2012

Cybercrime

Ronald C. Griffin
Florida A & M University College of Law, ronald.griffin@famu.edu

JICLT
Journal of International Commercial Law and Technology
Vol. 7, Issue 2 (2012)

CYBERCRIME

Ronald C. Griffin
PROFESSOR OF LAW
WASHBURN UNIVERSITY
TOPEKA, KANSAS
ronald.griffin@washburn.edu

Abstract. *This essay recounts campaigns against privacy; the fortifications erected against them; and hi-jinx attributable to hackers, crackers, and miscreants under the Fair Credit Reporting Act.*

1. Introduction

Hell is living on earth without love.

Dwellers feel empty inside.

Monotony is a curse. But……

America is changing.[1] Cyberspace blankets the continent. A new generation is at the nation's helm. Citizens are making weird accommodations with their surroundings.[2] Privacy is under siege.[3] People are anxious, fearful, and unsettled. Cyberspace makes things worst.

Like nature, in the past, cyberspace is indifferent to the antics of man. But cyberspace technology, when put in the wrong hands, is threatening and unfriendly.4 Business computers prowl the landscape to compile data about us.[5] Government software spies on people to trap law breakers.[6] This essay recounts campaigns against privacy; the fortifications erected against them; and hi-jinx attributable to hackers,[7] crackers,[8] and miscreants under the Fair Credit Reporting Act.[9]

---

[1] REICH, GREENING OF AMERICA 2-6 (1970); MARCUSE, NEGATION 33-34 (1968). Man is the original actor. He makes history. He chooses sides and acts.

[2] REICH, *supra* note 1, at 8.

[3] Chick, *Customary International Law: Creating a Body of Customary Law for Cyberspace. Part 2: Applying Custom as Law to the Internet Infrastructure*, 26 COMPUTER LAW & SECURITY REVIEW 185,193 (2010) (trolling search engine data bases (Google, Yahoo, and America Online) for academic reasons is suspect); Hafner & Richtel,*Google Resists U.S. Subpoena of Search Data*, N.Y. TIMES, Jan. 20, 2006, at A-1 (digging into ISP log files (i.e., asking providers to surrender the records for every person accessing a particular internet website) is a bit much); Electronic Frontier Foundation, *From EEF's Secret Files: Anatomy of a Bogus Subpoena*, http://www.eff.org/wp/anatomy-bogus-subpeona-indymedia (last visited Sept. 9, 2011).

[4] Aquilina, *Public Security Versus Privacy in Technology Law: A Balancing Act*, 26 COMPUTER LAW & SECURITY REVIEW 130 (2010) [hereinafter *Aquilina*].

[5]. McClung, *A Thousand Words are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 N.W.U. L.REV 63, 69 (2003) [hereinafter *McClung*]; Keck, *Cookies, the Constitution, and the Common Law: A Framework for the Right to Privacy on the Internet*, 13 ALB. L.J. SCI. & TECH. 83, 109 (2002); *see Online Profiling: Benefits and Concerns, Hearing Before the Sen. Comm. on Commerce, Science, and Transportation*, 106th Cong. (2000) (statement of Jodie Bernstein, Dir., Bureau of Consumer Protection, F.T.C.), *available at* http://www.ftc.gov/os/2000/06/onlineprofile.htm.

[6] People get shoved into the spotlight, indeed, find themselves put there by a swirl of events, politics, psychology, and emotions. What the government does under the Patriot Act is a horrifying example. American Civil Liberties Union, *Surveillance Under the USA Patriot Act*, *available at* http://www.aclu.org/National-Security/surveillance-under-usa-patriot-act; *see Aquilina*, *supra* note 4, at 133; *see also* Shipler, *Free to Search and Seize*, N.Y. TIMES, June 23, 2011, at A-21.

2. Sketch

Cyberspace is a parallel universe.[10] It is electrons, computers, routers, servers, local networks, clouds, webs, and super highways (nets) transporting information everywhere. The realm looks like an old growth forest. People dart in an out to trap information to solve problems.

Cyberspace is lawless.[11] It is indifferent to folks poaching data from others. Today's users demand privacy: patches of ground that accommodate images (self-constructed ones),[12] anonymity (things people want to keep secret),[13] solitude (peace and quiet),[14] and rights (claims against others).[15]

Rummaging through a computer is suspect.[16] Using a computer to poach data from other computers is a wrong.[17] Using webs to bully others is suspect.[18] Using them to goad somebody into taking their life is a crime.[19] Assuming somebody's identity is wicked.[20] Using a server to download proprietary information is suspect.[21] Selling the stuff to foreign governments is a crime.[22]

3. Landscape

3.1. Future Shock

Let's ease onto the landscape. In my lifetime books and television made indifference to suffering unfashionable. E-commerce made old fashioned deal-making obsolete. Machines performed tasks that took older generations time to complete.[23] Robotics changed everything.[24]

---

[7] Sinrod & Reilly, *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 177, 181 (2000).

[8] *Id.* at 182.

[9] Pintos v. Experian Info. Solutions, 605 F.3d 666 (9th Cir 2010); *see FTC Releases Survey of Identity Theft in the U.S., 27.3 Million victims in the Past 5 years, Billions in losses for Businesses and Consumers* (Sept. 3, 2003), *available at* http://www.ftc.gov/opa/2003/09/idtheft.htm.

[10] Hardy, *Law and the Internet*, 5 BUS. LAW TODAY 8 (1996).

[11] Rho, *Blackbeard of the Twentieth Century: Holding Cybercriminals Liable under the Alien Torts Statute*, 7 CHI. J. INT'L. L. 695, 713-74 (2007).

[12] Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*,11 BERKLEY TECH. L.J. 1, 78 (1996).

[13] Lester, *The Reinvention of Privacy*, ATLANTIC MONTHLY, vol. 284, no. 3, at 27, 31-32 (Mar. 2001).

[14] *See* Intel Corp. v. Hamidi, 71 P.3d 296 (Cal. 2003). Business webs create no-fly zones above their owners' space. When folk enter their realms they have a right to police a nuisance. *See* Epstein, *Intel v. Hamidi: The Role of Self- Help in Cyberspace*, 1 J. L. ECON. & POL. 147 (2005).

[15] *See* Cvent, Inc. v. Eventbright, Inc., 739 F.Supp.2d 927 (E.D.Va. 2010).

[16] Invading a reality created by a computer is a crime. 18 U.S.C. § 1030(a)(4) (2011). Looting data is wrongdoing. Paradigm v. Celeritas, 722 F.Supp. 2d 1250 (D.Kan. 2011).

[17] Lawson, *The Case of the Stolen WI-FI*, PC WORLD, Aug. 8, 2005, *available at* http://www.pcworld.com/article/122153/the-case-of-the-stolen-wifi.htlm.

[18] *See* Chaffin, *The New Playground Bullies of Cyberspace: Online Peer Sexual Harassment*, 51 HOW. L. J. 773 (2008).

