumer protection law, important examples are deceptive practices and outright fraud online. I am asserting that the institutional mechanisms for addressing those

2. Alexandra Natapoff, *Underenforcement*, 75 FORDHAM L. REV. 1715 (2006).
3. *Id.* at 1717.
4. *Id.* at 1719.

problems offline, based heavily at the local or state level, are likely to be less effective for online deception and fraud. I call this deficit in effectiveness "underenforcement." I propose more federal or federated institutions as a response to this underenforcement.

For some categories of harm, there is no simple offline baseline for comparison. Spyware, viruses, and other malicious software, for instance, are a much more severe problem in a networked, online environment than they are for stand-alone computers. For these examples, the meaning of "underenforcement" cannot be clearly defined by comparison with offline harms. In these instances, to define "underenforcement," we need some societal decision about the definition of what is harmful and how serious the harm is. This essay does not try to give a substantive theory of how to define harms caused by spyware or other malicious software. Nor does it take a position on other substantive issues, such as the hotly-contested issue of sharing or copying files of music or movies through peer-to-peer software. Instead, the significant but limited goal of this essay is to examine the institutional challenges raised by the information, commons, and forensic problems.

B. The Information Problem: "No Cop on the Beat"

Compared to the physical world, online perpetrators rarely live or work in the same jurisdiction as their victims. In the physical world, for instance, a local consumer protection bureau builds up local knowledge about which actors are good guys and which are bad guys. Then, when the next complaint comes in, enforcers prioritize action against the known or suspected bad actors. For the stereotypical example of used car dealers, local enforcers might act quickly against any new signs that Shady Sam is defrauding consumers again, but will give the benefit of the doubt to Honest Amy's Used Cars the first time a complaint is lodged.

The familiar situation of school discipline illustrates the point. A high school principal might catch students in an ambiguous situation, which may have an innocent or not-so-innocent explanation. For instance, the principal might catch a couple of kids in the locked part of the high school after hours, where students have been caught in the past doing drugs. The principal might treat some students as "good kids," such as editors of the school paper who say they are staying late to finish an issue. Other kids get treated as "troublemakers," such as another pair of students who are already on probation. The latter might get taken to the principal's office and searched, while the former walk away free even if they, too, were carrying drugs.

For the kids who get caught, this different behavior may well seem

unfair. It is quite likely rational, however, for the principal. Under a Bayesian approach to enforcement,[5] the principal tries to decide between two hypotheses. H-0 is that the person is innocent. H-1 is that the person is guilty. The principal bases his or her decision on the new information, which is that the two students were found in the locked part of the school. The principal also bases the decision on pre-existing information about the suspects, that some are good kids on the newspaper and others are on probation. The decision on whether to enforce is based on a combination of the new and pre-existing information about the suspects. The well-developed insights of Bayesian statistics show why it is rational in many instances for the principal to act differently toward the two sorts of suspects.

This Bayesian approach highlights why a cop on the beat is different from cyber-enforcement.[6] Cops on the beat build up a great deal of local knowledge.[7] They learn a great deal about whom to trust and what is "normal" for the time and place. They know what has happened in the neighborhood recently, spotting patterns of new crimes and seeing whether a next crime fits the modus operandi of previous crimes. When an incident occurs, the police officer relies on this background knowledge to assess who is likely telling the truth and when someone should be arrested.

Enforcement against Internet harms, by contrast, suffers from the lack of local knowledge. Both the victims and the perpetrators are geographically scattered. When the enforcement agency receives a complaint, there is no basis for knowing whether the perpetrator has harmed one victim (the local complainant) or numerous victims (who live predominantly in other jurisdictions). That is, the Bayesian signal is much weaker. In contrast to the cop on the physical beat, the cyber-enforcer is far more uncertain about the scope of the problem or whether this alleged perpetrator is more like Honest Amy or Shady Sam.

The initial response to the information problem is to share information among enforcement agencies. Ideally, the geographic scope

---

5. For further explanation of the Bayes theorem, see William B. Fairley & Michael O. Finkelstein, *A Bayesian Approach to Identification Evidence*, 83 HARV. L. REV. 489 (1970); Stephen E. Fienberg & Mark J. Schervish, *The Relevance of Bayesian Inference for the Presentation of Statistical Evidence and for Legal Decisionmaking*, 66 B.U. L. REV. 771 (1986); Roland Kirstein, Bayes Monitoring, http://ideas.repec.org/p/bep/dewple/2005-1-1132.html; Eliezer Yudkowsky, An Intuitive Explanation of Bayesian Reasoning: Bayes' Theorem for the Curious and Bewildered, http://yudkowsky.net/bayes/bayes.html.

6. See Susan W. Brenner & Leo L. Clarke, *Distributed Security: Preventing Cybercrime*, 23 J. MARSHALL J. COMPUTER & INFO. L. 659, 663-68 (2005), for one account of the differences between cybercrime and the historical cop on the beat.

7. See Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Product Liability and Other Issues*, 5 U. PITT. J. TECH. L. POL'Y 2 nn.86-89 (2005), for a discussion of cops on the beat and community policing.

on information collection would match the geographic scope of the harms. For local crimes, in the high school or the neighborhood, the principal or the cop on the beat is in a good position to make the Bayesian estimate of risk. For Internet crimes, however, new mechanisms are needed to share information among enforcement agencies.

