Introduction

Cyberwars: Navigating Responsibilities for the Public and Private Sector

Denis Binder

The *Chapman Law Review* is pleased to present this Symposium, carrying on our tradition of sponsoring an annual symposium on a timely subject. Our first Symposium in 1999 was "Tax Policy for the New Millennium." Our topic this year is "Cyberwars: Navigating Responsibilities for the Public and Private Sector," a subject which seemingly becomes more pressing each year as the number and impact of cyber breaches escalate. Indicating its relevance, Congress in the recently adopted Omnibus Budget Act of 2015 included the Cybersecurity Act of 2015.

Companies that have been the victims of cyber hacking include Anthem BlueCross, Chick-fil-A, Citigroup, Dairy Queen, Dominos, eBay, Goodwill, Home Depot, Hyatt Hotels, Jimmy Johns, Kmart, Michaels, JPMorgan Chase, Morgan Stanley, the *New York Times*, Neiman Marcus, Panda Express, P.F. Chang's, Target, Skype, Snapchat, SONY, Staples, SUPERVALU (Albertsons), UPS, U.S. Steel, VTech, the *Wall Street Journal*, Wyndham Hotels, and even the computer giants Apple, Facebook, Google, Microsoft, Twitter, and Yahoo. Sports teams have been hacked.

The federal government is not immune; not even the Pentagon or Department of Homeland Security. Other federal agencies that have been penetrated include the Postal Service, the Department of Energy, the Department of the Interior Department, the State Department, the National Oceanic and Atmospheric Administration, the Veterans Administration, and the Office of Personnel Management.

Hacked universities include Ohio State, UCLA, and USC. High school students have illegally hacked academic record systems to change grades. Hospitals have been victimized. Law firms have proven vulnerable to hacking.[1] Political figures who

[1] Estimates are that most of the major law firms have been hacked, but few wish to

have become victims include 2008 vice presidential candidate Sarah Palin.[2]

However, the data breach which has probably caused the most angst to individuals—mostly men[3]—was of the Ashley Madison site. The SONY[4] and Target[5] invasions also sent strong warnings to businesses to safeguard their sites.

The automobile revolutionized the twentieth century American lifestyle. The automobile opened up the suburbs and shrank the central city. Retailers moved to suburban malls and strip malls throughout the suburbs. The suburbs more recently morphed into exurbs. Land-use planning radically changed as the metropolitan areas chewed up the rural surroundings. Leisure time meant travel. Citizens could vacation at previously remote parks and forests.

The automobile did have its adverse consequences. Downtowns were drained of their vitality. Highways devoured farmland, divided neighborhoods, and destroyed wildlife and ecosystems. Smog engulfed urban areas, most notably Los Angeles. The automobile resulted in auto accidents with deaths of up to 50,000 annually, often involving alcohol. It created a new crime—grand theft auto.

However, it is the microchip that is defining the twenty-first century. Yesterday's economic juggernaut of Detroit, the center of the automobile revolution, is now Silicon Valley, the center of the high-tech revolution. The Information Age is the transformative force of the twenty-first century.

The mechanical revolution of the early twentieth century was challenged in the late 1900s by high technology, beginning with IBM's mainframe 360 Computer, and then the minis on Massachusetts' Route 128.

The Computer Age had arrived, but not yet as a revolution.

Under the aegis of Stanford's Dean of Engineering and then Provost Frederick Terman, two engineering graduates, David Packard and William Hewlett, set up shop in a Palo Alto garage. Thus was the rise of Silicon Valley, which has come to symbolize

come forward publicly for fear of clients discovering the firm has been unable to secure the clients' confidentiality.

[2] M.J. Stephy, *Sarah Palin's E-Mail Hacked*, TIME (Sept. 17, 2008), http://content.time.com/time/politics/article/0,8599,1842097,00.html [http://perma.cc/HGX6-UW97].

[3] Matt Rosoff, *Ashley Madison Was a Bunch of Dudes Talking to Each Other, Data Analysis Suggests*, BUS. INSIDER (Aug. 26, 2015, 7:31 PM), http://www.businessinsider.com/ashley-madison-almost-no-women-2015-8 [http://perma.cc/7QP7-33QF].

[4] Peter Elkind, *Inside the Hack of the Century: SONY*, FORTUNE, July 1, 2015, at 64.

[5] Michael Riley et al., *The Epic Hack, Target Ignored Its Own Alarms – and Turned Its Customers into Victims*, BUS. W., Mar. 23, 2014, at 42.

the technological revolution of the new millennium. Digital has replaced analog. The smart phone has become a critical item of our lives. Silver halide film is but a history to most of us. The microchip and personal computer is the new paradigm.

We have satlines, satellite TV, satphones and smart phones, GPS, live streaming, and video games, such as Grand Theft Auto. Say goodbye to landlines and cable, and hello to cord cutting. Artificial intelligence, robotics, and medicine are witnessing rapid advances. The Internet is now drawing commerce away from the suburban malls as consumers increasingly shop online. Today's smartphones may in many ways exceed the power of the mainframe computers of the 1960s.

