Chicago-Kent Law Review

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

Article 8

June 2009

Best Practices and the State of Information Security

Kevin Cronin

BEST PRACTICES AND THE STATE OF INFORMATION SECURITY

KEVIN CRONIN*

INTRODUCTION

In a book you might have read, *The Hitchhiker's Guide to the Galaxy*,[1] researchers from a pan-dimensional, hyper-intelligent race of beings construct deep-thought super computers. They enlist the second greatest computer of all time to calculate the ultimate answer to the universe. After seven and one half million years of computations, this computer comes up with the answer, which is "42."[2] The person who asked the question responded, "42? What kind of answer is that?" and the computer replied, "Well, I checked it very thoroughly, and that quite definitely is the answer. I think the problem, to be quite honest, is that you have never really known the actual question to ask."[3]

With that in mind, I am not going to try to give the ultimate answer to data security because I do not think there is an ultimate answer to data security. If you asked a deep-thought computer what is the ultimate answer to data security, it would, of course, give you one of these dead answers like "42" and would probably chastise you for asking the wrong question. There is no ultimate answer for data security. The closest set of answers will probably be found in the building process.

* Kevin Cronin has worked with pharmaceutical and information technology companies for over 20 years, as a principal and consultant, and is a Senior Fellow at the Thomas Jefferson University School of Population Health. Before his current positions, he was the CEO of Praxeon, Inc., a health informatics company providing drug discovery and e-health services to biopharmaceutical companies, CROs, health insurers and other sectors of the healthcare industry, and was a senior partner in the law firm Blank Rome LLP, where he advised companies in connection with mergers and acquisitions and technology matters.

Prior to practicing law, Kevin designed software and conducted research in pulmonology medicine and respiratory devices. He is the author of *Data Security and Privacy Law* (Thomson-Reuters/West Group), a comprehensive treatise on health IT and Internet law. Kevin received his law degree from Washington University and his undergraduate degree in biological sciences from the University of Chicago.

1. DOUGLAS ADAMS, HITCHHIKER'S GUIDE TO THE GALAXY (1979).
2. *Id.*
3. *Id.*

I. CORPORATE DATA SECURITY—AN INTRODUCTION

A. Corporate Data Security as a Corporate Governance Issue

Data security was once the domain of IT departments. However, what has happened in the past several years is that new regulations, statutes, agency enforcement actions, and private litigation actions have made data security a core concern for almost all corporations. This may be especially true for public corporations, but data security concerns extend even to private corporations. Security is no longer only an IT issue; rather, it is also a corporate governance issue critical to the future of corporations.[4]

Another thing that has happened in the past few years—maybe after the beginning of the shift of data security toward being more of a core corporate issue—is a movement toward establishing concrete standards for data security. This is a slow process, and we are not there yet. However, we are moving towards minimum standards of care. I will describe a little bit about this movement and where I think it is with regard to legal standards for data security. What I am going to try to do is elucidate just what these standards are. What does a company have to do with respect to data security and where is the bright line? Is there a bright line? What does a company have to do to discharge the statutory obligations for data security?

B. What is Corporate Data Security?

Data security means employing security measures to protect assets such as data, people, and infrastructure against threats. It is critical to realize that there is no such thing as absolute security in data security. Essentially, the only way to protect a computer from Internet threats is to unplug it, both from a telecommunication connection and from the wall. That would make your computer secure but, obviously, useless.

If we are plugged in, we are always going to have to live with some level of data security that is not absolute; the only question is whether we are more secure or less secure. Because there is no absolute security, the

4. For a discussion of corporate governance issues, see generally, Carter G. Bishop, *The Deontological Significance of Nonprofit Corporate Governance Standards: A Fiduciary Duty of Care Without a Remedy*, 57 CATH. U. L. REV. 701, 727–57 (2008); Alan Dignam & Michael Galanis, *Corporate Governance and the Importance of Macroeconomic Context*, 28 OXFORD J. LEGAL STUD. 201 (2008); Yair Listokin, *Interpreting Empirical Estimates of the Effect of Corporate Governance*, 10 AM. L. & ECON. REV. 90 (2008); Richard E. Mendales, *Intensive Care for the Public Corporation: Securities Law, Corporate Governance, and the Reorganization Process*, 91 MARQ. L. REV. 979 (2008); Houman B. Shadab, *Innovation and Corporate Governance: The Impact of Sarbanes-Oxley*, 10 U. PA. J. BUS. & EMP. L. 955 (2008); Betty Simkins & Steven A. Ramirez, *Enterprise-Wide Risk Management and Corporate Governance*, 39 LOY. U. CHI. L.J. 571 (2008).

standards that I am going to introduce do not require a guarantee of security. The three measures involved in data security are: (1) technical measures; (2) physical measures; and (3) administrative measures.