Some of these information-sharing institutions have emerged in the relatively short time, about fifteen years, since commercial activity began on the Internet.[8] The FTC has established Consumer Sentinel, an information-sharing network for consumer harms that now includes over 1,000 law enforcement agencies in Australia, Canada, and the United States.[9] As of year-end 2007, Consumer Sentinel received over one million reports about consumer harm from government and private sources.[10] A stated goal is to provide precisely the Bayesian assistance needed to face geographically-dispersed threats, "to determine whether a reported scheme is local, regional, national, or cross-border, and to help spot trends for law enforcement."[11] Other examples of information-sharing to fight geographically scattered cyber-harms include: the FBI's InfraGard program;[12] other cybercrime-oriented information sharing, such as at the G8 level;[13] and a centralized portal for telecommunications companies for data breaches involving their customers' information.[14] Additional forms of information sharing will be essential over time to address the reality that many harms caused through the Internet are perpetrated from other jurisdictions.

Information sharing is no panacea, however. My previous research has examined institutional incentives that often make it hard for law enforcement to share information effectively.[15] Information sharing can

8. See OFFICE OF INSPECTOR GEN., NAT'L SCIENCE, REVIEW OF NSFNET (1993), *available at* http://www.nsf.gov/pubs/stis1993/oig9301/oig9301.txt (plain text only), which states that the Scientific and Advanced Technology Act of 1992, 42 U.S.C. § 1862(g) (2000), "subtly modified [the National Science Foundation]'s authority to support computer networks that are not limited to research and education." This change was an important legal step toward development of commercial activity over what is now called the Internet.

9. *See* FTC, Consumer Sentinel Network: Law Enforcement's Source for Consumer Complaints, http://www.ftc.gov/sentinel/members.shtml.

10. FTC, CONSUMER FRAUD AND IDENTITY THEFT COMPLAINT DATA (2008), http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2007.pdf.

11. Int'l Ass'n. of Chiefs of Police, IDSafety, http://idsafety.org/enforcement/resources/.

12. Fed. Bureau of Investigation, InfraGard, http://www.infragard.net.

13. Computer Crime and Intellectual Prop. Section, U.S. Dept. of Justice, International Aspects of Computer Crime, http://www.usdoj.gov/criminal/cybercrime/intl.html.

14. *See* Scott D. Delacourt, *New CPNI Rules Could Alter Standard Carrier Practices*, WILEY REIN, May 2007, http://www.wileyrein.com/publication_newsletters.cfm?id=10&publication_ID=13066 (describing the "Customer Proprietary Network Information" rules, promulgated as 72 Fed. Reg. 45,911 (2007)). The Secret Service and FBI reporting provision can be found at 47 C.F.R. § 64.2011; the Apr. 2, 2007 FCC Order can be found at 22 FCC Rcd. 6927.

15. Peter P. Swire, *A Theory of Disclosure for Security and Competitive Reasons: Open Source,*

in some instances actually undermine security, such as when suspects learn they are under investigation and evade capture.[16] In addition, there can be serious privacy and other problems depending on how information sharing systems are designed. To address these problems, I have elsewhere proposed a "due diligence" list of steps to take when considering new information sharing systems.[17]

In addition to information sharing, another promising response to the information problem is to redefine what counts as a "beat." Historically, a cop was on a "beat" defined geographically, such as in a certain physical neighborhood. For the Internet, it likely makes sense to organize enforcement along more functional grounds. For instance, the FTC can assign personnel to "beats" such as spam, spyware, and phishing. These persons can gain Bayesian insights due to their knowledge of the subject matter, and not be limited by geography. This approach would lead to a more matrixed approach to law enforcement, with initiatives and budgeting based in part on geography and in part on function.

C. The Commons Problem: "It's Not My Problem"

The commons problem exacerbates the underenforcement caused by the information problem. For example, a local enforcer might say: "Why should I spend my scarce prosecutorial resources on a case when most of the victims are outside of my jurisdiction?" Prosecuting a distant perpetrator will be less of a priority as a matter of deterrence – the local enforcer will rationally prefer to deter conduct where all the deterrent effect is local rather than spread across the Internet. Prosecuting the distant perpetrator will also be less of a priority as a matter of public choice – the enforcer will presumably get more credit locally when all of the victims are local, rather than bringing a case against a perpetrator who mostly harms individuals outside of the jurisdiction. Where enforcement is spread across many local jurisdictions, we thus would expect a classic commons effect: Rational local enforcers will focus on local effects, leading to underenforcement for the system as a whole.

The history of identity theft illustrates how the commons problem operates. As identity theft became more widely known in the late 1990s, a common complaint was that a victim, say in New York, would trace the credit card fraud to someone living elsewhere, say in Los Angeles. Police

---

Proprietary Software, and Government Systems, 42 HOUS. L. REV. 1333 (2006).

16. Peter P. Swire, *A Model for When Disclosure Helps Security: What Is Different About Computer and Network Security?*, 3 J. TELECOMM. & HIGH TECH. L. 163 (2004).