[19] Breuer, *Cyber-Bullying Suicide Case Goes to Jury, available at* http://www.people.com/people/article/0,202242541,00.html [hereinafter*Breuer*].

[20] Folsom,*Defining Cyberspace (Finding Real Virtue in Place of Virtual reality)*, 9 TUL. J. TECH. & INTELL. PROP. 75, 105 (2007).

[21] Multiven v. Cisco Sys., Inc., 725 F.Supp. 2d 887 (N.D.Cal. 2010).

[22] Ngowi, *Ex-Tech Worker in Mass. Pleads Guilty in Spy Case*, BLOOMBERG BUSINESSWEEK, Aug. 30, 2011, *available at* http://www.businessweek.com/ap/financialnews/D9PEMJCG0.htm.

[23] GALBRAITH, THE NEW INDUSTRIAL STATE 293 (1967).

[24] THROW, THE ZERO SUM SOLUTION 146-147, 157 (1985).

Machines did the work of fifty men and freed-up labor to do other things. When software of all sorts was added to these machines (ordered by handlers to collate data and do other things) the machines did *other things* on their own.[25]

Then, like now, bits of code roamed untethered to anything.[26] When they collided with other bits they created intelligence---altering *machines results* and the cyberspace dweller's perceptions of his surroundings.[27]

Input errors and exaggerations made cyber space different.[28] During the sub-prime mortgage crisis authorities used unsuitable machines to account for the bad stuff swamping us. Government tools were overwhelmed by a blizzard of information. Nobody accounted for the economic activity of every sub-prime mortgage, or added-in the law of probabilities, to fix the useful life of sub-primes after bundling.[29] Something had to be done. Hackers came to our rescue.

3.2 Subprime Mortgages

These were heady days. Financial institutions trawled oceans, stocked with ordinary beings, to snare some to mortgages that fleeced them.[30] The mortgages were dumped into mortgage pools managed by agents.[31] They bundled a bunch; branded them bonds; and sold them downstream.[32] Smart investors bought the worst of the lot and good insurance to cover the risk that some would fail before maturity.[33]

Brokers and buyers traded heavily in subprime mortgages.[34] Pool agents grabbed the best mortgages for bundling.[35] Buyers took them to Moody's for upgrade and passed them on to others. Sadly, the values ascribed to ordinary bonds and sub-prime bonds were difficult to distinguish.[36] Though both carried an A-1 rating the latter was brimming with risk.

The mortgage market process was a cyclical activity.[37] Agents compiled the worst mortgages last.[38] When the worst sub-primes *blew up en masse,* chunks of the ordinary bond market blew up with them.[39] Insurance companies stepped up to cover the losses, but couldn't do so on a sustained basis.[40] Discerning a crisis, bondholders panicked and, as bond values dropped, the bond market lost its luster as a place where people could make piles of money.

---

[25] Yudkowsk, *Artificial Intelligence as a Positive and Negative Factor in Global Risk, in Global Catastrophic Risks*, Sec. 7 (Aug. 31 2006) (unpublished manuscript, on file with author).
[26] *Id.*
[27] *Id.*
[28] Benner, *Navigating Subprime Securities*, CNN MONEY, Aug. 23, 2007, *available at* http://money.cnn.com/2007/08/22/news/companies/value_subprime_securities.fortune/index.htm.
[29] Michael Malloy, Professor of Law, McGeorge School of Law (University of the Pacific, U.S.A.), Briefing at the Athens (Greece) Institute for Education and Research's 8th Annual Conference on Law (July 19, 2011) [hereinafter Malloy].
[30] *Id.*; *see* Lewis, THE BIG SHORT: INSIDE THE DOOMSDAY MACHINE 10 (2010) [hereinafter *Lewis*].
[31] Malloy, *supra* note 29.
[32] *Id.*
[33] *Lewis*, *supra* note 30, at 75.
[34] Malloy, *supra* note 29.
[35] *Id.*
[36] *Lewis*, *supra* note 30, at 74.
[37] Malloy, *supra* note 29.
[38] *Id.*
[39] *Lewis*, *supra* note 30, at 250-52. There is a longer account in the author's epilogue. See *id.* at 253-64.
[40] Doherty, *The Pebble and the Pool: The (Global) Expansion of Sub-prime Litigation* 5; *Andrews Class Action Litigation Rept.* 2, 12 (2008).

Accountants were supposed to account for the economic activity of every mortgage in the sub-prime market. They didn't do that.[41] Pool managers were supposed to file informational reports with the IRS. They were lax.[42] Somebody was supposed to file reports about the bonds with the bondholders, but no one did that.[43] Taxpayers filed incomplete tax returns. The IRS (working with unsuitable machines) could not catch mistakes. Hacking into private computers to get at the truth was difficult. Things were a mess. Hackers came to our rescue.

3.3 Trade Secrets

Then, like now, cyberspace was dazzling. It accommodated everyone: good guys, bad guys, villains, and mavericks. Some polluted the environment (gumming up servers so others could not use them.) Some overran business security systems. Giving victims notice about what they had done, they demand ransoms for promises not to do anything else.[44]

Trade secrets (corporate business aspirations, industrial plans, ways for doing things, product recipes owners did not want others to have) were everywhere.[45] Companies used non-disclosure agreements against current and former employees to discourage stealing.[46] Appropriators-succumbing to bribery, theft, and espionage-were shamed by their employer, branded social outcasts, and made felons.[47]

Sadly, human nature, *being what it is,* remained the same. Thieves planted software in computers to steal things. But, curiously enough, their fancy stuff had flaws allowing others to pilfer their stores. In 1996, the Economic Espionage Act came onto the scene.[48] Congress did something to stop the stealing. It was unlawful to pilfer information and sell it to others for profit.[49] The loot was called trade secrets. It was defined by examples. Selling the stuff to foreign governments was a crime.[50]

4. The Rubbish

The United States was a mess. There was crime, angst, anxiety, and mass unemployment.[51] This potage was attributable to the subprime mortgage crisis and the top-down policies of the nation's elite.[52] The Bush Administration tax cuts (that consumed the government's budget surplus), two unfunded wars (contributing to gross deficit spending by government), and a runaway financial sector (empowered by reckless deregulation) did awful things to us.[53]

People were nostalgic. They pined for the certainty and security of the past. Some turned on acquaintances (treating them like prey) to get a foothold in life. In this climate, hurting somebody---by stealing information

---

[41] Joseph McKinney, Professor of Law (Decedents Estates and Tax), College of Law, Washburn University (Topeka, Kansas, U.S.A.), Interview with author, June 25, 2011.

[42] *Id.*

[43] *Id.*

[44] Brenner & Schwerha, *Cyber Havens*, 17 BUS. L. TODAY 49 (2007) [hereinafter *Brenner*].

[45] Rustad, *The Negligent Enablement of Trade Secret Misappropriations*, 22 SANTA CLARA COMPUTER & HIGH TECH. L. J. 455, 508-10 (2010) [hereinafter *Rustad*]; *see* Lewis, *The Economic Espionage Act and the Threat of Chinese Espionage in the United States*, 8 CHI-KENT J. INTELL. PROP. 189, 201 (2009) [hereinafter *Espionage*].

