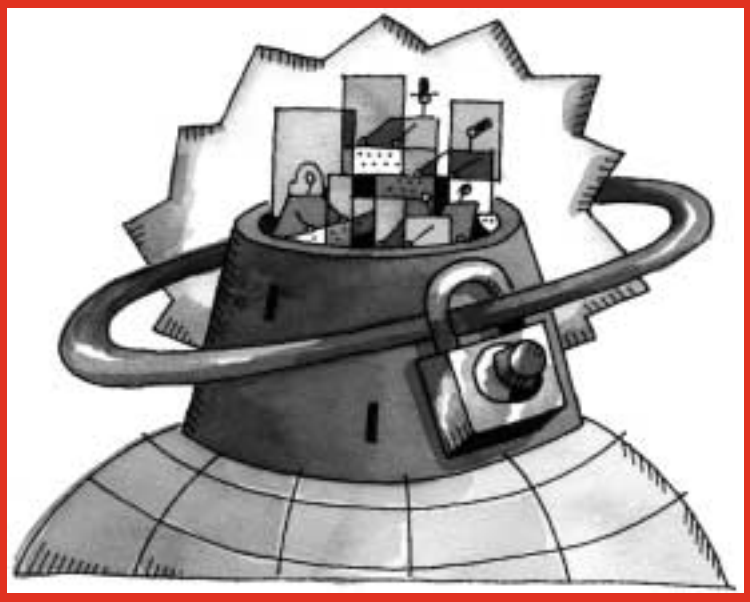
;login:
THE MAGAZINE OF USENIX & SAGE
December 2002 • volume 27 • number 6

Focus Issue: Security

Guest Editor: Rik Farrow

inside:



USENIX & SAGE
The Advanced Computing Systems Association &
The System Administrators Guild

“it depends”:

defining legal values for network behavior

by Erin Kenneally

Erin Kenneally is a Forensic Analyst with the Pacific Institute for Computer Security (PICS), San Diego Supercomputer Center. She is a licensed attorney who holds Juris Doctorate and Master of Forensic Sciences degrees.

erin@sdsc.edu

> “Men feed data to a computer and men interpret the answer the computer spews forth. In this computerized age, the law must require that men in the use of computerized data regard those with whom they are dealing as more important than a perforation on a card. Trust in the infallibility of a computer is hardly a defense, when the opportunity to avoid the error is as apparent and repeated as was here present.”

This was a response by a Court of Appeals to Ford Motor’s assertion that a computer mistake caused it to wrongfully repossess a customer’s car.[1] Although the punch card reference might cause one to dismiss its significance as antiquated pre–World Wide Web naïveté, the underlying message remains even more true in our current Internetworked society. Whether we are dealing with a disputed bill payment and mistaken repossession or questionable computer access and release of protected information, human use of computers involves conflicts over values and property that necessitate defining and enforcing socially acceptable behavior. This is where the standard known as “reasonableness” is paramount to guiding the acts and consequences involved in network behavior.

Ignorance Is Not Bliss

On one hand, people are quick to parrot the notion that Internetworked society is the new Wild Wild West, referring to the dearth of computer-specific laws and regulations, coupled with our free-market tradition of allowing industry to self-regulate and reward beneficial behavior. Nonetheless, even the habitation of “unchartered” land relied upon notions of reasonableness to guide the resolution of conflicts. To continue to use the relative dearth of historical network behavior as a justification for unacceptable behavior is to ignore the social indicators of consensus on what network behavior is tolerable.

“Reasonableness” itself is a relative and dynamic standard in that there is no fixed formula, and determinations are made on a case-by-case basis.[2] Yet this standard underlies many of our laws and constitutional rights. Reasonableness can be found at the heart of many mechanisms that are invoked to govern network behavior – laws such as the Computer Fraud and Abuse Act (CFAA), the Fourth Amendment, social pressures (i.e., public relations), and corporate privacy policies.

Recognizing that there are myriad standards regarding computer security and yet no single, overriding measuring stick, one is hard-pressed to know what standard should be followed so as to not run afoul of the law. Furthermore, the “reasonableness” standard facilitates the ignorance defenses, blaming the victim, and Robin Hood justifications, as evidenced by the cases discussed below.

