Chicago-Kent Law Review

Volume 84
Issue 3 *Symposium: Data Devolution: Corporate Information Security, Consumers, and the Future of Regulation*

Article 11

June 2009

Information Security, Contract and Liability

Jennifer Chandler

Follow this and additional works at: https://scholarship.kentlaw.iit.edu/cklawreview

Part of the Computer Law Commons, and the Contracts Commons

Recommended Citation

Jennifer Chandler, *Information Security, Contract and Liability*, 84 Chi.-Kent L. Rev. 841 (2010).
Available at: https://scholarship.kentlaw.iit.edu/cklawreview/vol84/iss3/11

This Article is brought to you for free and open access by Scholarly Commons @ IIT Chicago-Kent College of Law. It has been accepted for inclusion in Chicago-Kent Law Review by an authorized editor of Scholarly Commons @ IIT Chicago-Kent College of Law. For more information, please contact dginsberg@kentlaw.iit.edu.

INFORMATION SECURITY, CONTRACT AND LIABILITY

JENNIFER CHANDLER*

INTRODUCTION

Cyber security is a complex social problem for two reasons. First, the Internet has an insecure technical foundation,[1] and second, technology is changing rapidly, creating many possible points of failure.

I. VALUING THE PUBLIC GOOD

One of the key problems is that cyber security is a public good. Among the causes of cyber insecurity are the vulnerable or compromised computers of individual users, which are used to spread malware, spam, or other harmful communications. Individuals may invest in the security of their computers and so benefit both themselves and the public in general. However, in cases where the public benefits, the individuals do not capture all of the benefits from their investments in cyber security, and so they may not have sufficient incentives to make the level of investment that is optimal from the public perspective. The result is a classic free rider problem: people either wait for someone else to produce the security or, if they do invest, they do not produce the best kind or quantity of security.

A. *Free Riders and Investments in Security*

Law and economics scholars suggest that there are two types of private security investments. One type of investment tends to lower the amount of crime generally. This includes investments that help to detect and catch criminals as well as investments in hidden security measures that raise the general cost of committing crime, thereby decreasing the amount of crime. The second type of security investment merely shifts the crime

* Jennifer Chandler is a professor of law at University of Ottawa. This is the text of Professor Chandler's remarks at the Center for Information Research Conference. Jennifer Chandler, Address at the University of Florida's Center for Information Research Conference: Data Devolution: Corporate Information Security, Consumers and the Future of Regulation (Feb. 3–4, 2006).

[1] Jennifer A. Chandler, *Improving Software Security: A Discussion of Liability for Unreasonably Insecure Software, in* SECURING PRIVACY IN THE INTERNET AGE 155 (Chander, Gelman & Radin eds., 2007).

elsewhere and does not produce a net social benefit. Examples of the second type include visible security measures like locks on doors or windows, advertisements for security systems, or private security guards. The justification for this type of investment is self-interest; it provides protection by encouraging criminals to go elsewhere.

Interestingly, cyber security does not map neatly onto this dichotomy. Private self-protective measures in cyber security neither shift the crime elsewhere nor lower the level of crime by making crime less attractive. Instead, efforts taken to protect one's computer from compromise directly benefit many other people from harm in the form of distributed denial of service (DDoS) attacks,[2] spam, phishing, and the propagation of malware because networks of compromised computers are commonly used to launch these forms of attack. Therefore, a more accurate analogy between cyberspace and real space security investments would be to view cyber security measures as akin to barred windows that prevent a house from being occupied by a sniper bent on attacking others from the house. Thus, the issue is no longer the protection of an individual asset.

B. The Harms of Cyber Insecurity

Although computer security is primarily a concern of each computer owner, a large number of third parties depend on the security of other users' computers. This creates a situation where computer owners may take steps to protect their own computers for their own benefit and are willing to invest money and time to do so, but they will not necessarily want to take into account the interests of either these third parties or the public interest. As a result, information security is often insufficient to protect the public interest.

As mentioned above, an inadequately secured computer may be compromised and then integrated into a network of compromised computers known as a "botnet."[3] In some cases, botnet membership is not necessarily too great an inconvenience to the owner of the compromised computer, but the botnet may be used for a range of nefarious purposes against other Internet users. In other cases, the user of the computer directly bears the harm from the compromise of that user's computer, as is the case with spyware.

[2] For a discussion of denial of service attacks, see, for example, Jennifer A. Chandler, *Security in Cyberspace: Combatting Distributed Denial of Service Attacks*, 1 U. OTTAWA L. & TECH. J. 233, 233–37 (2004).