Indeed, the computer is becoming seemingly ubiquitous in our normal activities with computers in the classroom, the home, the factory, the office, and the roads and highways. Computer design and computer models are widespread. Today, law students almost exclusively take class notes on laptops, rather than by hand. Hollywood special effects are increasingly computerized. Humans are becoming overly dependent on computers.[6]

We are living the computer revolution.

Revolutions trigger risk of the unknown and create unknown risks. The computer revolution has created three major risks so far in privacy, security, and bullying.

Cyberspace has its risks. Information is easier to assemble and destroy than bricks and mortar. One of the greatest threats today is the loss of privacy, which is increasingly limited. The paradox is that the more we wish to maintain our individual rights of privacy, the less privacy we have. Today's computer information age with the Internet puts privacy at risk. The information accessible through the Internet tells the world so much about us, even without looking on social media. Cell phone cameras, tablets, and video recorders are ubiquitous. Seemingly anyone can record us anywhere at any time, often without our knowledge, much less approval. The recordings can then show up

[6] Asiana Airlines Flight 214 landed short of the tarmac at San Francisco International Airport when it hit the seawall separating the airport from the bay. Three died in the July 6, 2013 accident. Blame is placed on over-reliance by the pilots on the autopilot flight system rather than manually overriding the system when it became clear that the plane was descending too rapidly. *Asiana Jet Crash: Over-Reliance on Autopilot System, Poor Pilot Training?*, BUS. KOR. (Dec. 12, 2013, 12:47 PM), http://www.businesskorea.co.kr/english/news/politics/2428-asiana-jet-crash-over-reliance-autopilot-system-poor-pilot-training [http://perma.cc/L6VP-UN8P]; *see also* Nicholas Carr, *Automation Makes Us Dumb: Human Intelligence Is Withering As Computers Do More, but There's a Solution*, WALL ST. J. (Nov. 21, 2014, 12:02 PM), http://www.wsj.com/articles/automation-makes-us-dumb-1416589342.

on social media, and perhaps go viral. Webcams can record and send, often secretly.

Public records are increasingly accessible through the Internet. News articles today are posted digitally online. Materials from decades ago are increasingly converted to PDFs and loaded onto the Internet. Our past, our being, is open to the world through downloads.

A second problem with today's computer age is cybersecurity, or, more accurately, the lack thereof. Identity theft and cyber breaches are major problems.

So much of our personal and financial information is online somewhere and, thus, vulnerable to either hackers or misuse by those with otherwise proper access to it. The improper access is reprehensible, but the subsequent "misuse" can be devastating. Personal cell phones, tablets, and computers are often at risk because of the carelessness of the owner in ignoring basic security precautions, such as password protections. These same users might also store highly personal photos on their devices, or perhaps sext to others, who in turn resend the messages or are hacked.

Cybersecurity has become a mission-critical business challenge. The challenges can come from seemingly infinite directions.

Critical information is threatened when laptops, DVDs or flash drives are lost, misplaced, or stolen. Sometimes improper attachments or links are included in emails. People are careless in hitting "reply all," in that improper addresses may be buried somewhere in the chain. Others sometimes push "send" in an ill-tempered or otherwise ill-advised moment.

Passwords, the initial barrier to entering a website, may be highly vulnerable. Some users are careless in providing their passwords to others. Users with a common password that applies to all their accounts are inviting hackers. A breach on one account opens up the rest. In addition, easy to crack passwords provide little security.

No matter how strong cybersecurity controls are at a company, weaknesses can still exist at off-site locations, such as connected customers, suppliers, providers, routers, servers, and Wi-Fi[7] connections. A chain is only as strong as its weakest link. So too with cybersecurity. Even interactive video games have risks. The weakest connection is the weak link in security.

[7] *See* Jennifer Valentino-DeVries, *Bugs in Wi-Fi Hookups Cripple Web Security*, WALL ST. J., Jan. 19, 2016, at A1, col. 2.

Damage occurs once a site is improperly accessed. If the wrongful information is published and goes viral, then it cannot be removed from the worldwide web even if the original wrongdoer is called to account.

Today's computer hosts have to be seemingly paranoid about cybersecurity. They say in Southern California that there are two types of homes—those that had termites and those that will. The same is true of cybersecurity risks; many of us have been victims of identity theft, or will be. We learn of malware, Trojan Horses, phishing, spear phishing, ransomware, spyware, viruses, and worms. Infamous viruses include Stuxnet,[8] Melissa, ILoveYou, Sasser, Zues, Mydoom, and Code Red.[9] Firewalls can be breached.

The list of those at risk includes employees, consumers, customers, students, patients, and governments. Students' academic records are accessed, credit cards compromised, financial accounts drained, personal photos released, and medical records disclosed. Emails, search histories, texts, and sexts are vulnerable. Lives are ruined, careers lost, and reputations destroyed. The economic costs to people and businesses are in the billions. All sometimes with only a few keystrokes because of inadequate or non-existent security. We hear of the vulnerability of the nation's electrical grid. Several celebrities had their cell phone photos hacked and leaked a few years ago.