17. Peter P. Swire, *Privacy and Information Sharing in the War on Terrorism*, 51 VILL. L. REV. 951, 952 (2006).

and prosecutors in Los Angeles would give a low priority to this sort of crime. Based on my experience in working on identity theft policy at the time,[18] one reason for reluctance to act in Los Angeles was entirely rational – enforcers were worried that the New York witness would not appear in court in Los Angeles if they successfully caught the fraudster. A bigger problem, in my view, was the sense in Los Angeles (or any other city in the same situation) that "it's not my problem." The victim was outside of the jurisdiction, so press and political credit for the prosecution would likely be lower. After all, a District Attorney gets reelected by protecting the people in the jurisdiction, and not victims far away. In addition, the deterrent effect of prosecution would be less – the perpetrator had already demonstrated that one victim was far away, and so at most only a fraction of the deterrent effect would be in the locality.

A new study by the Center for American Progress and the Center for Democracy and Technology highlighted the limited actions of state attorneys general against fraud on the Internet.[19] The study indicated that in 2007, the FTC reported 221,226 Internet-related fraud complaints, with Internet fraud complaints scoring high as well from states that report statistics.[20] Nonetheless, after examining available information, the authors concluded: "Most attorneys general are giving relatively low priority to online fraud and abuse."[21] For the online cases that are being reported to the National Association of Attorneys General, over 60 percent involved sexual enticement of minors or child pornography.[22] By contrast, just 8.9 percent involved data security, confidential records, or identity theft; 15.5 percent involved online sales and services; and 8.3 percent involved spyware, adware, spam, and phishing (the large majority of which were brought in New York and Washington state).[23] The report stresses that some enforcement efforts at the state level have been pathbreaking, such as the states that have taken the lead in acting against spyware.[24] The overall verdict, however, is

18. I served as Chief Counselor for Privacy in the U.S. Office of Management and Budget from the beginning of 1999 until the beginning of 2001, and worked then on identity theft because of the connection to misuse of personal information. For a description of the National Summit on Identity Theft, convened in March, 2000, see Press Release, U.S. Dep't of Treasury, Treasury Convenes Identity Theft Summit, http://www.treas.gov/press/releases/ls465.htm.

19. REECE RUSHING, ARI SCHWARTZ & ALISSA COOPER, CTR. FOR AM. PROGRESS & CTR. FOR DEMOCRACY & TECH., ONLINE CONSUMERS AT RISK AND THE ROLE OF STATE ATTORNEYS GENERAL (2008), http://www.americanprogress.org/issues/2008/08/pdf/consumer_protection.pdf.

20. *Id.* at 2, 8.

21. *Id.* at 13.

22. *Id.* at 18.

23. *Id.* at 2.

24. *Id.* at 1.

consistent with the analysis of this article, that incentives for state enforcement of Internet fraud are not strong enough.

For the commons problem, it is difficult to give local enforcers incentives to go after distant perpetrators. A more federal or federated approach is likely to be more successful. A federal approach could be similar to that discussed above, for the information problem. A federal agency, such as the FTC, could redefine a "beat" on functional rather than geographic lines. For instance, this has already been done to some extent in the FTC, where there are now experts for each type of harm, such as spam, spyware, phishing, or identity theft.[25] This federal approach helps solve the commons problem because there is a better match between the geographic area of the harm (national and sometimes international) and the geographic area of the enforcement (nationwide by the FTC).

A more federated approach recognizes the usefulness of enforcement task forces that draw on multiple jurisdictions. Federal-state task forces, for instance, have been used widely for drug prosecutions and, more recently, in fighting terrorism.[26] Such task forces have information sharing advantages, because members of the team are experienced at using their own computer systems and are authorized to see into their own classified databases. Such task forces also help address the commons problem, such as if a New York detective and a Los Angeles detective worked together on our identity theft case. In that instance, both detectives could plausibly feel that it is "their" case, and they would get credit within the task force for successful enforcement. These sorts of federated approaches could apply at various levels, including state-to-state, state-to-federal, and between U.S. and non-U.S. agencies.

D. The Forensic Problem, Both Legal and Technical

Compared to the information and commons problems, highlighted above, Congress and policymakers have paid more attention to date to the forensic problem. The forensic problem, as described here, results from the fact that it is often technically and legally difficult to gather evidence where the perpetrator is physically distant from the victim.

The legal aspect of the forensic problem arises where one jurisdiction lacks compulsory process to get evidence in another

25. The FTC has now created the Division of Privacy and Identity Protection within its Bureau of Consumer Protection, to provide functional expertise on privacy, identity theft, and related harms to consumers. *See* FTC, Div. of Privacy and Identity Prot., http://www.ftc.gov/bcp/bcppip.shtm.

26. U.S. Dep't of Justice, Joint Terrorism Task Force, http://www.usdoj.gov/jttf/.

jurisdiction. Within the United States, a state or local enforcer will need to get cooperation from enforcers in another jurisdiction, or else go through potentially laborious processes to compel production of documents or ensure cooperation from witnesses. The problems are usually much greater for enforcement involving evidence from outside the United States. Congress has now ratified the Council of Europe Cybercrime Convention, which is designed to smooth international production of evidence relevant to prosecuting crimes occurring over the Internet.[27] For enforcement of consumer protection laws, Congress in 2006 enacted the U.S. SAFE WEB Act, easing the procedures for seeking evidence from outside of the United States.[28] These laws provide new routes for international cooperation on Internet investigations, but cross-border enforcement is still generally more burdensome than enforcement within a jurisdiction. Additional legal changes may be appropriate over time to ease those burdens.