[3] For a discussion of botnets, see, for example, Jennifer A. Chandler, *Liability for Botnet Attacks*, 5 CAN. J.L. & TECH. 13, 13–18 (2006); Lilian Edwards, *Dawn of the Death of Distributed Denial of Service: How to Kill Zombies*, 24 CARDOZO ARTS & ENT. L.J. 23, 23–59 (2006).

Some forms of spyware stay on a computer, log key strokes, and try to intercept financial data for use in fraudulent transactions. Undoubtedly, this theft causes inconvenience to the person whose credit card number is compromised. Yet, considerable inconvenience is caused to others, such as merchants who become subjects of credit card charge backs after disputes of fraudulent transactions, and, by extension, all consumers who bear the increased cost of products due to the amount of fraud.

C. Creating Security-Enhancing Incentives Through Tort Liability

The question of how to deal with inadequate cyber security has become an international public policy problem. Two possible solutions are to impose liability for developing unreasonably insecure software and harboring botnets on networks.

Identification of an appropriate plaintiff is one of the obstacles in using tort law as a solution. For example, software flaws are key sources of computer insecurity. Yet, the purchasers of software are usually contractually bound by end user license agreements ("EULAs"), which contain generic disclaimers about fitness, functionality, or quality, as well as exclusions of liability exempting the vendors from any problems that arise from defects.[4] As a possible solution, a party not bound by an EULA could be the plaintiff.[5] For example, in the case of a DDoS attack, the target of the attack would make a logical plaintiff:[6] This party was harmed by an attack launched by the infected computers and is not bound by the relevant EULAs.[7] But this article focuses on the role of contracts, and so will not further discuss these tort arguments. Contractual provisions, particularly in software EULAs, can exacerbate the cyber security problem. Arguably, a legal solution is needed: either a regulation that invalidates certain types of provisions or a common law objection based on public policy.

II. CONTRACT

Various kinds of provisions found in software EULAs undermine cyber security.[8] The public cannot depend upon software purchasers to

[4] For a discussion of vendor liability, see, for example, Michael D. Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?*, 67 MD. L. REV. 425, 425–85 (2008).

[5] Chandler, *supra* note 1, at 155–58; Jennifer A. Chandler, *Security in Cyberspace: Combating Distributed Denial of Service Attacks*, 1 U. OTTAWA L. & TECH. J. 233, 233–37 (2004); Jennifer A. Chandler, *Liability for Botnet Attacks*, 5 CAN. J.L. & TECH. 13, 13–18 (2006).

[6] *Id.*

[7] *Id.*

[8] For further discussion, see Jennifer A. Chandler, *Contracting Insecurity: Software License Terms that Undermine Cybersecurity*, *in* HARBORING DATA: CORPORATIONS, LAW AND INFORMATION

resist these provisions for several reasons. First, there is an externality problem: People may consent to the terms that impose costs elsewhere because they either do not know or care enough about the external costs. Second, contracts sometimes insufficiently disclose the security-undermining features of software. In any event, disclosure is unlikely to help, given that people simply do not read EULAs. Thus, as a matter of contract law, the only viable way to discourage the inclusion of these kinds of terms and, therefore, to minimize these negative externalities is to refuse to enforce the harmful contractual terms and to deny legal protection to arrangements that undermine cyber security.

A. The Sony Rootkit

The Sony Rootkit debacle is an example of the problem of inadequate information disclosure in EULAs.[9] It involved "copy protection" or "digital rights management" software included on a number of Sony music CDs. The existence of the software was disclosed in the EULA, although it was questionable whether it was properly disclosed.[10] The rootkit was installed at a low level in a purchaser's computer, enabling writers of malware to design harmful programs to take advantage of the newly-introduced vulnerability. As the fiasco unfolded, Sony made available an uninstaller program, which created a further serious security risk, thus necessitating a second uninstaller for the first uninstaller.[11]

Predictably, a number of class actions and government investigations ensued, raising a number of claims, including those under the Computer Fraud and Abuse Act, under state laws prohibiting deceptive marketing practices and false advertising, and under various other grounds. A New York Court approved a settlement that contained several relevant terms,[12] including disclosure requirements for the installation of copy protection software and for the function of any updates or changes. The settlement also required Sony to obtain an opinion from an independent, qualified

SECURITY 3–6 (A.M. Matwyshyn, ed., 2009).

[9] For a discussion of the Sony Rootkit issues, see, for example, Bruce Schneier, *Real Story of the Rogue Rootkit*, WIRED, Nov. 17, 2005, http://www.wired.com/news/privacy/ 0,1848,69601,00.html.