Multiple goals explain the hacking attacks: to discover corporate secrets, trade secrets, and military secrets. Hackers seek to obtain personal information, perhaps to use in future blackmail or extortion efforts. The hackers can be individuals, businesses, or even governments.[10] Sovereign nations wish to gain military advantages.

[8] Israel and the United States are reported to have used the Stuxnet virus to disable roughly 20% of Iranian centrifuges. David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES (June 1, 2012), http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0 [http://perma.cc/D5R2-YVB8].

[9] "Hacking" can also be by security experts testing the cybersecurity of a site. It also sometimes seems humorous. For example, the District of Columbia Board of Elections and Ethics held a mock election to test the security of a proposed voting system. The source code was published with the public and computer science researchers provided time to attempt to hack in. A University of Michigan engineering team quickly found a vulnerability in the system and essentially hijacked the site, leaving "The Victors," the University of Michigan fight song, on the site. Scott Wolchok et al., *Attacking the D.C. Internet Voting System*, PROC. 16TH CONF. ON FIN. CRYPTOGRAPHY & DATA SECURITY (Angelos D. Keromytis ed., 2012); Mike DeBonis, *D.C. Vote-Hackers Publish Their Vote-Hacking Exploits*, WASH. POST (Mar. 6, 2012), https://www.washingtonpost.com/blogs/mike-debonis/post/dc-vote-hackers-publish-their-vote-hacking-exploits/2012/03/06/gIQArbG4uR_blog.html [http://perma.cc/4BG6-P7XL].

[10] China acknowledged that Chinese citizens hacked into the United States Office of

Sometimes the goal is to obtain incriminating or highly personal information to release to the public to embarrass the victims. Some hackers seek revenge and vengeance; revenge porn has become a major problem in recent years.

We face cyberattacks, cyber bots, cyberbullies, cyber cafes, cyber harassment, cyber incidents, cyber insurance, Cyber Mondays, cybernauts, cybernetics, cyber networks, cyberphobia, cyber power, cyber rings, cyber risk, cyber searches, cybersecurity, cyberspace, cyberstalking, cyber strategy, cybertechnology, cyberterrorism, cyberthreats, cyberwarfare, cyberweapons, and a cyber world.

Cars crash, and so, too, do computers. Today's computers run cars, not to mention boats, trains, and planes. They can also be programmed to crash cars, boats, trains, and planes.[11]

Sometimes it's as simple as a few clicks to cause substantial damage, often due to inadequate or careless security. The hacking can come from anywhere in the world, even from sovereign governments.

H.G. Wells published *The War of the Worlds* in 1898. Hollywood brought the story of the Martian invaders to the big screen in 1953 with Earth's bacteria and viruses killing the invaders. The movie Independence Day in 1996 had the invaders defeated by computer viruses, a harbinger of the future.

We are in a war between the hackers, often government-based, and security, between offense and defense. The cyberwarriors engaged in this battle of wits are often brilliant, operating on the edge of computer technology. Cybersecurity catches up to new threats, while attackers create new waves of attack. The ongoing war places personal and national security at risk. Software remains vulnerable. No human-designed system can ever be free of risk.

Victims of cyber breaches have often brought lawsuits, including class action suits, against service providers and account holders,[12] even if the victims cannot legally reach the

Personnel Management, but said it was the work of criminal activity rather than a state sponsored cyberattack. Michael Forsythe & David E. Sargent, *China Says Hacking of U.S. Workers Data Was Common Crime, Not State Action*, N.Y. TIMES, Dec. 3, 2015, at A10, col. 1.

[11] Two security researchers were able to hack into and remotely control jeeps with a flaw common to Chrysler Fiat vehicles. Nicole Perlroth, *Hackers Get Inside a Jeep, and Fiat Chrysler is Dismayed*, N.Y. TIMES, July 22, 2014, at B4, col. 1.

[12] *See, e.g.*, Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015); *In re* Target Corp. Cust. Data Sec. Breach Litig., 66 F. Supp. 3d 1154 (D. Minn. 2014); In Re SCI . Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14 (D.D.C. 2014); Galaria v. Nationwide Mut., Inc., 998 F. Supp. 2d 646 (S.D. Ohio 2014).

hacker. In addition, the Federal Trade Commission has brought action against companies with inadequate security.[13]

The *Chapman Law Review* Symposium presents distinguished experts and scholars on cybersecurity. Harvey Rishikof, Co-Chair of the ABA Cybersecurity Legal Task Force and Chair of the Advisory Committee for the ABA Standing Committee on Law and National Security, delivers the keynote address, "Framework for the Future of Cybersecurity." Panels focus on the perspectives of the government and corporate sectors and cybersecurity for the practitioner.

[13] For a discussion of the lessons from the FTC cases, see FEDERAL TRADE COMMISSION, START WITH SECURITY: A GUIDE FOR BUSINESS: LESSONS LEARNED FROM FTC CASES (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [http://perma.cc/2BHE-GD29].