The technical aspects of the forensic problem are also challenging. Many local and state enforcement agencies lack the technological sophistication of the most effective Internet criminals. Attacks through the Internet also typically evolve at Internet speed, so that it is hard to have effective enforcement except where the enforcers are keeping up with technology full-time.

One logical response, which also responds to the information and commons problems, is to increase support for countering the functional types of Internet harms, such as spam, spyware, phishing, and identity theft. A related response is to designate federal centers of excellence for responding to Internet harms. The Department of Justice did this in the 1990s, such as through the creation of the Computer Crimes and Intellectual Property Section (CCIPS) in the Criminal Division.[29] As discussed below, I have suggested that the FTC should upgrade its own technical capacities to fight harms occurring through the Internet.[30]

---

27. The U.S. Senate ratified the COE Cybercrime Convention on August 3, 2006. Press Release, U.S. Dep't of State, U.S. Senate Votes To Ratify Cybercrime Convention (Aug. 7, 2006), available on Westlaw at 2006 WLNR 13638778; *see also* U.S. Dep't of Justice, International Aspects of Computer Crime, http://www.usdoj.gov/criminal/cybercrime/intl.html. I generally support the aspects of the Cybercrime Convention that facilitate sharing evidence for crimes committed over the Internet. I believe there are other flaws in the Convention, however, as explained in Ctr. for Democracy and Tech., Comments of the Center for Democracy and Technology on the Council of Europe Draft "Convention on Cyber-crime" (Draft No. 25), http://www.cdt.org/international/cybercrime/010206cdt.shtml.

28. U.S. SAFE WEB Act of 2006, Pub. Law 109-455, 120 Stat. 3372 (2006) (amending various sections of the FTC Act, 15 U.S.C.A. §§ 41, 45-46, 56-58).

29. *See* U.S. Dep't of Justice, Computer Crime & Intellectual Property Section, www.cybercrime.gov.

30. *See* Swire, *infra* note 37.

II. ANSWERING POSSIBLE CRITIQUES

Part I explained the information, commons, and forensic problems that make Internet enforcement more difficult than offline enforcement. It recommended a more federal or federated approach to Internet harms than the more localized enforcement that exists offline. This Part examines five possible critiques of this approach.

A. "The Internet Hasn't Really Changed Anything"

An initial critique is that "the Internet hasn't really changed anything." After all, Montgomery Wards was a major mail-order merchant across state lines a century ago, and telemarketing and national chain stores have been prominent for decades.[31] So why should we expect the current consumer protection system, based on local and state enforcement, to break down when it comes to the Internet?

Upon inspection, however, emerging forms of interstate commerce have historically led to a greater federal role, as contemplated in this essay for Internet consumer protection and cybercrime. Consider a few examples. First, the blue sky state laws for securities gave way in 1933 and 1934 to our modern federal securities regime, led by the Securities and Exchange Commission.[32] Second, the rise of mail-order business was accompanied by a growing role for federal mail fraud prosecutions, later joined by wire fraud prosecutions.[33] Third, sales by telephone, often across state borders, have been matched by a number of federal initiatives, such as the Telemarketing Sales Rule and Do Not Call Rule issued by the FTC.[34] Fourth, the emergence of identity theft as a prominent problem has appropriately led to recent federal statutes and enforcement initiatives.[35] In short, growing harms from interstate commerce have historically been matched by a growing role for the federal government in addressing such harms.

The Internet poses forensic problems that likely can best be approached with an increased federal presence. On the legal side, the federal government necessarily plays a leading role in getting evidence

---

31. *See* Montgomery Ward, About Montgomery Wards, http://www.wards.com/wards/aboutus.asp.

32. JOEL SELIGMAN, THE TRANSFORMATION OF WALL STREET: A HISTORY OF THE SECURITIES AND EXCHANGE COMMISSION AND MODERN CORPORATE FINANCE 42-72 (3d ed. 2003) (1982).

33. Federal Wire Fraud Act of 1952, Pub. L. No. 82-554, § 18, 66 Stat. 711, 722 (codified as amended at 18 U.S.C. § 1343 (2006)).

34. Telemarketing Sales Rule, 6 C.F.R. § 310 (2008); Do Not Call Rule, 47 CFR § 64.1200 (2008).

35. Gramm-Leach-Bliley Financial Modernization Act, Pub. L. No. 106-102, § 521, 113 Stat. 1338, 1446 (codified at 15 U.S.C. §§ 6821-6827 (2006)).

from overseas through Mutual Legal Assistance Treaties, other treaties, and diplomatic activities. Federal enforcers also generally face fewer barriers than local or state prosecutors in serving process or otherwise gathering evidence across state lines.[36]

The technical side of forensics also leads to a greater federal role. Many counties and states will find it hard to stay at the cutting edge of such current consumer protection issues as spam, phishing, computer security, data breaches, and spyware. As I have written previously,

> Information technology issues are much more important than before because online commerce and Internet safety lie at the intersection of technology and law enforcement. The FTC must therefore consider a new office of information technology to assist the Commission in making effective decisions about how to protect consumers in Internet activities. This office would parallel the FTC's in-house capability in economics, and would permit the FTC to act strategically to protect consumers from emerging online threats.[37]

For these technical issues, the FTC can play a leadership role in amassing enough technical expertise to address emerging consumer protection issues. The national role of the FTC, and its growing relationships with enforcement agencies overseas, is also a good match to the national and international nature of online threats to consumers.