Nevertheless, both the physical and digital realms employ laws, contracts and licenses, and informal social pressure as mechanisms to notify and implement acceptable behavior. However, a notion of what constitutes acceptable computer network behavior is much less developed. For example, there is no disputing that taking a golf club to my neighbor’s window is unacceptable; yet employing an equally malicious software tool against a fellow Netizen’s computer does not necessarily evoke such a binary judgment of right and wrong. Although consensus about acceptable network behavior is

1. *Ford Motor Credit Company v. Swarens*, 447 S.W.2d 53 (1969).

2. What is a reasonable search is not to be determined by any fixed formula. The Constitution does not define what are “unreasonable” searches and, regrettably, in our discipline we have no ready litmus test. The recurring questions of the reasonableness of searches must find resolution in the facts and circumstances of each case. *United States v. Rabinowitz*, 339 U.S. 56 at 63 (1950).

embryonic and there are comparably fewer laws that are specific to "cyber-behavior," notions of right and wrong do exist. Recent conflicts involving Ziff-Davis, HP and Snosoft, Princeton and Yale universities, and ForensicTec illustrate how we are defining reasonableness in our Internetworked society.

Law as a Metric for Reasonableness

If reasonableness is a consensus standard, what is the relevant metric? Although bad PR/public opinion is not a formal category that courts check off when adjudging reasonableness, it nonetheless can be a gauge of what society believes to be right and wrong behavior. Other metrics for ascertaining reasonableness include regulations, policies and practices, contemporary litigation, notice/knowledge, and capability.

As with ForensicTec, employees accessed government and other private networks and viewed and downloaded files containing military procedures, email, SSNs, and financial data.[3] Attempting to justify their actions, ForensicTec allegedly noted that they used publicly available scanning software to identify vulnerable computers, as well as using easily guessed passwords to gain "unobstructed" access to these sites.

In response to criticism and allegations that it had violated the federal computer crime law (CFAA), ForensicTec played the Robin Hood card by claiming that it was merely pointing out serious vulnerabilities in various networks. Even though ForensicTec was a "legitimate" company on paper, its actions were no different from that of a teenaged hacker conducting the digital equivalent of chest beating. In the eyes of the law, the same elements that constitute a crime are present in both cases: intentional access to a protected computer without authorization.[4] As for the intent element, ForensicTec admitted to repeatedly navigating through multiple government and private networks, thus illustrating knowledge and directed control of its scanning, cracking, and probing activities for connecting to and entering other systems. Insofar as "protected" has been interpreted to mean any computer connected to the Internet, that element can be checked off. And finally, unless ForensicTec had some type of agreement or consent from the government agencies and companies that it accessed, its digital exploration was unauthorized.

Never mind that it notified the vulnerable victims *after* contacting the media, ForensicTec had no legal right to troll through networks where they had no legitimate and authorized business reason to be. Is this any different from trying to justify strolling through your neighbor's house because you discovered their door was open? The ease with which one can access another's property, be it their computer or homestead, is not a factor in determining whether one's actions are lawful. The situation would be no different if ForensicTec had used a million-dollar, one-of-a-kind software tool and/or the victim computers were locked 50 feet below the Pentagon behind a 24/7-managed intrusion detection-firewall schema. Furthermore, although motivation may be a mitigating factor in the penalty phase, the law only considers the "why" insofar as it can be used to infer proof of some element (act or intent) of the offense. This is why Robin Hood and Jean Valjean were both criminals, despite the honorable motivations behind their acts.

Defining Expected Network Behavior

Another emperor without clothes was sighted in the case of the Princeton University administrator who used the SSN and birth dates of student applicants to access admission records at Yale University.[5] Similar to the ForensicTec case, Princeton's actions

3. See Robert O'Harrow, "U.S. Probes Firm in Security Breach: Consultants Invaded Federal Computers," Washington Post.com (August 21, 2002): *http://www.washingtonpost.com/wp-dyn/articles/A42019-2002Aug20.html*.

4. See 18 U.S.C. § 1030.

5. See Karen Arenson, "Princeton Pries into Web Site for Yale Applicants," New York Times Online (July 26, 2002): *http://www.nytimes.com/2002/07/26/education/26IVY.html*.

invoke laws that decry and punish Princeton's network behavior. Primarily, the federal Computer Fraud and Abuse Act prohibited Princeton's intentional entry into Yale's Web site without authorization.[6] The official in question admitted to using the students' identification information to call up their application status from the non-public, restricted Web site, which provided notice that it was authorized for use by prospective students only.