[10] For the purposes of this article, it does not matter whether disclosure was adequate, because increased disclosure is likely insufficient to deal with the problem since people usually do not read EULAs.

[11] J. Alex Halderman, *Not Again! Uninstaller for Other Sony DRM Also Opens Huge Security Hole*, FREEDOM TO TINKER, Nov. 17, 2005, http://www.freedom-to-tinker.com/?p=931; John Leyden, *First Trojan using Sony DRM spotted. Roots you, Sir*, REGISTER, Nov. 10, 2005, http://www.theregister.co.uk/ 2005/11/10/ sony_drm_trojan/.

[12] Settlement Agreement, In re SONY BMG CD Technologies Litigation (S.D.N.Y. 2006) (No. 1:05-cv-0975).

third party that the copy protection software did not damage computer security, and that the software met some security standard.[13]

But because most users do not read EULAs, this improved disclosure alone seems unlikely to solve the problem. In this case, the copy protection software installed on users' computers benefits the licensor rather than the licensee, and also increases the vulnerability of computer systems. The software harms the owner of the computer as well as third parties because vulnerable computers may be compromised and used to launch attacks on third parties. Licensors should not be permitted to insulate themselves from complaints merely by disclosing the existence of such copy protection software in the EULA.

B. Network Associates Anti-Benchmarking Provisions

Another example concerning EULA disclosures occurred in 2003 when the Attorney General of New York sued Network Associates because of an anti-benchmarking provision in a Network Associates EULA that prohibited the publication of a comparison of its firewall product with others.[14] The New York Attorney General questioned whether it was in the public's interest to suppress this kind of information. More generally, the concern is that free and open discussion of software quality is necessary to both ensure public knowledge of defects and exert public pressure on software manufacturers to prevent or fix security vulnerabilities in their products.

Unfortunately, the New York Supreme Court did not actually rule on whether anti-benchmarking provisions are contrary to public policy or not.[15] Instead, the ruling was quite narrow and stated only that the particular provision in this case was deceptive.[16]

Anti-benchmarking provisions are another example of a contractual impediment to cyber security. A bench mark test is designed to test the performance of a software program and to make a meaningful comparison with similar software programs. On the one hand, these tests are useful to software purchasers who are unable to assess software quality and make well-informed purchase decisions on their own. On the other hand, software vendors argue that benchmark tests can be misleading because independent testers may either test the wrong version or pick inappropriate metrics. Where there are problems with a test, it is difficult for a software

[13] *Id.*

[14] Spitzer v. Network Assocs., Inc., 758 N.Y.S.2d 466 (N.Y. Sup. Ct. 2003).

[15] *Id.*

[16] *Id.*

vendor to criticize a benchmark test because the vendor's complaints are likely to be construed as sour grapes. As a result, vendors may have understandable reasons to wish to control benchmark testing of their products.

Anti-benchmarking provisions are a subset of a larger category of "contracts of silence," which are themselves very controversial. Confidential settlement agreements in the context of product liability dispute are another example of a contract in which a party agrees to remain silent in exchange for some benefit. These agreements are also controversial because they involve the suppression of publicly useful information. Although we do not wish to promote the public interest by forcing people to speak unwillingly, we should consider whether the law should promote freedom of contract so that contracts of silence are blindly enforced. Parties to a contract of silence will judge the contract's terms according to their private interests and are unlikely to consider the public harms and the full social cost of the contract.

III. NEGATIVE AND POSITIVE CONTRACT RIGHTS

These examples illustrate how contractual arrangements between consenting parties may erode cyber security. As a result, the next inquiry is whether courts should enforce these contractual arrangements. Before engaging in this inquiry, it is important to address the meaning of the idea of "freedom of contract."

One must distinguish the ability to engage in a transaction from the right to have the state enable that ability by enforcing a transaction. In liberal theory terms, this is the distinction between a negative and a positive right. Although liberalism is receptive to claims of negative rights—rights to be free of state interference in one's actions—it is another thing to make claims of positive rights that the apparatus and resources of the state be used in a positive sense to give effect to our own desires. The claim to "freedom of contract" confounds these two ideas of rights, but it is very important to keep the ideas separate when analyzing the appropriate role of the state in enforcing contracts.