[46] Garfield, *Promises of Silence: Contract Law and Freedom of Speech*, 83 CORNELL L. REV. 261 301-04 (1998).

[47] *Two Men Plead Guilty to Stealing Trade Secrets from Silicon Valley Cos. To Benefit China*, U.S. Dep't of Justice, Dec. 14, 2006, *available at* http://www.justice.gov/criminal/cybercrime/yePlea.htm.

[48] *Rustad, supra* note 45, at 464-68.

[49] U.S. v. Kai-Lo Hsu, 155 F.3d 189, 195-96 (3d Cir. 1998).

[50] *Id.*

[51] Krugman, *The Unwisdome of Elites*, N.Y. TIMES, May 8, 2011, at A-23.

[52] *Id.*

[53] *Id.*

from their computers---was swashbuckling, heroic, romantic, un-policed and profitable. Authorities used laws to stop them.

4.1. Harm

Computers are like books. When employers proscribe employee use, opening one is a crime. Opening computers to read or alter privileged information is a violation of the Computer Fraud and Abuse Act (CFAA).[54] Opening one to share proprietary information is suspect. Giving the data to rivals is a crime.[55]

1. Gast Case

Jeffery Gast was a Shamrock Foods Company employee. He signed a confidentiality agreement promising not to disclose trade secrets.[56] Gast was a good employee. He was offered and accepted a promotion with his employer because of his hard work. On January 4, 2008, he sent his employer's confidential and proprietary information to his computer. A day later he told Shamrock about a rival food company's offer of employment.[57] He told Shamrock that he was going to work for them.[58] On January 14, 2008, he submitted his resignation. A short time later Shamrock conducted a forensic audit and discovered an email Gast sent to himself.[59]

Untethered proprietary information (susceptible to capture by rivals) was (in Shamrock's mind) a threat to the firm. Shamrock brought an action against Gast to recover damages for the cost of the forensic audit under the CFAA.[60] The question was: whether Gast's deed clashed with the statute. After a careful consideration of the pertinent cases, the court said no. Because Gast was a full-time employee and authorized to use company computers, using one to send data to himself was allowable under the law.[61]

Though Shamrock's lawsuit made the firm feel good; cast a pall over the food business for a while; chilled a rival's impulse to use their stuff; it left the plaintiff without tools to reign-in untethered data.

2. Drew Case

On May 15, 2008, a grand jury indicted Lori Drew for violations of the CFAA.[62] She used a made-up boy's name (Joshua Evans) to establish a phony MySpace account.[63] She used the account to befriend a thirteen year old girl and, at Evan's behest, goaded her into committing suicide.[64] The U.S. Attorney prosecuted Drew and a jury convicted her of a crime, but the court set aside the conviction.[65]

The court found that criminalizing the use of a web site gave the CFAA too broad a reach, that the verdict invested the police with too much power, and that the verdict gave too little notice to citizens using the internet.[66]

---

[54] Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1998).
[55] Multiven, 725 F. Supp. 2d at 889.
[56] Shamrock Food Co. v. Gast, 535 F.Supp. 2d 962, 963 (D. Ariz. 2008).
[57] *Id.*
[58] *Id.*
[59] *Id.*
[60] *Id.*
[61] *Id.* at 968.
[62] Chunga, *The Computer Fraud and Abuse Act: How computer Science Can Help with the Problem of Over Breath*, 24 HARV. J.L. & TECH. 233 (2010).
[63] *Id.*
[64] *Id.*
[65] *Id.*
[66] U.S. v. Drew, 259 F.R.D. 464, 467 (C.D. Cal. 2009).

But, having said that, there is something eerie, unsettling, and distasteful about the outcome. If laws facilitate healthy interactions between human beings, laws and their interpretations that facilitate unhealthy interactions are wrong.[67]

3. Sloan Case

Suzanne Sloan was a patient in a Virginia hospital.[68] Slovanna Sloan was a hospital employee.[69] Because of their name similarities and identical birthdates, Slovanna stole Suzanne's identity to make money. Slovanna spent the loot (Suzanne's identity) on loans, new credit cards, cash advances, and services totaling $30,000.[70] Suzanne discovered the theft in January 2004. She notified the police, Equifax, and other consumer credit reporting agencies.[71] She called her creditors; completed notarized forms about these acts; and sent them to everybody to correct her credit history.[72]

Equifax assured Suzanne that it would do everything to correct her credit history.[73] But that promise was never kept. When Suzanne applied for credit, she was rebuffed by creditors and banks.[74] More than thirteen months after reporting the theft, Suzanne battled Equifax.[75]

There were twenty four erroneous accounts in her credit report.[76] Equifax removed twenty two of them.[77] Two months later Suzanne wrote a letter contesting the outstanding accounts. From that skirmish she unearthed the fact that Equifax (for whatever reason) had restored the twenty two deleted accounts.[78]

After a twenty months effort to correct her credit report Suzanne filed a Fair Credit Reporting Act complaint against Equifax.[79] The case went to trial. The jury returned a verdict for Suzanne, ordering Equifax to pay $106,000 in damages for economic loss and $245,000 for mental anguish, humiliation, and emotional distress.[80]

4. . Russian Case

In the year 2000, Russian hackers took apart American businesses. They stole trade secrets from company computers and threatened to make public the cache. They made no effort to conceal their identity. Because there was no cybercrime-related extradition treaty between the Russian Confederation and the United States, they did what they wished with impunity.[81]

The government lured the hackers to the United States. They were invited to a bogus interview with a fake computer company in Seattle, Washington. Once there, they demonstrated their hacking skills on laptops rigged with FBI software.[82] The gadgets captured the hackers' user names, passwords to the Russian server, and tools of their trade. With this evidence in hand, the FBI arrested the Russians; indicted, tried, and convicted one of them under the Economic Espionage Act.[83]

---

[67] *Murphy, Lon Fuller and The Moral Value of the Rule of Law*, 24 LAW & PHILOSOPHY 239, 242 (2005).
[68] Sloan v. Equifax Info. Svcs. Inc., 510 F.3d 495, 498 (4th Cir. 2007).
[69] *Id.*
[70] *Id.*
[71] *Id.*
[72] *Id.*
[73] *Id.*
[74] *Id.*
[75] *Id.*
[76] *Id.*
[77] *Id.*
[78] *Id.*
[79] *Id.*
[80] *Id.*
[81] *Brenner*, *supra* note 44.
[82] *Id.*
[83] *Id.*

At trial, the defense counsel moved to suppress the evidence on Fourth Amendment grounds. The Supreme Court found that the Fourth Amendment did not extend to searches and seizures outside of the United States.[84] The Fourth Amendment protected citizens and resident aliens. Because non-citizens were beyond the scope of the 4th Amendment,[85] the evidence could be used by the government to put them away.

