Journal of Technology Law & Policy

Volume XIV – Spring 2014

ISSN 2164-800X (online)

DOI 10.5195/tlp.2014.143

http://tlp.law.pitt.edu

Introduction: Cybersecurity in Pittsburgh

Kevin D. Ashley

Introduction: Cybersecurity in Pittsburgh

Kevin D. Ashley*

Like subatomic particles racing through a laboratory cloud chamber, consumers today leave traces, albeit digital ones, as they conduct their lives and transact their business via the Internet. Digital traces are created when we use a credit or debit card to pay for a Web purchase, receive a paycheck by direct deposit, file a tax return online, drive through a tollbooth with EZpass, engage in electronic banking, send an email, view a website, turn on a cellphone. Sometimes the data may be intercepted at its source or en route. In the normal course, however, it is stored in repositories connected to the Internet, where it may be analyzed and interrelated with other data to generate a remarkably complete picture of our lives, our preferences, and our very identities. These traces have value, not only to commercial marketers and government investigators, but also to hackers and thieves who can sell or manipulate them.

In the first few months of 2014, the citizens of Pittsburgh, presumably not an unrepresentative American urban center, learned of a number of disturbing events.

1) U.S. Attorney for the Western District of Pennsylvania, David J. Hickton, announced the indictment of five defendants accused of using identify theft and fraud to collect $10 million by, among other things, electronically filing tax returns in the names of some 2,400 victims, fraudulently seeking tax refunds, and directing

* Kevin D. Ashley is an expert on computer modeling of legal reasoning and cyberspace legal issues. He has reported his research in conference proceedings of the American Association for Artificial Intelligence, the International Association for Artificial Intelligence and the Law, and the Cognitive Science Society. He has also published in journals such as IEEE Expert, International Journal of Man/Machine Studies, and Journal of Artificial Intelligence and the Law, of which he is a member of the editorial board. Professor Ashley is a Principal Investigator of a number of National Science Foundation grants to study reasoning with cases in law and professional ethics. Professor Ashley is also the author of *Modeling Legal Argument: Reasoning with Cases and Hypotheticals* (MIT Press/Bradford Books 1990). A former National Science Foundation Presidential Young Investigator, Professor Ashley was also a visiting scientist at the IBM Thomas J. Watson Research Center, and a recipient of an IBM Graduate Research Fellowship. He is a member of the American Association for Artificial Intelligence, and Vice President of the International Association of Artificial Intelligence and Law. In addition to his appointment at the School of Law, Professor Ashley is a research scientist at the Learning Research and Development Center, an adjunct associate professor of computer science at the University of Pittsburgh, and a faculty member of its Graduate Program in Intelligent Systems.

Journal of Technology Law & Policy

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.143 ● http://tlp.law.pitt.edu

them to be paid into bank accounts the defendants set up, in the names of the unknowing victims, at financial institutions like PNC Bank.[1]

2) In April, the University of Pittsburgh Medical Center ("UPMC") reported that a data breach announced in February as affecting only a few dozen employees actually compromised the personal information of nearly 27,000 employees, hundreds of whom had experienced tax frauds or unauthorized bank withdrawals.[2]

3) Last December, Target officials revealed a massive security breach at Target stores; hackers stole credit card information of more than 40 million shoppers. Four months later, Target announced that the personal contact information of 70 million people had also been taken. A week later, the Pennsylvania Attorney General warned consumers of "phishing" attacks aimed at luring customers concerned about damaged credit into revealing yet more confidential information.[3]

Given news reports like these and others involving the National Security Agency and foreign government-sponsored cyber attacks, citizens and consumers rightly feel worried. Society's abject dependence on computers and networks is nearly total, and the subsequent risks to individuals and institutions have become palpable. The perpetrators are hidden and mysterious, availing themselves of the Internet's unprecedented opportunities for anonymously perpetrating bad actions at a distance, beyond the territorial reach of law enforcement. Who else can help? Who else can be held responsible?

In response to these risks, experts in technology and law have been developing a new field of research and practice: Cybersecurity. Following the suggestion of Prof. David Thaw, an expert in cybersecurity and privacy regulation who will soon join the faculty of the University of Pittsburgh Schools of Law and of Information Science, the term "cybersecurity," as employed here, refers to the "information security measures that custodians of consumer data take to protect

---

[1] Rich Lord, *5 indicted in massive identity-theft scheme, Young people, PNC Bank among victims*, PITTSBURGH POST-GAZETTE, Apr. 23, 2014, 12:00 PM, http://www.post-gazette.com/local/city/2014/04/23/5-indicted-in-massive-identity-theft-scheme/stories/201404230170.

[2] Deborah M. Todd, *UPMC data breach could be part of a national scheme, Health care providers across the nation have been targeted by cybercriminals*, PITTSBURGH POST-GAZETTE, Apr. 18, 2014, 12:00 PM), http://www.post-gazette.com/business/2014/04/19/UPMC-could-have-mitigated-cyber-damage-experts-say/stories/201404190049.

[3] Andrew McGill, *Con artists target Target patrons, AG Kane warns of fraud against unwary victims*, PITTSBURGH POST-GAZETTE, Jan. 13, 2014, 10:04 AM), http://www.post-gazette.com/business/technology/2014/01/14/Con-artists-target-Target-patrons/stories/201401140105.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.143 ● http://tlp.law.pitt.edu

such sensitive information,"[4] including, for instance, certain personally identifiable information, financial information, protected health information, and student educational records.[5] The custodians of consumer data include merchants like Target, employers like UPMC, financial institutions like PNC Bank, government agencies like the IRS, and those federal and state agencies that regulate, or could regulate, the above. Information security measures include the "administrative, technical, and physical methods and practices involved in maintaining the regulatory standards imposed on private data custodians."[6]

The student authors of the Pittsburgh Journal of Technology Law & Policy's Spring Article Series explore some of these issues. In *An Era of Rapid Change: The Abdication of Cash & The FTC's Unfairness Authority*, Elie Freedman explores the scope of the Federal Trade Commission's ("FTC's") power to require companies to provide information security for electronically collected and stored personal information. Robert Gyenes, in *A Voluntary Cybersecurity Framework Is Unworkable—Government Must Crack the Whip*, considers the utility of the threat of liability under federal regulation as an incentive to companies' strengthening protections against cyber attacks. Lawyers' responsibilities for protecting confidential information stored in the "Cloud" is the subject of Leah Lach's *Throwing New Flags: Criminal or Civil Sanctions for Lawyers or Service Providers Who Breach Confidentiality?* Larry McIntyre also focuses on data stored in "cloud services" and its susceptibility to government seizures in *Cyber-Takings: The War On Crime Moves Into the Cloud*.

As these articles exemplify, the history of law in Cyberspace is a tale of exploring the tradeoffs in different ways to incentivize the actors on the digital stage to preserve the advantages, while protecting against the risks, of a brave, new digitally connected world.

[4] David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. L. REV. 6 (2014), *available at* http://dx.doi.org/10.2139/ssrn.2241838.

[5] *Id.* at n.13.

[6] *Id.* at 6.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.143 ● http://tlp.law.pitt.edu