The rhetoric of the freedom of contract should be set aside when determining whether contracts should be enforced. Courts must weigh the advantages of default rules that favor contractual enforcement, such as predictability and certainty, against the disadvantages of enforcing contracts that undermine the public interest. Even at the height of judicial deference to freedom of contract in the nineteenth century, judges invalidated contracts that they considered contrary to public policy. These included contracts deemed in restraint of trade, and those that pertained to sexual immorality as it was conceived at the time. As Atiyah's study of the freedom of contract argues, the only thing that has changed over the last couple hundred years is not the strength of freedom of contract, but the importance of the particular public policy that collides with the so-called freedom of contract.[17]

Although the refusal to enforce contracts that are contrary to public policy may undermine the value of freedom of contract, the doctrine of unenforceability on grounds of public policy is the doctrine best able to deal with externality problems. Certainly, judges are leery of using the doctrine of unenforceability on grounds of public policy. They are concerned that it is not their role to pronounce the public policy, and they do not have the resources or the ability to identify the various interests that might be affected by whatever they recognize and apply as public policy. Judges state that public policy determination is a job for the legislatures. Nonetheless, in some well-defined situations, judges are willing to act to promote public policy.

The Restatement (Second) of Contracts provides a general balancing test: A contract is unenforceable on grounds of public policy if the interest in its enforcement is clearly outweighed by a public policy against the enforcement of such terms.[18] As a legal test, this leaves a certain amount of specificity to be desired. The Restatement goes on to say that in making the determination, a court should consider the strength of the policy as manifested by legislation or judicial decisions.[19]

A. *Unenforceability and Public Policy*

Applying the Restatement approach to the two examples, the Sony Rootkit would be unlikely to generate a court pronouncement on public policy and the Sony EULA. But a term that exempts a party from tort liability for harm that was caused intentionally or recklessly is unenforceable on public policy grounds.[20] Arguably, Sony's rootkit constituted a recklessly-imposed harm, and, therefore, the liability disclaimers in the Sony EULA should not have been enforced. Vendors need a solid incentive to perform proper security testing, and the refusal to enforce disclaimers of liability would encourage this behavior. Accordingly, we should consider imposing strict liability on vendors whose copy protection software intro-

[17] P.S. ATIYAH, THE RISE AND FALL OF FREEDOM OF CONTRACT 778 (Oxford University Press 1985).

[18] *See* RESTATEMENT (SECOND) OF CONTRACTS § 178 (1979).

[19] *Id.*

[20] *Id.* § 195.

duces new security vulnerabilities in users' computers.

Turning to the anti-benchmarking provisions, it is unfortunate that the *Network Associates* court did not discuss the public policy implications of anti-benchmarking provisions. In my view, an anti-benchmarking provision should not be enforceable because (a) it suppresses critical information about software quality in a market with high information costs, and (b) other mechanisms exist to address the legitimate concerns of software developers. We have causes of action for trade libel and other ways to deal with improperly conducted bench mark tests. They may be cumbersome, but they exist.

B. *Future Paths*

Courts have demonstrated the desire to protect the information marketplace. In 1915, a newspaper, which advised Britons buying land in Canada, agreed not to comment on a particular land vendor in exchange for the forgiveness of a debt.[21] The English court stated that this was contrary to public policy because it was inconsistent with the proper role of a newspaper. This is a precedent for the judicial protection of the information market place.

States have also addressed problematic contractual provisions through statutory measures. A statute can directly prohibit certain kinds of contractual provisions. Under both Canadian and American consumer protection laws, consumers cannot waive certain rights that are provided under the legislation. This removes a degree of freedom of contract to protect consumers from themselves.

The third approach is illustrated by Canada's comprehensive federal statute that protects personal information privacy.[22] The statute provides that personal information can be collected if the affected people consent. It is thus a consent-based regime, which raises the possibility that parties might contract around its protections, contrary to the interests of the weaker parties. However, the statute provides that notwithstanding consent, personal information may be collected only for reasonable purposes—uses that a reasonable person would consider appropriate.[23] In other words, although individuals can consent to some things, there is a minimal floor that they cannot contract around.[24] The statute also provides that businesses cannot, as a condition of supplying a product or service, require someone to con-

[21] Neville v. Dominion of Canada News Co. Ltd., (1914) 3 Eng. Rep. 556 (K.B.).

[22] Personal Information Protection and Electronic Documents Act, 2000 C. Gaz., ch. 5 (Can.).

[23] *Id.*

[24] *Id.*

sent to the collection of personal information beyond that which is required to fulfill legitimate purposes.[25] This is an example of a method by which a minimum level of protection, defined by an objective standard, is guaranteed by statute.

In the end, either the courts or the legislature will need to take steps to limit the use of contractual provisions that undermine cyber security.

[25] *Id.*