One hacker was acquitted of all charges and returned to Russia. The other hacker was convicted, served three years, and went home.[86] Thereafter, the Russian Federal Security Service brought charges against the FBI case agent, working the Russian case, for mucking around in foreign computers. Although the American was never turned over to Russian authorities for prosecution, and no trial *in absentia* ever took place, Russian officials felt the charges were necessary to assert their sovereignty.[87]

5. Fe Ye Case

On November 23, 2001, federal authorities arrested Fe Ye and Ming Zong at the San Francisco International Airport. Fe Ye is a U.S. citizen and Ming Zong is a permanent resident.[88] Both had tickets for a flight to the People's Republic of China and had corporate trade secrets in their possession.[89] The U.S. government knew they were going to give the trade secrets to a government-funded Chinese corporation.[90] Charges were brought against them under the Economic Espionage Act. Ye and Zong plead guilty to the charge of economic espionage.[91]

6. The Gang Case

On August 4, 2011, New York authorities indicted six members of a of an identity theft and cybercrime gang for stealing one million dollars from 80 clients of J.P. Morgan Chase Bank. The indicted were accused of harvesting information about people from the bank's data base and, when the occasion allowed, assuming the identity of some Chase clients to pick their pockets. Some gang members used their positions at the bank to gather information from the bank's system to withdraw funds from the accounts of unwitting patrons The accused were charged with computer trespass, conspiracy, larceny, and identity theft. If convicted, they face five years of imprisonment.[92]

7. Koch Case

Koch Industries assembled a website to spread controversial messages about global warming and climate change. Its foes ("John Does") plumbed public records to assemble a phony website for Koch, in order to put Koch Industries in a false light.[93] Koch spent time and money fixing its messages. Thereafter, it brought an action to recover damages under the CFAA.[94]

---

[84] *Id.*
[85] *Id.* But, having said that, aliens can deploy the Fourth Amendment against outrageous government conduct (e.g., kidnapping) outside of the United States. U.S. v. Toscanino, 500 F.2d 267, 280 (2d Cir. 1974).
[86] *Id.*
[87] *Id.*
[88] *Lewis*, *supra* note 30, at 207. There is an opinion. *See* U.S. v. Fei Ye, 436 F.3d 1117 (9th Cir. 2006).
[89] *Id.*
[90] *Id.*
[91] *Id.*
[92] Debusmann, *NYPD Busts Gang of Identity Thieves: Cyber-Criminals: DA's Office*, http://www.reuters.com/assets/print?aid=USTRE7737DJ20110804.
[93] Koch Indus., Inc. v. John Does, 2011 WL 177565 at *1 (D. Utah).
[94] *Id.* at *2.

The court dismissed Koch's action.[95] Reconstituting public information to manufacture fake websites is suspect. When the setup addles the public (i.e., puts established-businesses in a false light), the deeds violate the CFAA.[96] Owners must post password protection sentinels around their websites , use bold words to ward-off miscreants, and patter to the public about a website user assenting to terms and usage language.[97] The court held that Koch could not recover damages, in this case, because it did nothing along these lines.[98]

8. Multiven Case

Cisco Systems, Inc. manufactures network switches, routers, and related services.[99] Then, like now, Cisco Technology was a wholly-owned subsidiary of Cisco Systems, Inc. As late as May, 2005, Peter Alfred Adekeye worked as an employee with Cisco Technology. On March 2, 2005, Adekeye founded a Delaware corporation.[100] Its name was Multiven, Inc.[101] Multiven furnished services and maintenance support for routers and network systems, including products manufactured and placed into the stream of commerce by Cisco, Inc.[102]

Adekeye terminated his employment with Cisco.[103] Afterwards, Adekeye convinced a Cisco employee to share his employee user name and password so Adekeye could plumb Cisco data for his business.[104] When Cisco discovered the intrusion it brought an action to recover damages under the CFAA.[105] Cisco sought money to cover the cost of staunching the flow of privileged information.[106]

The court's opinion was piled high with judicial hints. Poking into somebody's computer is vile. Tricking a server is suspect. Poaching information crosses the line. When victims spend their money staunching the flow of information, the culprit must reimburse them. Cisco got damages.[107]

9. Kai-Lo Hsu Case

This was a disclosure case under the Economic Espionage Act (EEA).108 The question was whether the government was obliged to divulge trade secrets under the guise of providing the defense with real evidence against their clients.109 The court said no.

A federal grand jury indicted Kai-lo Hsu, Chester Ho, and Jessica Chou under the EEA.[110] The indictment alleged that the defendants sought processes, methods, and formulas for the manufacture of Taxol, an anti-cancer drug manufactured and marketed by Bristol Myers Squibb.[111] Hsu met with Hartmann, an undercover FBI agent, in Los Angeles, California.[112] He outlined his Taiwanese firm's interest.[113] When Hartmann told Hsu that Bristol Myer would not share information about Taxol, Hsu told Hartmann that "we'll get it another way."[114]

---

[95] *Id* at *6-7.
[96] *Id.* at *6
[97] *Id.*
[98] *Id.*
[99] Multiven, 725 F. Supp. 2d at 889.
[100] *Id.*
[101] *Id.*
[102] *Id.*
[103] *Id.* at 892.
[104] *Id.*
[105] *Id.* at 894-95.
[106] *Id.* at 895.
[107] *Id.*
[108] U.S. v. Kai-Lo Hsu, 155 F.3d 189 (3d Cir. 1998) [hereinafter Kai-Lo Hsu].
[109] *Id.* at 191.
[110] *Id.* at 197.
[111] *Id.* at 191.
[112] *Id.*
[113] *Id.* at 192.
[114] *Id.*

The conspirators plied Hartmann to get the information. After some time had passed Hartmann arranged a bogus meeting to transfer something.

When the meeting with Hartmann ended at a Los Angeles hotel, the FBI arrested the conspirators. Defense counsel demanded disclosure of the so-called trade secret, passed on to his clients, to authenticate (in his mind) what they were caught holding.[115] If the data was bogus, counsel said, he was going to use legal impossibility as a defense.[116]

Because Congress denied defense counsel the option to use legal impossibility to mount a defense, the government was precluded from disclosing trade secrets under the guise of affording defendants evidence against them.[117]

EEA's legislative history was clear with regard to attempt and conspiracy cases.[118] Other defenses like entrapment and outrageous conduct wouldn't suffice to wrench information from the government.[119] Under section 1832(a)(4)-(5), government need not prove trade secrets to get convictions.[120] Under section 1835, federal courts retain the power to protect trade secrets throughout when defense counsel sought them under other guises.[121]

10. Aleynikov Case

At the time, Sergey Aleynikov was a software innovator, systems engineer, and an employee of Goldman Financial Services ("Goldman").[122] Goldman purchased and tweaked a system, using information and algorithms, to execute internet trades in the stock market.[123] Goldman hid its scheme and posted sentinels to preclude public scrutiny. Aleynikov was acquainted with the system and knew how it worked.[124] During Aleynikov's employment he downloaded the system's codes, beamed them to himself in Germany, and hid what he'd done from Goldman.[125] Sometime thereafter, Aleynikov met Teza, a trading firm and a soon-to-be employer.[126] Aleynikov brought his laptop and a flash drive containing Goldman's codes to share his loot with Teza.[127] Because the acts were wrongdoing, and Aleynikov got caught doing them, he was arrested and indicted by authorities for crimes under the National Stolen Properties Act ("NSPA"), the EEA, and the CFAA.[128]