Technical security measures are safeguards incorporated into hardware, software, and related devices. Among other things, they are designed to improve system availability and to provide access control. On the other hand, physical security measures are those that are intended to protect tangible items such as the actual computers from destruction through real-space immobilization or damage. Finally, administrative measures are procedural management controls that an administrator or auditor uses to provide protection for a network. Security is all about defining targets, goals, and processes[5] for achieving goals in a way that best implements and discharges data security duties under statutory and common law.

Similarly, three subcategories exist under each of the main security measure categories just discussed: (1) preventative measures; (2) detective measures; and (3) reactive measures. Preventive measures include firewalls and antivirus software. Detective measures involve figuring out when you are being attacked by using methods such as recording attacks, intrusion detection, and port scans.[6] Reactive measures involve reacting once there is a breach of security or threatened breach of security and include measures such as shutting down systems and getting law enforcement involved.

The types of attacks and threats that are part of security involve theft, damage, destruction, or interference with the operation of the computer or network. Those things can be "acts of god" or unintentional acts such as natural disasters, infrastructure failures, hurricanes, and power outages. These attacks and threats can also be intentional acts like intentional destruction of computer equipment, damage from malware, viruses, spyware, or worms, and denials-of-service attacks. The last types of threats are social, or people-related, threats. These come from individuals directly attacking either the network or computer system. An example of such a social threat is an employee compromising or stealing credit card data.[7]

5. For a discussion of the basics of information security, see generally ROSS J. ANDERSON, SECURITY ENGINEERING: A GUIDE TO BUILDING DEPENDABLE DISTRIBUTED SYSTEMS (2001).

6. Port scans are queries sent to servers to receive information about the extent of security on the system and what services are running. *See* ZDNet, Port Scan: Definition, http://dictionary.zdnet.com/index.php?d=port+scan (last visited Mar. 10, 2009).

7. For a discussion of insider/outsider threats, see generally Susan W. Brenner & Leo L. Clarke, *Distributed Security: Preventing Cybercrime*, 23 J. MARSHALL J. COMPUTER & INFO. L. 659, 681 (2005); Jennifer A. Chandler, *Security in Cyberspace: Combatting Distributed Denial of Service Attacks*, 1 U. OTTAWA L. & TECH. J. 231 (2004); Michael L. Rustad, *The Negligent Enablement of Trade Secret Misappropriation*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 455 (2006); Karen Sepura, Note, *Economic Espionage: The Front Line of a New World Economic War*, 26 SYRACUSE J. INT'L. L.

Social threats also include an individual who is implementing one of the technical threats mentioned above.

What are the goals of data security? They are five-fold: availability, access, confidentiality, integrity, and authenticity.[8] Every data security process has some variant of these five goals. These goals are reflected in the framework of the legislation that dictates data security standards.

II. THE EMERGING LAW OF INFORMATION SECURITY

A growing number of federal and state[9] statutes govern data security. These statutes prescribe details regarding the rules for data security standards.[10] Contractual obligations are another source of data security standards, as nearly all corporate transactions include requirements to safeguard data. Such contractual obligations insure that industry best standards or best practices are being used in collecting, safeguarding, and destroying data. Finally, courts are beginning to incorporate negligence law into data security litigation.

A. Statutes

Until recently, most laws addressing information security stated that companies needed to use reasonable standards to safeguard data, but, they did not go any further. Consequently, those statutes only gave a general prescription for data security. Today, some new laws like the Children's Online Privacy Protection Act (COPPA),[11] the Gramm–Leach–Bliley Act (GLBA),[12] the Health Insurance Portability and Accountability Act

& COM. 127 (1998).

8. *See* ANDERSON, *supra* note 5, at 120.