B. "Enforcement Works Better on the Internet"

A second critique of my under-enforcement thesis would be that enforcement may actually work better on the Internet. Optimists about the potential of the Internet, especially during the bubble of the late 1990s, have been enthusiastic about the "friction-free" and near-perfect market that they say will occur online.[38] For these techno-optimists, the Internet offers unprecedented transparency for consumers — individual surfers can comparison shop and reputation systems cue consumers about

---

36. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 , Pub. L. No. 107-56, § 220, 115 Stat. 272, 291 (codified as amended at 18 U.S.C. §§ 2703, 2711 (2006)).

37. Peter Swire, Ctr. for Am. Progress, Funding the FTC: Globalization and New Information Technologies Necessitate an Appropriations Boost, http://www.americanprogress.org/issues/2007/02/ftc.html. The idea of a new FTC office of information technology was cited by the Democratic Policy Committee in 2007 as one of its "Fresh 50" policy ideas. DEMOCRATIC POLICY COMM. NEW IDEAS PROJECT, THE 2007 FRESH 50: FIFTY NEW POLICY IDEAS FOR SENATE DEMOCRATS 11 (2007).

38. J. Bradford DeLong & A. Michael Froomkin, *Speculative Microeconomics for Tomorrow's Economy*, *in* INTERNET PUBLISHING AND BEYOND: THE ECONOMICS OF DIGITAL INFORMATION AND INTELLECTUAL PROPERTY 6, 10-13 (Brian Kahin & Hal R. Varian eds., 2000).

which sellers they should trust.

There is an important element of truth in this optimistic view. Comparison shopping is undoubtedly easier online than offline for many purchases, because it is easier to check prices on a dozen websites than drive to a dozen physical stores. In addition, savvy consumers can easily use modern search engines to check the reputation of various sellers.

With that said, the magical effects of online reputation can easily be overstated. As an opening point, it is useful to remember the tautology that half of consumers are below-average when it comes to sophistication. The history of consumer protection law has shown that successful frauds work well against some consumers even though they would never fool others.[39] Consumer protection law should thus not assume that online consumers are all sophisticated both economically and technically.

In addition, my previous work has explained important limits to the techno-optimist vision of online commerce. Reputation systems alone have proven insufficient to protect consumers against fraud. eBay has perhaps the most famous reputation system for e-commerce, in which buyers rate their experience with the numerous sellers who put items up for auction. The original reputation system, however, has had to be supplemented by layers of legal guarantees and a large and growing antifraud enforcement effort.[40]

Along with ways that reputation systems can be gamed by fraudsters, there is a more general limit on the extent that reputation alone is not enough to protect consumers from fraud. For the Internet, I have long stressed the difference between large organizations, which I call "elephants," and the nimble, small actors, which I call "mice."[41] In brief, elephants have thick hides when they are attacked, hides which include excellent PR firms and attorneys. But elephants such as famous-brand retailers are particularly lousy at hiding. If Amazon.com or any other famous website is ripping people off on the Internet, then that is likely to be highly visible and enforcers will be alerted quickly.

By contrast, most of the criminal and fraudulent behavior on the

---

39. For instance, the FTC Statement on Deception states: "An interpretation may be reasonable even though it is not shared by a majority of consumers in the relevant class, or by particularly sophisticated consumers. A material practice that misleads a significant minority of reasonable consumers is deceptive." Cliffdale Associates, 103 F.T.C. 110, 174 n.20 (1984) (citing Heinz W. Kirchner, 63 F.T.C. 1282 (1963)), *available at* http://www.ftc.gov/bcp/policystmt/ad-decept.htm.

40. *Trustwrap*, *supra* note 1 (describing legal guarantees and other antifraud measures); *see also* Mary M. Calkins, Alexei Nikitkov, & Vernon Richardson, *Mineshafts on Treasure Island: A Relief Map of the eBay Fraud Landscape*, 8 J. TECH. L. & POL'Y 1 (2008) (describing current details of eBay's antifraud efforts).

41. *See Elephants and Mice Revisited*, *supra* note 1; *Of Elephants, Mice, and Privacy*, *supra* note 1.

Internet is perpetrated by mice who are good at hiding, including those who bombard consumers with spam, spyware, and phishing attacks.[42] Phishing attacks, for instance, typically send the surfer to a fake but authentic-seeming website. The surfer provides the personal information that the phisher is seeking, and the site itself typically closes down within days.[43] The operator of the website thus hides away before enforcers arrive on the scene.

The phishing example highlights three aspects of fraud on the Internet. First, the fraud is done by elusive mice, who hide away in nests that are often offshore. Second, the fraud is done by professional criminals, and not by the sorts of hackers who caused mischief on the Internet in the 1990s. Whereas legitimate businesses care deeply about their brand and online reputation, professional criminals do not. Third, the fraud occurs where the fraudsters devise a way to defeat the effects of reputation. In phishing, the fraudsters create the fake but authentic-seeming website. In spyware, the fraudsters trick the consumers into downloading software programs that the consumers don't realize have harmful effects.