Aleynikov moved to dismiss the indictment. The counts, counsel said, weren't accompanied by plain, concise, and definite statements of essential facts for each charge.[129] Indictments, he claimed, put people on notice about suspected crimes. They parrot statutory language and, hopefully, carry sufficient facts to make it likely (in the court's mind) that a crime was committed.[130] Courts must dismiss indictments when the accused's

---

[115] *Id.*
[116] *Id.*
[117] *Id.* at 197,199.
[118] *Id.* at 199, 200.
[119] *Id.*
[120] *Id.* at 204.
[121] *Id.* at 197. 202.
[122] U.S. v. Aleynikov, 737 F. Supp. 2d 173, 174 (S.D.N.Y. 2010).
[123] *Id.* at 175.
[124] *Id.*
[125] *Id.*
[126] *Id.*
[127] *Id.*
[128] *Id.*
[129] *Id.* at 176.
[130] *Id.*

deeds are neither covered nor endorsed by some statute.[131] Aleynikov maintained that this was his case. His deeds weren't crimes and the indictment against him should be dismissed.

Generally speaking, courts should follow the rules of statutory construction and, thereafter, parse a statute, to resolve a problem like this. When Congress omits a definition for a contested term ordinary meaning should be ascribed to statutory language.[132] Courts should ignore legislative history when the word or words in question are clear, plain, and unambiguous.[133] The question was whether Goldman's codes were "goods" under the NSPA? The court said yes.

Under the statute, when goods (an undefined term in the act) was given its ordinary meaning (anything subject to commerce),[134] Goldman's codes were goods. If they were lifted from Goldman's place of business and transported by Aleynikov across state lines, the deeds ascribed to the accused constitute crimes[135].

There were tougher questions under a different statute that the court had to address. Was Goldman's source-code a product under the EEA?[136] Was Aleynikov's delivery of the code to Teza a crime under the EEA?[137] The court said yes . If Goldman's source-code made its trading system go, then the source-code was a product.[138] EEA defined them by example (e.g., products, codes, programs, squirreled away from public scrutiny, and surrounded by sentinels).[139] Since that is what we had under these facts, and evidence that Aleynikov delivered them to Teza, the accused's deeds were crimes.

But holding Aleynikov accountable under the CFAA was tricky business. The statute criminalized electronic trespassing.[140] Since misuse of looted info was beyond the scope of the act,[141] the court dismissed the CFAA count.

11. Paradigm Alliance Case

Paradigm and Celeritas were parties to a joint venture.[142] Each placed their business interests in the other's hands on an understanding that they would nurture their relationship. One day, long after their relationship was underway, a Celebritas' employee hacked Paradigm's computer.[143] He looted information from the machine and poured the booty into a patent application for new type of software.[144] Celebritas was aware of the hack but said nothing.[145] After the joint venture ended, Celebritas' employee sold the patent application to Celebritas to develop, own, and market for his clients.[146] When Paradigm got wind of the deeds, it brought an action to

[131] *Id.* at 176-77.
[132] *Id.* at 177.
[133] *Id.*
[134] *Id.* at 186.
[135] *Id.* at 187, 190.
[136] *Id.* at 178.
[137] *Id.*
[138] *Id.*
[139] *Id.*
[140] *Id.* at 192.
[141] *Id.*; LVRC Holdings v. Brekka, 581 F.3d 1127, 1130-31 (9th Cir. 2009); Univ. Sports Pub. Co. v Playmakers Media Co., 725 F. Supp. 2d 378, 382-84 (S.D.N.Y. 2010).
[142] Paradigm v. Celeritas, 722 F.Supp. 2d 1250, 1262-64 (D.Kan. 2011).
[143] *Id.* at 1265.
[144] *Id.* at 1267.
[145] *Id.*
[146] *Id.* at 1265.

recover damages.[147] The theories for the case were breach of contract, breach of a fiduciary relationship, misappropriation of trade secrets, and a CFAA violation.[148]

Under joint ventures parties must nurture their relationship. Regrettably, that did not happen in this case. Hacking was a breach of contract.[149] Looting an instrument and concealing the theft was a breach.[150] Knowing about a theft and saying nothing was breach of a fiduciary duty.[151] Pouring looted material into a patent application that got assigned to the defendant was a breach.[152] Rummaging through Paradigm's computer was a violation of the CFAA.[153]

12. Combs Case

Kelli Combs owned five internet websites.[154] James Diaz stole them.[155] He hacked her email account; inserted his password; obliterated Comb's access to the sites; and made them his own so he could milk them without obstruction for money.[156] In a lawsuit Comb's claimed that there was a conversion of her websites and multiple violations of the CFAA.[157] She deployed the Electronic Communications Privacy Act and the California Penal Code against the defendant to get relief.[158]

In California, Combs went about establishing Diaz's identity.[159] He was served with process by publication. When he failed to make a court appearance, the court entered a default judgment.[160] The district court judge said that all factual allegations were taken as true.[161] In California, internet domain names amounted to property and served as a basis for a conversion claim in torts.[162] Plaintiff had to show (as Combs did in this case) ownership, or a right to control, wrongful disposition, and damages. Since the allegations (taken as truths) established that, there was conversion.[163]

The measure of damages, chimed the court, was the value of the property at the time of conversion and the amount spent to rescue it from Diaz.[164] The court gave Combs a sum equal to the money spent to redesign her websites, publish corrective advertisements, purchase and register her new websites, and profits.[165]

4.2 Troubling Stuff

What's troubling about the rubbish is the legalese courts must use to resolve problems.[166] Judges must: (1) analyze cases; (2) use pertinent words in statutes; (3) give them their ordinary meaning; (4) give into the plain

---

[147] *Id.* at 1257.
[148] *Id.*
[149] *Id.* at 1268. Where there is both a confidential and non-competition agreement, the parties ought to, indeed, must nourish the relationship. Where one uses the other's confidential information to feather his nest there is a breach.
[150] *Id.* at 1267.
[151] *Id.* at 1265-66.
[152] *Id.* at 1268.
[153] *Id.* at 1269.
[154] Combs v. Diaz, 2011 W.L. 738052, at *1 (N.D. Cal.).
[155] *Id.*
[156] *Id.*
[157] *Id.*
[158] *Id.*
[159] *Id.*
[160] *Id.*
[161] *Id.* at *2.
[162] *Id.*
[163] *Id.*
[164] *Id.*
[165] *Id.*

meaning rule to rationalize what's being done; (5) utilize legislative history; (6) read and synthesize house and senate reports; (7) adopt the reasons for certain expressions highlighted in legislative history; (8) implement legislative aspirations; (9) make use of *pari materia* to determine when two statutes on the same subject are compatible; and (10) adopt presidential missives about cybercrime legislation to cypher the meaning of a particular act.[167]