Notwithstanding a seemingly clear violation of the law, the public outcry in response to Princeton's actions is perhaps a stronger metric for the unreasonableness of its network behavior. Princeton officials were quick to express regret and exact discipline almost as soon as the news hit the academic community. In this respect, there was no disagreement that Princeton's digital behavior was illegal and unethical. However, a great deal of attention was shifted by legal scholars to what this situation said about the state of competitiveness in Ivy League admissions. Surely in this breach of student trust the very act of digitally trespassing onto the property and values of another should be the primary focus, rather than the perceived symptom of collegial competitiveness.

The medium of storage or method of transmission should not alter one's (lack of) right to interfere with another's property or values. Would we tolerate a Princeton official using the same information to request and obtain physical records contained in a file cabinet or to greet the postal carrier at the students' mailboxes under such false pretenses? If we bear in mind this non-distinction between traditional and cyber-actions when assessing acceptable network behavior, it is harder to get sidetracked by defenses that obscure the wrongfulness of the act. To do otherwise would dismiss unauthorized intrusive acts as "gaining access out of curiosity about a site's security" or lead down the slippery path of blaming the victim. To be sure, Yale could have implemented stronger security measures such as PINs or randomly generated identifiers to secure applicant records. Other laws such as the Federal Education Records and Privacy Act would give applicants a reasonable expectation that their personal records would not be misused or unprotected by the schools. However, Yale's duty to protect its students' information is an issue distinct from whether Princeton acted with knowledge that it was not permitted to digitally trample on Yale's property rights and values. If someone enters your house and snatches your child's savings bonds – regardless of whether he climbs through an open window or blasts a battering ram through the steel-fortified door – he is violating your reasonable expectations to be secure in your home, as defined under the burglary laws (your child's ability to afford college being a separate matter).

Policy: Another Metric for Reasonableness

Laws and regulations present relatively clear metrics for standards of tolerable behavior, since they are supposed to be formal embodiments of society's values. Private policies, licenses, and contracts are other mechanisms by which society defines, enforces, and adjudges reasonable network behavior. Insofar as individuals can more easily dictate the scope of policies and contracts, these mechanisms may more accurately reflect and more immediately shape notions of reasonableness.

The expectation of online personal data privacy, defined by Web site policies and enforced by informal consumer sanctions, is a prominent instance of acceptable network behavior. This was illustrated in the case involving the Ziff-Davis settlement payment of $150,000 to various states and customers for exposing the credit card

6. In addition, Princeton may have run afoul of the Federal Education Records and Privacy Act (FERPA; 20 U.S.C. 1232g (1993), regulations at 34 C.F.R. 99 (1993)), which creates minimum standards for educational institutions receiving federal funds to protect students' records. FERPA considers student SSNs an education record in and of itself. SSN collection and disclosure by government agencies is generally prohibited by the Privacy Act of 1974.

numbers and identifying information of many of its subscribers.[7] Here, expectations of reasonable behavior were primarily derived from Ziff-Davis's privacy policy, which promised reasonable security in protecting its customers' financial and identity data stored in its databases.[8]

Policies that speak to protecting customer private financial information create a bilateral notice that one party is agreeing to disclose data to the other party that is not for public consumption. Alongside this knowledge is the expectation that the party receiving the data has the capability to protect it from prying eyes, as well as the duty to enforce the promise. These expectations are not unique to Internetworked society – they speak to the same "reasonableness" that demands notice, consent, security, and enforcement of rights to control physical property. If you give your Visa card to the clerk at Krispy Kreme, you reasonably expect that the information will not be posted to the telephone pole outside. In fact, you feel entitled to have that information protected by the physical store owner.

Likewise, the level of computer literacy in the public is such that people have transferred that sense of entitlement to the transmission of private information over the Internet. As such, vendors are expected to implement technical measures to ensure that this information is not exposed to the public. Increased publicity surrounding identity theft has certainly added force to that reasonable expectation.

In fact, the Federal Trade Commission's regulation of unfair and deceptive trade practices is heavily influenced by expectations established by privacy policies.[9]

The expectations become less clear regarding the extent to which a company posting a privacy policy must go to protect the customer data. This will likely be resolved on a case-by-case basis, depending on how specifically the policy was worded, as well as what the cost-benefit analysis reveals. In the Ziff-Davis case, the data was readily exposed by anyone engaging in normal Internet surfing, as opposed to having been unlawfully accessed by someone with über-hacker skills. Despite the fact that Ziff-Davis claimed this was a result of a coding error, it's likely that the potential negative publicity – with corresponding loss of good will and customer base – factored into its decision to pay for its insecure posture. Thus, the risk of damaging commercial reputation and profitability are ways that informal social pressures can be a metric for defining reasonable network behavior.