9. *See* National Conference of State Legislatures, State Security Breach Notification Laws, http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm (listing current data breach notification statutes from forty-four states) (last visited Dec. 19, 2009).

10. *See* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 918 (2007) (arguing in favor of creating a coordinated response architecture and developing the elements of such an approach with a "coordinated response agent" that oversees steps for automatic consumer protection and heightens mitigation).

11. For a discussion of the Children's Online Privacy Protection Act (COPPA), see generally Joseph A. Zavaletta, *COPPA, Kids, Cookies & Chat Rooms: We're From the Government and We're Here to Protect Your Children*, 17 SANTA CLARA COMPUTER & HIGH TECH. L.J. 249, 253–55 (2001); Danielle J. Garber, Note, *COPPA: Protecting Children's Personal Information on the Internet*, 10 J.L. & POL'Y 129, 153–60 (2001); Melanie L. Hersh, Note, *Is COPPA a Cop Out? The Child Online Privacy Protection Act as Proof That Parents, Not Government, Should Be Protecting Children's Interests on the Internet*, 28 FORDHAM URB. L.J. 1831, 1853–56 (2001); Joshua Warmund, Note, *Can COPPA Work? An Analysis of the Parental Consent Measures in the Children's Online Privacy Protection Act*, 11 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 189, 194–201 (2000).

12. For a discussion of the Gramm-Leach-Bliley Act (GLBA), see generally R. Bradley McMa-

(HIPAA),[13] and other statutes such as the FTC Act[14] and the Homeland Security Act,[15] are moving toward defining specific process-based standards for data security. These new standards are not only about using reasonable technical standards in a company's security determination; they are also about the adequacy of the specific process by which a company goes through to safeguard or to establish data security. The statutes are beginning to define information security specifically, not just generally. They address the protection of information systems from unauthorized access, use, disclosure, disruption, and the preservation of integrity, confidentiality, availability, and proper authentication.[16]

In the future, we will probably hear more about process based security; security through obscurity[17] is finally dead or should be dead. Technical

hon, Note, *After Billions Spent to Comply with HIPAA and GLBA Privacy Provisions, Why Is Identity Theft the Most Prevalent Crime in America?*, 49 VILL. L. REV. 625, 633–38 (2004); Jason Shroff, Note, *California: A Privacy Statute Meets the GLBA & FCRA*, 9 N.C. BANKING INST. 223, 226–27 (2005).

13. For a discussion of the Health Insurance Portability and Accountability Act (HIPAA), see generally Cicely N. Tingle, *Developments in HIPAA and Health Information Technology*, 3 I/S: J. L. & POL'Y FOR INFO. SOC'Y 677, 678–81 (2008); Kirsten N. Arnold, Note, *Getting Payment for a Clean Bill of Health: Reconciling the Health Insurance Portability and Accountability Act ("HIPAA") with the Fair Debt Collection Practices Act ("FDCPA") for Health-Care Debt Collection*, 93 IOWA L. REV. 605, 611–14 (2008); Joshua D.W. Collins, Special Project Note, *Toothless HIPAA: Searching for a Private Right of Action to Remedy Privacy Rule Violations*, 60 VAND. L. REV. 199, 200–03 (2007); Dustin C. George, Comment, *HIPAA, the Privacy Rule, and the Texas Public Information Act: How Texas Health and Human Services Agencies Should Referee the Game of Exception Ping-Pong That These Laws Play*, 8 TEX. TECH. ADMIN. L.J. 277, 280–82 (2007); Daniel J. Oates, Comment, *HIPAA Hypocrisy and the Case for Enforcing Federal Privacy Standards Under State Law*, 30 SEATTLE U. L. REV. 745, 748–50 (2007).

14. For a discussion of the FTC Act, see generally Julie L. Williams & Michael S. Bylsma, *On the Same Page: Federal Banking Agency Enforcement of the FTC Act to Address Unfair and Deceptive Practices by Banks*, 58 BUS. LAW. 1243 (2003); Michael A. Rabkin, Comment, *When Consumer Fraud Crosses the International Line: The Basis for Extraterritorial Jurisdiction Under the FTC Act*, 101 NW. U. L. REV. 293, 297–99 (2007).