The CFAA arms the government with the power to prosecute computer crimes. It covers stealing, vandalizing computers, and wrenching control of high technology to disrupt everybody's life.[168] The statutory language is awful:

1. To successfully bring an action under section 1030(a)(4), plaintiffs must show that defendants: accessed a "protected computer" without authorization, or exceeded an authorization that was granted, knowingly, with the intent to defraud, to make money, causing a loss over one year of $5,000.[169]

2. To successfully bring an action under 1030(a)(5), plaintiffs must show that defendants: accessed a "protected computer" without authority, intentionally and "as a result of such conduct caused damage."[170]

What constitutes a "protected computer" under the CFAA? Protected computers are tools suitable for internet use.[171] What does "without authorization" mean? "Without authorization" occurs when a person rummages through computers without permission (or after permission is rescinded).[172] What's the meaning of the words "knowledge and intent"? It's wrongdoing.[173] What is the meaning of "damages" and "loss"? It's vandalizing data, systems, programs, and information.[174] Loss is the cost of repair.[175]

EEA language is no better. Judges and clerks battle awkward language to pound-out results in economic espionage cases. "Trade secrets" are defined by examples (all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing.)[176] The material must have intrinsic value, squirreled away from scrutiny, and surrounded by sentinels.[177] The government's obligation is to do whatever to preserve a business's trade secrets.[178]

---

[166] There are competing visions about the operation of the CFAA. One presupposes an obligation to nourish employment relationships and treats an employee's nefarious acts, within realities created by computers, as crimes. Int'l Airport Cntrs v. Citrin, 220 F.3d 418 (7th Cir. 2008). The other presupposes invasions of a reality created by computers and somebody poaching information from patches in that reality, that one's not authorized to read, as a crime. U.S. v. Nosal, 642 F.3d 781 (9th Cir. 2011). The latter is a strict reading of the statute. *Id.* at 687-88.
[167] See Perez v. Rent-A-Center, 892 A.2d 1255 (N.J. 2005).
[168] Multiven, 725 F. Supp. 2d at 891.
[169] 18 U.S.C. § 1030(a)(4); *see id.*
[170] Multiven, 725 F. Supp. 2d at 891.
[171] *Id.*
[172] *Id.* at 892.
[173] *Id.*
[174] *Id.* at 894-95.
[175] *Id.* at 895.
[176] *Kai-Lo Hsu*, *supra* note 108, at 196.
[177] *Id.*
[178] *Id.* at 197.

4.3. Solutions.

a) How should we police this mess? What are the solutions? We could say: *Cyberspace is an ocean. Hackers are pirates.*[179] Since they are enemies of all mankind and difficult to capture, any country holding one has the authority to try them.[180] A private cause of action against a hacker must be beyond conjecture. The deed or deeds must be universally wrong. Exhaustion of domestic criminal remedies against the hacker, or inaction by the executive branch, are ways to start the ball rolling.

b) We should use statutes against hackers.[181] The CFAA covers breaking and entering by computer.[182] It's using this instrument beyond the scope of one's authority to collect national security information,[183] information in financial records, or information of a department or agency of the United States.[184] Any unauthorized entry is crimes.[185] Compromising an employer-employee relationship to collect somebody's trade secrets is a crime. Using somebody else's computers to trick a server into divulging information without authorization is a crime.[186]

c) We could put robotic cops on the business scene: computer software *bearing the names* of employees using a firm's computer system to access the internet. While all employees would share in the use of the business system, the software would guarantee that the files stored in a computer belonged to the user. There would be *access control lists* for everybody. The software would code files downloaded from the internet for people to read, edit, and pass on to others. The scheme presupposes that downloaders will read and brand their files at the end of a session or the software will brand it for them to restrain use.[187]

5. Commodification

For the moment, information is free and everybody possesses some. Collectors in cyberspace (e.g., newspapers) should brand their storage and price the stuff for consumption. Seekers would buy bits at nodes to regulate the flow. Downloaders would need to mark their harvests for reading, use, edit, or transfer to others. Because cyberspace is lawless, some (if not all of cyberspace) would be ceded to software engineers and counter-engineers (beat cops), to police against theft and hawked encryptions (Illustration A) that benefit everybody.[188]

---

[179] Raval, *Hacking:Cyber Pirates*, INDIA TODAY, Apr. 12, 1999, at 58, *available at* 1999 WLNR 567838 (Westlaw).
[180] *Brenner*, *supra* note 44.
[181] Bakewell, Koldaro, & Tjia, *Computer Crimes*, 38 AMER. CRIM. L. REV. 481, 486-511 (2001).
[182] *Chunga*, *supra* note 62, at 235-37; *see* Decker, *Cybercrime 2.0: An Argument to Update the United states Criminal Code to Reflect the Changing Nature of Cyber Crime*, 81 S.C.L. REV. 959, 979-84 (2008) [hereinafter *Decker*].
[183] *Chunga*, *supra* note 62, at 236.
[184] *Id.* at 236-37.
[185] *Decker*, *supra* note 157, at 984.
[186] Multiven, 725 F. Supp. 2d at 889.
[187] *Chunga*, *supra* note 62, at 247-50.
[188] Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, 8 TELCOMM. & HIGH TECH. L. 359, 392-400 (2010).

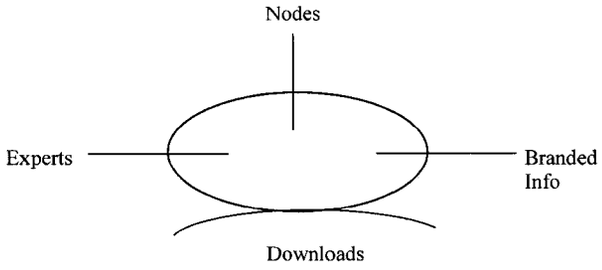

Illustration A

There is this glob with nodes around the rim. People use the nodes to harvest information from the far corners of the world . There are software creators and systems engineers (experts) to police the traffic. Branded info is news harvested by online newspapers. Consumers spend money to read the caches.

6. Crime

What should we do about crime? Phishing (e.g., phone scams),[189] fishing,[190] and auction fraud constitute crimes.[191] Using computers and GPS systems to locate password-free servers is suspect. Selling the collections to others should be a crime.