Reasonableness as a Balancing Act

Amid the cases discussed thus far, a consensus of "reasonable" network behavior has been relatively clear because analogies could be drawn from notions of right and wrong surrounding physical property. The Snosoft-HP case involves conflicting standards of reasonableness, emanating from different measuring sticks. The issue in this case was the reasonableness of disclosing a computer security vulnerability. Snosoft researchers uncovered a vulnerability in the Tru64 UNIX operating system distributed by Hewlett-Packard (HP).[10] Before disclosing the exploit to the public, Snosoft followed the informal custom of informing HP so as to give it time to develop a patch and disseminate it to the community of users. As a result of HP's failure to respond, a Snosoft researcher alerted the public to the flaw. In response, HP threatened Snosoft with violations of the federal Digital Millennium Copyright Act (DMCA) and Computer Fraud and Abuse Act.

On one hand, Snosoft claimed its actions were a reasonable application of its fair use rights under copyright law, the First Amendment right to free speech, and a reasonable

7. See, generally, Seanna Adcox, "Ziff Davis Agrees to Pay Settlement," Findlaw News and Commentary (visited August 29, 2002): *http://news.findlaw.com/ap_stories/f/1310/8-28-2002/20020828141503_76.html.*

8. See *http://www.ziffdavis.com/terms/index.asp?page=privacypolicy*.

9. Federal Trade Commission, "Privacy Online: A Report to Congress" (June 1998): *http://www.ftc.gov/reports/privacy3/priv-23a.pdf.*

10. See Declan McCullach, "Security Warning Draws DMCA Threat," CNET News.com (July 30, 2002): *http://news.com.com/2100-1023-947325.html.*

means to protect themselves and other Tru64 UNIX community members. HP invoked other legal mechanisms to justify the reasonableness of its actions to protect its copyrighted property. Although the debate surrounding the DMCA is well-published, contentious, and beyond the scope of this article, the significance of these conflicting values is that informal social pressure prevailed over institutionalized legal standards in defining reasonable network behavior.

Despite having the force of law and case precedent (to date, every lawsuit challenging the DMCA has failed) on its side regarding the DMCA's broad prohibition on circumventing copyright protection technologies, HP backed off of federal charges against the researchers who published the exploit. The case for Snosoft's reasonableness boiled down to the public support for this socially beneficial act of alerting potentially harmed parties who were denied knowledge and protection from the vendor. The power of this informal social pressure was surely manifest in the remnants of bad publicity that befell Adobe when it was embroiled with Dmitry Sklyarov over a similar issue. Similar to Ziff-Davis, the social sanctions (harm to reputation and commercial profitability) turned out to be a formidable ally in reaching some sort of consensus on right and wrong Internetwork behavior. HP's prior knowledge of the flaw, capability to rectify the vulnerability, wait-and-see approach, and reactionary attempt to use the law to counterattack did not gain it social popularity points.

Just as the Fourth Amendment has become the de facto reference point for defining "reasonableness" (in the search and seizure context) and has been interpreted by the US Supreme Court as a balancing test between conflicting interests, a similar weighing is evolving in the context of network behavior.

This is undoubtedly not the last time we will encounter the conflict between rights and property that DMCA brings about. Perhaps the introductory case of *Ford v. Swarens* holds greater significance and foresight than we are willing to acknowledge. As that scenario played out, the collectors returned for the last time to collect from Swarens, who, Ford admitted, was always current on his payments. Frustrated with their groundless visits, Swarens advised them that he would show them no more records, and strongly suggested that they leave his home . . . while brandishing a shotgun. They left, but first reminded him of their experience in the repossession of automobiles and promised him that they would repossess his.[11]

As we know, however, the court had little sympathy for the computer-error defense raised by Ford. Instead, it chose to use the context-dependent standard of reasonableness – a standard that humans must continually define if we wish to resolve digital repossessions and cyber gun-slinging conflicts that are sure to arise in our increasingly technology-centric interactions with one another.

11. *Ford Motor Credit Company v. Swarens*, 447 S.W.2d 53 (1969).