15. For a discussion of the Homeland Security Act, see generally Karen E. Jones, Comment, *The Effect of the Homeland Security Act on Online Privacy and the Freedom of Information Act*, 72 U. CIN. L. REV. 787, 790–93 (2003).

16. *See, e.g.*, Catherine Guthrie & Brittan Mitchell, *The* Swinton *Six: The Impact of* State v. Swinton *on the Authentication of Digital Images*, 36 STETSON L. REV. 661 (2007) (discussing the legal meaning of authentication); William J. Haddad, *Authentication and Identification of E-Mail Evidence*, 96 ILL. B.J. 252, 253–54 (2008) (same); Ritu Singh, *Two-Factor Authentication: A Solution to Times Past or Present? The Debate Surrounding the Gramm-Leach-Bliley Security Safeguards Rule and the Methods of Risk Assessment and Compliance*, 2 I/S: J. L. & POL'Y FOR INFORMATION SOC'Y 761 (2006) (same).

17. *See, e.g.*, Andrea M. Matwyshyn, *Material Vulnerabilities: Data Privacy, Corporate Information Security, and Securities Regulations*, 3 BERKELEY BUS. L.J. 129 (2005) (discussing security through obscurity); Andrea M. Matwyshyn, *Technoconsen(t)sus*, 85 WASH. U. L.R.. 529, 538 n.39 (2007) (same); Peter P. Swire, *Privacy and Information Sharing in the War on Terrorism*, 51 VILL. L. REV. 951 (2006) (same); Peter P. Swire, *A Theory of Disclosure for Security and Competitive Reasons: Open Source, Proprietary Software, and Governmental Systems*, 42 HOUS. L. REV. 1333 (2006) (same); Daniel P. Tokaji, *The Paperless Chase: Electronic Voting and Democratic Values*,73 FORDHAM L. REV. 1711 (2005) (same).

standards and legal standards can be similar, but what companies are doing technically is not necessarily the same as the legal standard. Similarly, the legal standard is not always reflective of the state-of-the-art technical standard.[18] There is, however, a significant overlap between the technical and the legal standard, and we are seeing a parallelism between the process-based paradigms of data security show up in law.[19] For example, the GLBA has a very process-based prescription for data security.[20]

B. Contract

Organizations engaged in computer processing frequently outsource their computer operations; accordingly, they will need an agreement to guarantee a certain level service. Often, these agreements include provisions dictating data security standards, and some courts have held companies to these standards and awarded hefty damages where the standards were not met. For example, Verizon was sued for system outages that were precipitated by the "Slammer worm" a few years ago.[21] The Slammer worm[22] shut down Verizon's operations in some sectors of the East coast, and damages were awarded for these outages under existing customer contracts. Verizon said that these outages were not its fault because they were hit by the worm.[23] However, Verizon waited six months to implement critical system patches that would have eliminated the vulnerability to the worm,[24] something the court deemed a breach of the service-level agreement.[25] These service-level agreements are commonly being negotiated now, but data security is not absolute. Inevitably, someone may be able to compromise your system, and there is no guarantee that you will have ab-

18. *See* Matwyshyn, *Technoconsen(t)sus*, *supra* note 17, at 541 (discussing the conflict between the legal standard and new technology).

19. *See* Matwyshyn, *Material Vulnerabilities*, *supra* note 17, at 134.

20. *See, e.g.*, Thomas J. Smedinghoff, *The Emerging Law of Data Security: A Focus on the Key Legal Trends*, 934 PLI/PAT 13 (2008) (discussing the Gramm-Leach-Bliley security regulations).

21. *See, e.g.*, Reply Comments of Verizon Virginia Inc. on its Petition For a Waiver of Certain Service Quality Results Measured under the Performance Assurance Plan for January 2003, http://www.scc.virginia.gov/puc/comp/ccimom/ccimomfiles/vrespslam.pdf (last visited Dec. 10, 2009) (discussing Verizon's problems with Slammer).

22. *See, e.g.*, Susan Landau, *National Security on the Line*, 4 J. TELECOMM. & HIGH TECH. L. 409 (2006) (discussing the Slammer worm); Meiring de Villiers, *Opinionated Software*, 10 VAND. J. ENT. & TECH. L. 269 (2008) (same); *see generally* Richard W. Downing, *Thinking Through Sentencing in Computer Hacking Cases: Did the U.S. Sentencing Commission Get it Right?*, 76 MISS. L.J. 923 (2007) (discussing hacking worms).