Using computers to poach information from other computers is suspect. Poaching classified information is a crime.[192] Using thumb drives to download business secrets is suspect. Spiriting the loot out of the country is a crime.[193] Using personal information to assume another's identity is suspect. Using another's identity to get loans and credit cards is a crime.[194]

Using a phony identity to establish accounts with Facebook is suspect. Using it to bring about the death of another is a crime[195] (Illustration B). Borrowing a user's name and password is wrong. Using them to poach confidential information is suspect. Using the loot to feather one's nest is a crime.[196]

[189] *Decker*, *supra* note 157, at 974-76.
[190] Fishing is jargon for data mining. *McClung*, *supra* note 5, at 69-70.
[191] *Decker*, *supra* note 157, at 971-72.
[192] *Id.* at 983
[193] *Id.* at 984.
[194] Sloan v. Equifax Info. Svcs. Inc., 510 F.3d 495, 498 (4th Cir. 2007).
[195] Steinhauser, *Missouri Woman Accused of Driving Girl to Suicide is Indicted in California*, N.Y. TIMES, May 16, 2008, at A-15. Cf. Ryan Patrick Murray, Comment, *MySpace-ing is Not a Crime: Why Breaching Terms of a Service Agreement Should not Implicate the Computer Fraud and Abuse Act*, 29 LOY. L. A. ENT. L. REV. 475, 475-77 (2009).
[196] Multiven, 725 F. Supp. 2d at 889.

JICLT
Journal of International Commercial Law and Technology
Vol. 7, Issue 2 (2012)

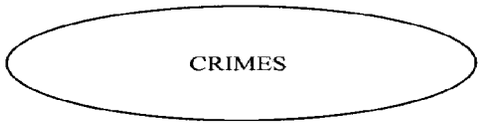

Illustration B

> We should outlaw back-dooring (bits of program code written into an application that grants the programmer access to a program without going through normal security controls); brute force attacks (capturing encrypted messages and, thereafter, imposing interrogation software on the messages to break their codes); sniffing (illicitly inserting software somewhere in a network to capture user passwords as they pass through the system); and spoofing (posing as the user to rummage through her computer).[197]

7. Damages

Hackers do untold damage. Truth is the first casualty. Nobody believes that users of cyber space can transfer stuff to others without compromising security and confidential information.[198] The debris left behind by today's thieves is everywhere. MCI lost $50 million when hackers downloaded more than 50,000 credit cards.[199] Citibank lost $10 million when its computer network was compromised by a crime group in Russia.[200] Of 1,290 businesses surveyed by Ernst and Young, nearly half were victims of information security breaches.[201] Seventy percent of respondents reported serious hacking attacks.[202]

8. Appeasement

We can appease hackers by decriminalizing hacking.[203] Business and security firms can sponsor hacker conventions, launch contests, and reward contestants for stratagems that penetrate, manipulate, and render understandable complicated business networks and security systems.[204] The sponsors would have to announce hack-in-days, exposing networks or dummy networks to hacking.[205] There would be guidelines for the contests and government oversight. Felons, people under federal indictment, and folks with seedy reputations would be excluded from these contests.[206] Contestants would receive cash awards based upon milestones and

---

[197] Lawack-David, *The Legal and Regulatory Framework of Mobile Banking and Mobile Payment in South Africa*, *in* LAW ACROSS NATIONS: GOVERNANCE, POLICY, AND STATUTES 320, 329 (S. Kierkegaard ed., Int'l Ass'n of IT Lawyers 2011).
[198] *McClung*, *supra* note 5, at 63-69. Since 2005, roughly 341 million records bearing personal information have been disclosed in the U.S. without proper authorization. Privacy Rights Clearinghouse, *A Chronology of Data Breaches* (Dec. 18, 2009), *available at* http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP.
[199] Hofmeister, *Calling Card Fraud Goes High Tech*, N.Y. TIMES, Oct. 5, 1994, at D2.
[200] Johnston, *Russians Accused of Citibank Computer Fraud*, N.Y. TIMES, Aug. 18,1995, at 6.
[201] Lewis, *Breaches on the Rise, a Study Finds*, N.Y. TIMES, Nov. 20, 1995, at 2.
[202] *Id.*
[203] Lewis, *Prevention of Computer Crimes Amidst International Anarchy*, 41 AMER. CRIM. L. REV. 1353, 1368-71 (2004) [hereinafter *Prevention of Computer Crimes*].
[204] *Id.* at 1369, *see also* Wible, *A Site Where Hackers Are Welcome: Using Hack-in Contests to Shape Preferences and Deter Computer Crime*, 112 YALE L. J. 1577, 1591-92 (2003) [hereinafter *Wible*].
[205] *Id.* at 1596; *Prevention of Computer Crimes*, *supra* note 177, at 1369.
[206] *Wible*, *supra* note 178, at 1609. Hacking inside a contest is alright. Hacking outside of a contest is wrong. Using acquired knowledge to feather one's nest is punishable. Hacking computers contestants use in hack-in ontest is a crime. *Id.* at 1599.

achievements in each contest.[207] Sponsors would harvest knowledge provided by the contestants to patch their networks and make them better.[208]

9. Benefit

All this would leave our criminal laws intact; disaggregate the hacker community; and last but not least, de-stigmatize hackers operating without a malicious intent.[209] So-called look-and-see hacking and other forms of hacking, motivated by bragging rights, would get channeled into contests (dissipating the need for and the use of law enforcement resources.)[210] Contests would provide a forum for hackers to pursue their curiosity, think creatively, and make technological discoveries that benefit everybody.[211]

10. Market Scheme

The Federal Communications Commission could erect hacking standards (using approved firewall protection schemes for the private sector) and caps. The schemes would be subject to written comments under the Federal Administrative Procedure Act before they took effect and got imposed upon internet service providers (ISPs).

Providers would have to pledge to do whatever, using all available technology, to keep hacking below the caps. At the end of a year, assuming ISP hacking protection software was within standard, and malicious hacking attempts remain below the caps, the differences would get banked by the ISP or sold to others who broke their vows.

The difference between usage and cap would be currency. Owners could buy from others to make up deficiencies, or sell their excess to others. When the differences turned scarce and, thinking fortuitously, too expensive for ISPs to purchase from others, vow breakers would have to pay fines to the government (amounting to a percentage of the cost of repair.)

This scheme is likened to a third party beneficiary contract. Because ISPs and the FCC are invested in one another's success, and have the wherewithal to do something profound about hacking, everybody (to include the public) benefits.

11. Another View

People want privacy—the right to be left alone.[212] They want sentinels in torts, property, contracts, trusts and constitutional law to keep intruders away.[213] People can't publish private letters because somebody owns them.[214] People can't publish a distinguished Prof's lectures because *she* owns them.[215] Artists can use common

---

[207] *Id.* at 1603.
[208] *Id.* at 1592.
[209] *Id.* at 1611.
[210] *Id.* at 1612.
[211] *Id.*
[212] People have "a right to be left alone." The phrase is jargon for personhood (mind and body), physical spaces occupied by people, their relationships, the shadows these concepts cast, and objects caught in the shadows that a person controls and believes others will leave alone. *Mell*, *supra* note 12, at 28. Mining, compiling, and synthesizing internet data about somebody is suspect. Selling the result to third parties without the compiled party's consent is wrong. *Id.* at 9-10; *see* Katz v. U.S., 389 U.S. 347, 350-51 (1967); State v. Kabayama, 236 A.2d 164, 165 (N.J. Super. 1967); State v, Mallan, 950 P.2d 178, 227 (Hi. 1998).
[213] *Mell*, *supra* note 12, at 26.
[214] *Id.* at 28.
[215] *Id.*

law copyright to prevent others from publishing their works.[216] People have the power to restrict use of their names and images for money.[217] They can exclude folk from their dwellings,[218] deny the government the option to rummage through their household belongings,[219] and last, but not least, deny officials the option to conduct electronic surveillance of their home without probable cause.[220]