In sum, reputation systems on the Internet are helpful but very far from a complete answer. In the important instances where they are not sufficient, we are likely to see underenforcement due to the information, commons, and forensic problems.

C. "We Don't Want Enforcement"

The next critique is that some in the cyberspace community are hesitant to create effective institutions for enforcing against harms on the Internet, for two principle reasons. First, there are disagreements about the extent to which some activities should count as "harms" worthy of enforcement. Notably, there have been vigorous debates about enforcement for file sharing of copyrighted music[44] and for measures to

42. One variation, which has become more important over time, is that spam rings and other fraudsters have organized themselves on a larger scale, but do their activities from safe nests overseas where local law enforcement does not stop their activity. These organized crime activities are thus no longer truly small mice, but instead what Ari Schwartz has described as "Rodents of Unusual Size." *For FTC, e-Commerce Means Managing 'Mice'*, PHYSORG.COM, July 25, 2006, http://www.physorg.com/news73065889.html; *see also* Ctr. for Am. Progress, The Internet and the Future of Consumer Protection, http://www.americanprogress.org/events/2006/7/b593305ct2758595.html. To go after these "rodents," Internet consumer protection will increasingly need to be part of task forces that include prosecutors experienced in fighting organized crime.

43. NAT'L CONSUMERS LEAGUE, A CALL FOR ACTION: REPORT FROM THE NATIONAL CONSUMERS LEAGUE ANTI-PHISHING RETREAT 1 (2006), http://www.nclnet.org/news/2006/Final%20NCL%20Phishing%20Report.pdf. I served as "reporter" for this document.

44. *See, e.g.*, Electronic Freedom Found., Intellectual Property,

combat indecent or pornographic material, especially as accessible by minors.[45] Those who are opposed to enforcement for the music or pornography actions may not want precedents or effective institutions to combat cybercrime or online fraud.[46] Second, the techniques for combating cybercrime and online fraud can raise privacy issues about the techniques for tracing online activity.[47] In response to the first argument, my view is that there should be debates on the merits of each area that some believe cause harm through the Internet. For instance, the rules about online pornographic and indecent material should be based on legal and policy analysis about such material, including the First Amendment implications of possible legal restrictions. The rules about transfer of copyrighted music should also be debated on the merits about copyright law. Similarly, the problems of cybercrime and online fraud should be assessed on the merits. Where reasoned analysis shows harms to victims and underenforcement, then it makes sense to improve enforcement techniques.

I have written extensively elsewhere on the issue of privacy concerns.[48] Privacy issues are most relevant to the forensic problem of how to trace bad actors. A good approach is the Center for Democracy and Technology position on the COE Cybercrime Convention, that updated forensic techniques should be accompanied by due process and privacy protections.[49] Privacy issues are sometimes important for the information problem, as discussed in my writing on information-sharing systems.[50] Privacy issues are not generally important, however, for the commons problems that this essay highlights. The Internet often breaks the geographic link between fraudsters, victims, and prosecutors. The point of this essay is that more federal or federated approaches are needed to solve the resulting information and commons problems.

---

http://www.eff.org/issues/intellectual-property (describing the Electronic Frontier Foundation's position on copyrighted music, which favors broad consumer rights); Recording Industry Ass'n of Am., Piracy: Online and On the Street, http://www.riaa.com/physicalpiracy.php (describing the Recording Industry Association of America's position on copyrighted music, which favors broad industry rights).

45. *See, e.g.*, *Introduction to the 2007 BYU Law Review Symposium: Warning! Kids Online: Pornography, Free Speech, and Technology*, 2007 B.Y.U. L. REV. 1413 (2007).

46. *See, e.g.*, Natapoff, *supra* note 2 at 1741-42 (describing reasons why underenforcement of intellectual property rights on the Internet may be desirable).

47. *See Elephants and Mice Revisited*, *supra* note 1 at 1999-2001.

48. *E.g.*, Peter P. Swire, *Katz is Dead. Long Live Katz*, 102 MICH. L. REV. 904, 904 (2004); Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1311 (2004).

49. *See* Ctr. for Democracy and Tech., *supra* note 27.

50. *See* Swire, *supra* note 17, at 951.

D. "States Need to Be Laboratories of Experimentation"

Federalism concerns are a fourth possible critique of a greater federal role for enforcement of consumer protection or computer crime. The recommendations in this essay, however, are entirely consistent with federalism principles, for two principle reasons. First, the essay's basic point is that we are likely to have underenforcement for online harms, so reforms are appropriate to get closer to the level of enforcement we would achieve in the offline world. If this point is correct, then there is little reason for concern about overenforcement or other intrusion into states' rights. Second, my policy recommendation is to have greater federal or federated enforcement responses to online harms. Online harms often occur across state borders. In some instances, such as where there is specialized technical knowledge at the federal level, then enforcement should be increasingly federal. In other instances, the correct institutional response is federated; we should create better mechanisms for sharing information, expertise, and prosecutorial resources in order to match the broader geographic scale of online harms.