23. *See* Reply Comments, *supra* note 21.

24. *See id.*

25. For a discussion of Verizon's patching time table, see Erin E. Kenneally, The Byte Stops Here: Duty and Liability for Negligent Security, http://www.stanford.edu/class/msande91si/www-aut04/aut04/slides/erinCSIpresent.ppt (last visited Mar. 10, 2009).

solute security.

Another interesting case is the *Pharmatrack*[26] case, which involved a website search engine vendor that provided services to pharmaceutical companies. Pharmatrack collected data that it should not have been collecting, and a class-action lawsuit ensued. A number of the pharmaceutical company defendants pointed to the disclaimers and specific security requirements of the vendor's contract, which explicitly restricted the vendor from collecting personally identifiable information.[27] The court used the language of this agreement to support a motion for summary judgment on behalf of the pharmaceutical companies.[28]

C. *Negligence*

An interesting theory of possible data security liability is negligence.[29] We are seeing more interest in suing companies under negligence theories for violation of a duty of care and a breach of data security standards. The elements of a negligence case, of course, are duty,[30] breach,[31] causation,[32]

26. *See In re* Pharmatrak, Inc., 329 F.3d 9, 12 (1st Cir. 2003).

27. *Id.*

28. *Id.* at 17.

29. *See, e.g.*, John S. Gray & Richard O. Faulk, *"Negligence in the Air?": Should "Alternative Liability" Theories Apply in Lead Paint Litigation?*, 25 PACE ENVTL. L. REV. 147 (2008) (discussing alternative negligence liability); Michelle M. Mello & David M. Studdert, *Deconstructing Negligence: The Role of Individual and System Factors in Causing Medical Injuries*, 96 GEO. L.J. 599 (2007) (discussing negligence); Perry A. Zirkel & John H. Clark, *School Negligence Case Law Trends*, 32 S. ILL. U. L.J. 345 (2008) (same); Brian M. Serafin, Current Development, *Comparative Fault and Contributory Negligence as Defenses in Attorney Breach of Fiduciary Duty Cases*, 21 GEO. J. LEGAL ETHICS 993 (2008) (same).

30. *See, e.g.*, John C.P. Goldberg & Benjamin C. Zipursky, *Shielding Duty: How Attending to Assumption of Risk, Attractive Nuisance, and Other "Quaint" Doctrines Can Improve Decisionmaking in Negligence Cases*, 79 S. CAL. L. REV. 329 (2006) (discussing negligence duty); David Hunter & James Salzman, *Negligence in the Air: The Duty of Care in Climate Change Litigation*,155 U. PA. L. REV.1741, 1744 (2007) (same); Faith J. Jackson, *A Streetcar Named Negligence in a City Called New Orleans—A Duty Owed, A Duty Breached, A Sovereign Shield*, 31 J. MARSHALL L. REV.557, 557 (2006) (same); Nils Jansen, *Duties and Rights in Negligence: A Comparative and Historical Perspective on the European Law of Extracontractual Liability*, 24 OXFORD J. LEGAL STUD. 443 (2004).

31. *See, e.g.*, Patrick J. Kelley, *Restating Duty, Breach, and Proximate Cause in Negligence Law: Descriptive Theory and the Rule of Law*, 54 VAND. L. REV. 1039, 1041 (2001) (discussing breach in negligence); William B. L. Little, *"It is Much Easier to Find Fault with Others, Than to be Faultless Ourselves": Contributory Negligence as a Bar to a Claim for Breach of the Implied Warranty of Merchantability*, 30 CAMPBELL L. REV. 81 (2007) (same); Michael L. Rustad & Thomas H. Koenig, *Extending Learned Hand's Negligence Formula to Information Security Breaches*, 3 I/S: J. L. & POL'Y FOR INFORMATION SOC'Y 237 (2007) (same).

32. *See, e.g.*, Clarence Morris, *Duty, Negligence and Causation*, 101 U. PA. L. REV. 189 (1952) (discussing negligent causation); Paul Homer, Comment, *Invisible Injury Negligence Cases – Proving Causation Among Multiple-Source Polluters: A State-by-State Survey of the Law for New England, and a Proposal for a New Causation Framework*, 3 PIERCE L. REV. 75 (2004) (same).

and damages.[33] However, the economic loss doctrine[34] prevents a plaintiff from receiving an award of damages for non-physical injury and this doctrine often acts as a bar in data-loss cases.