But these sentinels are ill-suited for cyberspace.[221] This realm is different.[222] People want to protect their identity, solitude and anonymity. Some want mild forms of libertarianism to minimize government interaction with the internet.[223] Others want authorities to draw statutory lines beyond which internet users cannot go.[224]

If emailers make a representation that "they'll do x" and it's accompanied by evidence that "they intend to do y," that is fraud in fact.[225] If they type a lie (e.g., "I am x and authorized to do something beneficial for you"), that is fraud in inducement.[226] These deeds sound in tort and contracts. *They are crimes*. When tricksters use another's user id and password to circumvent software barricading websites, the deeds merit punishment.[227]

12. Parting Thought

In 2011, computers are things. They accommodate user ids, passwords, recognition devices, and software. All software comes with a license.[228] Misuse amounts to a breach. Software licensors can shut down licensees,[229] put them on a black list and, in appropriate cases, pursue a private cause of action for damages.[230]

Hackers commit crimes when they send friendly emails with attachments and websites bearing malware (software that steals information from other computers).231 People commit crimes when they insert malware

---

[216] *Id.*
[217] *McClung*, *supra* note 5, at 69.
[218] *Mell*, *supra* note 12, at 34; *see* Agnello v. U.S., 269 U.S. 46 (1925) (home); Chapman v. U.S., 365 U.S. 610 (1961) (rental property); Minn. v. Olsen, 495 U.S. 91 (1990) (temporary dwelling); Oliver v. U.S., 466 U.S. 170 (1984) (curtilage).
[219] *Mell*, *supra* note 12, at 34;. *see* Boyd v. U.S., 116 U.S. 616 (1886).
[220] Kyllo v. U.S., 533 U.S. 27 (2001). Surveillance occurs when the government uses a sense-enhancing device not in general use, to probe a home in detail. It is a Fourth Amendment search and presumptively unreasonable without a warrant. *See* U.S. v. Warshak, 631 F.3d 266, 287-88 (6th Cir. 2011) (privacy captures emails, its contents, and email customers).
[221] *Wible*, *supra* note 178, at 1577-78, 1621-62.
[222] There is a realm and it's expanding. It accommodates individuals, government, small business, large organizations, software creators, systems engineers, and others, jostling one another and, in the end, clamoring for attention. What they do becomes law when their deeds are recurrent; everybody is aware of them; a majority condones the acts; that is, they formally ratify them or do so by silence. *Chick*, *supra* note 3, at 186-90.
[223] *Wible*, *supra* note 178, at 1590.
[224] *See, e.g.*, *Aquillina*, *supra* note 4, at 140-42; Burton, Lane, & Van Nessen, *Mandatory Notification of Data Breaches: Issues Arising from Australia and EU Legal Developments*, 26 COMPUTER LAW & SECURITY REV. 115 (2010) (private sector obligations to protect unauthorized disclosure of personal information).
[225] *See* Anzivino, *The Fraud in the Inducement Exception to Economic Loss Doctrine*, 90 MARQUETTE L. REV. 921, 943 (2007).
[226] *Id.* at 933. When claims about goods are accompanied by untrue collateral claims, coughing-up money for such collateral claims is fraud in the inducement. HTP, Ltd. v. Lineas Aereas Costarricenes, S.A., 685 So.2d 1238, 1239 (Fla. 1996); Idem. Ins. Co. v. Amer. Aviation, Inc., 891 So.2d 532, 542-43 (Fla. 2004); Huron Tool & Eng'g Co. v. Precision Consulting Serv., Inc., 532 N.W.2d 541, 546 (Mich. Ct. App. 1995); G.E. Healthcare Financial Servs. v. Cardiology & Vascular Assoc., 2006 WL 950286, at*2 (E.D. Mich. Apr. 12, 2006); Kaloti Enters., Inc. v. Kellogg Sales Co., 699 N.W.2d 205, 219 (Wis. 2005).
[227] Multiven, 725 F. Supp. 2d at 889.
[228] Poe, *Pulling the Plug: The Use and Legality of Technology Based remedies By vendors in Software Contracts*, 56 ALB. L. REV. 609, 620-22 (1996) [hereinafter *Poe*].
[229] Am. Computer Trust Leasing v. Boemer, 763 F. Supp. 1473, 1492-93 (D. Minn. 1991).
[230] *Poe*, *supra* note 196, at 620-22.
[231] Brenner, *Nano Crimes*, 2011 UNIV. ILL. J. OF L. TECH. & POL'Y 39, 77 at fn. 241 [hereinafter *Nano Crimes*]; Cheng, *Do Spybots Finally Have Some Allies: An Analysis of Current Spyware Legislation*, 58 SMU. L. REV. 1497, 1500-01 (2005).

into a herd of computers, all resting until the hacker tells them what to do. Hackers commit crimes when they order computers to make simultaneous demands that force targeted servers to shut down.[232]

Stated boldly, hackers shouldn't disturb another's solitude. Something must be done to preserve anonymity. A lot should be done to protect people's identity, wealth, sense of self-worth, and privacy. Be it physical reality or virtual reality, rummaging through a person's belongings is a tort.[233]

These days, everybody's endowed with the option to spy on others or do nothing. If a person chooses the first option and ploughs through materials another controls, and assumes others will leave alone, its wrongdoing. If the deed peeks ire;[234] that is, makes the victim angry because he's screened the stuff from view and the public, as a matter of practice, has gone about its business without disturbing the stuff, there is a tort. Producing evidence about compromised credit card information, trade secrets, personal correspondence, and exploitable social security numbers warrants damages. Plaintiffs should get a pile of money equal to the sum spent to clean up the mess.[235]

13. Conclusion

America is rife with modern day fears, anxiety and guilt. For some, life is too fast for them. In the Twenty-First Century, man is a wildcard and Earth's latest experiment. Having assaulted mother-nature and discovered that nature will push back, man has created a parallel universe where he can do anything. Problems arise when man drops in and out of cyberspace to do evil. Something must be done about the wickedness. Some ideas have been proposed in this work to deal with irritating and outrageous conduct. Time will tell us what we'll do.

* * * * *

[232] *Nano Crimes*, *supra* note 205, at 58-59.
[233] Dalsen, *Civil Remedies for Invasions of Privacy: a perspective on Software Vendors and Intrusions upon Seclusion*, 2009 WIS. L. REV. 1060, 1068-69 [hereinafter *Dalsen*]; *see* RESTATEMENT (SECOND) OF TORTS § 652B (1977).
[234] *Dalsen*, *supra* note 232, at 1072-73.
[235] *Id.* at 1086.