This call for a greater federal or federated enforcement role is distinct from the issue of when and whether there should be preemption of state initiatives against online harms. I support caution in preemption of state initiatives against online harms.[51] Recent notable examples of state experimentation include data breach laws and credit freeze laws.[52] In both instances, initial adoption in some states was followed by continued experimentation and further adoption in other states. [53] At the time of this writing in early 2008, both sorts of laws are being studied at the federal level and we may eventually see national legislation in both areas.[54] My intent in raising these examples is not to say that the state laws have gotten the issues exactly right, although there is recent evidence that data breach laws have led to improved computer security in the private sector.[55] My intent instead is to point out that the states were far swifter than Congress in identifying significant consumer problems

51. See William W. Buzbee, *Asymmetrical Regulation: Risk, Preemption, and the Floor/Ceiling Distinction*, 82 N.Y.U. L. REV. 1547, 1555-57 (2007), for a recent scholarly analysis of reasons to be cautious about such preemption.

52. *See, e.g.*, MINN. STAT. § 325E.61 (2007).

53. See Michael E. Jones, *Data Breaches: Recent Developments in the Public and Private Sectors*, 3 I/S J.L. & Pol'y for Info Soc'y 555, 557 (2007-2008), for analysis of state data breach laws. Multiple committees in Congress have passed their own variations of federal data breach legislation. *Id*. at 574. For credit freezes, Congress has tasked the FTC with studying the state initiatives. *Id*. at 576.

54. *See id.* at 570-71.

55. SAMUELSON LAW, TECH. & PUBLIC POLICY CLINIC, UNIV. OF CALIFORNIA-BERKELEY SCHOOL OF LAW, SECURITY BREACH NOTIFICATION LAWS: VIEWS FROM CHIEF SECURITY OFFICERS 8-9 (2007), http://groups.ischool.berkeley.edu/samuelsonclinic/files/cso_study.pdf.

and beginning to design plausible solutions. States also have the notable advantage of being able to experiment on a relatively small scale, with the knowledge that mistakes can be fixed relatively easily at the state (repeal the law) or federal (preempt the law) levels. The best initiatives at the state level are likely to spread to other states, and eventually into federal legislation.

I would highlight two points concerning federalism. First, states should have considerable freedom to experiment with new ways to address online and data-related harms, as they have done with data breaches and credit freezes. This freedom, however, is subject to the dormant commerce clause and to prudence about not splitting the national online market into balkanized domains.[56] Second, federal preemption, when it occurs, should generally match the scope of effective national standards. Outside of the reach of national standards, states should retain their traditional ability to experiment.

E. "The Feds Don't Do Small Potatoes"

A final critique is that many online frauds and cybercrimes are "small potatoes," or cases not large enough to deserve federal attention. Orin Kerr has written a blog post entitled "Enforcing copyright law. How about a role for the states?"[57] Professor Kerr observes that copyright is an exclusively federal concern, "but involves low enough stakes that few violations will ever be of much concern to federal investigators and prosecutors."[58] He notes: "The feds generally bring big cases against really bad people; they don't mess around with the small stuff."[59] He then suggests that state prosecutors could be empowered to bring criminal copyright cases, perhaps with only modest penalties attached.

I agree with Professor Kerr that U.S. Attorney offices set a priority on "big cases against really bad people" such as drug kingpins or suspected terrorists. This fact has been one obstacle to prosecution of identity theft cases, because many prosecutors have not seen identity theft to be as serious a crime as others that they face.[60] Other federal

---

56. Mark A. Lemley, *Place and Cyberspace*, 91 CAL. L. REV. 521, 530 (2003).

57. Posting of Orin Kerr to The Volokh Conspiracy, http://volokh.com/2003_06_22_volokh_archive.html (June 22, 2003, 7:01 PM).

58. *Id.*

59. *Id.*

60. THE PRESIDENT'S IDENTITY THEFT TASK FORCE, COMBATING IDENTITY THEFT: A STRATEGIC PLAN 54 (2007), http://www.identitytheft.gov/reports/StrategicPlan.pdf; THE PRESIDENT'S IDENTITY THEFT TASK FORCE, COMBATING IDENTITY THEFT: A STRATEGIC PLAN, VOLUME II: SUPPLEMENTAL INFORMATION 45 (2007), http://www.identitytheft.gov/reports/VolumeII.pdf. See Press Release, FTC, The President's Identity Theft Task Force Releases Comprehensive Strategic Plan to Combat Identity Theft

agencies such as the FTC have a similar need to set priorities. So Professor Kerr raises an important point when he points out that federal prosecutors don't make a priority of the "small potatoes" cases.

The problem, however, is that state enforcers have to set priorities as well. This essay has explained the information, commons, and forensic problems that have a disproportionate effect on state enforcers. My argument is not that federal enforcement for online harms is a panacea. My argument instead is that the *relative* role of federal enforcement should grow for online harms. Whatever the mix of state and federal enforcement has been, online harms will likely be better addressed with a greater federal role than before.

One reason for the greater federal role goes back to the idea of "the cop on the beat." In addition to learning the local terrain, the cop on the beat develops relationships with local sources of information. For online harms, the useful sources of information quite often will be at the national or international level. For instance, the FTC and the FBI can develop ongoing relationships with ISPs and other actors who may be useful partners in fighting against online harms.