Another problem when using the negligence theory in data security litigation is articulating the appropriate standard of care.[35] What goes into a comprehensive data security program? How do you assess the risk? How do you plan? How do you develop security measures? In the end, you have to continuously review and revise the program—the key is evolution. The process has to evolve; it has to be dynamic.

As mentioned above, there is a distinction between technical standards and legal standards, but there is an overlap as well. Statutes are starting to be modeled after technical standards. A company violates technical standards for data security at its own peril because these technical standards might be the standards that apply under a statute or under principals of negligence.[36] Particularly when the negligence-per-se doctrine[37] is applied, violation of a statutory standard could lead to a negligence action; this is true even if the statue does not describe a private right of action.[38] How do technical standards come into play? For example, Visa and Mastercard have what are called "PCI Data Security" guidelines.[39] Banks, vendors, and retailers are being held responsible for violation of the PCI guidelines.[40] The guidelines are fairly rigorous and can carry steep penalties for failing to abide by them.

The complicated nature of these questions becomes evident in the real world. One of my clients, a large national retailer, came to be known, to the company's chagrin, for losing approximately 400,000 credit card num-

33. *See, e.g.*, Phillip M. Kannan, *A New Approach to Defining and Computing Comparative Negligence Damages*, 23 MEM. ST. U. L. REV. 173 (1992) (discussing negligent damages); Kevin L. Austin, Note, *Punitive Damages in Negligence Cases: The Conflicting Standards*, 60 MO. L. REV. 693 (1995).

34. *See, e.g.*, Ralph C. Anzivino, *The Economic Loss Doctrine: Distinguishing Economic Loss From Non-Economic Loss*, 91 MARQ. L. REV. 1081 (2008) (discussing the economic loss doctrine).

35. *See, e.g.*, Sande L. Buhai, *Act Like a Lawyer, Be Judged Like a Lawyer: The Standard of Care for the Unlicensed Practice of Law*, 2007 UTAH L. REV. 87 (discussing standards of care); Drew Millar, Note, *Judicially Reducing the Standard of Care: An Analysis of the Bad Faith/Gross Misjudgment Standard in Special Education Discrimination*, 96 KY. L.J. 711 (2008) (same).

36. *See* Andrew E. Costa, *Negligence Per Se Theories in Pharmaceutical & Medical Devices Litigation*, 57 ME. L. REV. 51, 81 (2005).

37. *See, e.g., id.* (discussing negligence per se); Caroline Forell, *Statutory Torts, Statutory Duty Actions, and Negligence Per Se: What's the Difference?*, 77 OR. L. REV. 497 (1998) (same).

38. *See* Costa, *supra* note 36, at 53; Forrell, *supra* note 37, at 525.

39. *See, e.g.*, PCI Compliance Guide: A Five Step Guide for Gaining PCI Compliance, http://www.pcicomplianceguide.org/aboutpcicompliance.html (last visited Dec. 10, 2009) (discussing PCI guidelines).

40. *See id.*

bers—potentially triggering instances of identity theft. They received a lot of bad publicity. In this case, the question was whether the retailer had a duty not to collect certain information. Hackers—probably sitting in the parking lot or someplace close to their buildings—hacked into the main transaction processing systems of this client and downloaded a large amount of credit card information.

When you swipe a credit card, information that you do not see is transferred. It is not just your name, the expiration date, and the credit card number; there are all kinds of authorization code data on that strip. Some additional information used for verification and approval purposes was not supposed to be collected by this company; but this company, apparently in violation of the Visa PCI Standards, actually collected and retained this data. Because of this retention, the hackers had all the data needed to print actual credit cards. Naturally, litigation arose because credit card holders lost a significant amount of money as a result of this incident.

III. CONCLUSION

Cases involving liability for data breaches are just beginning to find their way into the court system. In the coming years, many of these issues will require much greater attention. The United States will need to move from a fragmented approach towards data security and privacy standards, towards a more comprehensive set of standards with new penalties and effective enforcement in order to better reflect the inherent value of personal data in today's global marketplace.