To address online harms, it may be useful to develop task forces and other new institutional arrangements that are tailored to online harms. A good model might be the CCIPS in the Justice Department. CCIPS has developed the sort of focus on online harms, technical expertise, and relationships with key actors that I suggest may be appropriate more broadly in addressing online harms. On a day-to-day basis, the prosecutors in CCIPS are not having to weigh their mission (online harms) against whatever other cases are in a U.S. Attorney's office. There will, of course, continue to be decisions about how to set priorities, but the process can say, overall, what level of effort is appropriate for each category of online harm. When it comes to categories of harm such as spyware, identity theft, or spam, it may similarly make sense to create an overall staffing organized around issue areas. That sort of staffing is more likely to be achievable at the federal level, such as in the FTC or in a multi-agency task force, than at the state level.

CONCLUSION

I will conclude this essay with a story from when I was working on the 2000 federal report on Unlawful Conduct on the Internet.[61] The

(June 5, 2007), http://www.ftc.gov/opa/2007/04/idtheft.shtm, for a brief summary of those reports.

61. THE PRESIDENT'S WORKING GROUP ON UNLAWFUL CONDUCT ON THE INTERNET, THE ELECTRONIC FRONTIER: THE CHALLENGE OF UNLAWFUL CONDUCT INVOLVING THE USE OF THE INTERNET (2000), http://www.usdoj.gov/criminal/cybercrime/unlawful.htm. I served as a representative of the

story illustrates both some important aids to enforcement on the Internet, but also, in the end, the reasons to be concerned about underenforcement.

The Report begins with the facts of an online stock fraud:

> On April 7, 1999, visitors to an online financial news message board operated by Yahoo!, Inc. got a scoop on PairGain, a telecommunications company based in Tustin, California. An e-mail posted on the message board under the subject line "Buyout News" said that PairGain was being taken over by an Israeli company. The e-mail also provided a link to what appeared to be a website of Bloomberg News Service, containing a detailed story on the takeover. As news of the takeover spread, the company's publicly traded stock shot up more than 30 percent, and the trading volume grew to nearly seven times its norm. There was only one problem: the story was false, and the website on which it appeared was not Bloomberg's site, but a counterfeit site. When news of the hoax spread, the price of the stock dropped sharply, causing significant financial losses to many investors who purchased the stock at artificially inflated prices.[62]

These facts fit the classic "pump and dump" stock scheme – the perpetrators pump up the price of a stock with false information, and dump their own shares at the peak, leaving the other investors with the loss.[63]

The PairGain facts were placed in an early draft of the Report by Justice Department lawyers who wanted to make the point about how dangerous the Internet is. Essentially, they were saying: "Look at how bad fraud is on the Internet. The bad guy was able to create one false website, and consumers all over the world were fleeced of their money within hours!"

My own reaction to the facts was quite different. I asked what had happened to the perpetrator. The final Report now continues,

> Within a week after this hoax appeared, the Federal Bureau of Investigation arrested a Raleigh, North Carolina man for what was believed to be the first stock manipulation scheme perpetrated by a fraudulent Internet site. The perpetrator was traced through an Internet Protocol address that he used, and he was charged with securities fraud for disseminating false information about a publicly

---

U.S. Office of Management and Budget to this multi-agency working group which was chaired by the Department of Justice.

62. *Id.*

63. In the PairGain case, interestingly enough, the person who created the fake web site apparently got cold feet and did not trade; CHRISTOPHER M.E. PAINTER, TRACING IN INTERNET FRAUD CASES: PAIRGAIN AND NEI WEBWORLD (Apr. 26, 2005), http://www.usdoj.gov/criminal/cybercrime/usamay2001_3.htm.

> traded stock. The Securities and Exchange Commission also brought a parallel civil enforcement action against him. In August, he was sentenced to five years of probation, five months of home detention, and over $93,000 in restitution to the victims of his fraud.[64]

In short, the Internet actually made it far *easier* to stop the bad guy. The hoax was detected within hours, and the perpetrator was arrested within a week.[65]

The PairGain story exemplifies both advantages and disadvantages for law enforcement in fighting unlawful conduct on the Internet. For web sites, detection can happen at Internet speed. The criminal or fraudster faces this fundamental problem – what the marks can see the cops can see. Illegal activity thus can quickly come to the attention of enforcers. On the other hand, criminals shift to less easily traced methods of fraud. More recent pump and dump stock schemes have been done through spam emails rather than through a static web site.[66] Tracing the source of such emails is a far harder challenge, raising the information, commons, and forensic challenges described in this essay. Compared with the historical patterns for offline fraud and crime, a more federal or federated approach will often be needed for the harms caused to individuals in the online world.

64. THE PRESIDENT'S WORKING GROUP ON UNLAWFUL CONDUCT ON THE INTERNET, *supra* note 61.

65. *Id.*

66. LAURA FRIEDER & JONATHAN ZITTRAIN, SPAM WORKS: EVIDENCE FROM STOCK TOUTS AND CORRESPONDING MARKET ACTIVITY (Berkman Ctr. Research Publ'n No. 2006-11, Mar. 14, 2007), *available at* http://ssrn.com/abstract=920553.