Volume VII - Article 2

"I JUST BOUGHT A FLAT SCREEN T.V. IN KOLKATA?" APPLICATION OF LAWS FOR INTERNATIONAL OUTSOURCING RELATED IDENTITY THEFT

by Samantha Grant[*]

Fall 2006

Abstract

Because the internet makes it economical to do so, many American companies have sent their customer service jobs overseas. Workers in these outsourced jobs often have access to personal financial information of American citizens. Recent identity thefts, both in America and abroad, highlight the need for laws mandating tighter security by the companies that hold and trade personal information. This paper explores American legislation attempting to deal with identity theft crime as well as parallel laws in India, where many of the outsourced jobs are located. Furthermore, this paper suggests that any federal legislation ought not to preempt state law, as California law is currently protecting consumer privacy stronger than proposed legislation would.

Introduction

In May of 2005, four American Citibank customers "reported that $426,000(Rs 1.90 crore) was missing from their bank accounts."[1] The bank found that the money had

[*] Samantha Grant is currently an attorney with Lindahl, Schnabel, Kardassakis & Beck, LLP practicing civil litigation. Ms. Grant is a 2006 graduate of the University of California, Davis School of Law where she served as the Articles Editor of the U.C. Davis Law Review. Ms. Grant has previously published articles on topics related to environmental policy.

been electronically transferred to accounts in Pune, India. The thieves had registered fake email accounts in the names of the victims, so all notifications of the transfers were diverted. After laying a trap, the bank caught two men who worked in call centers in Pune. Apparently, after Citibank taught them to make friendly chit-chat with their global customers, the two call center employees were able to talk customers into unwittingly divulging passwords and pin numbers over the phone, and the call center employees stole thousands of dollars in the process.

Although some call center employers now take extreme personnel security precautions, identity theft is becoming increasingly more common.[2] To complicate matters, often the internet thief is located in a different country from the victim. This essay explores laws that apply to identity theft, and how they may apply to transnational identity theft crimes. Part I examines the parallel growth in identity theft and outsourcing.[3] Part II explores American and Indian laws upon which plaintiffs might base a cause of action.[4] Part III argues that the recently proposed federal identity theft legislation provides consumers with less protection than current state law.[5] This part suggests that companies ought to employ federal laws that are already in place to prosecute identity theft criminals. In addition, Part III argues that to best protect and empower American victims of identity theft, Congress ought to pass a consumer protection law similar to the California Database Protection Act and should require

---

[1] Malini Bhupta, *Call Centre Con*, India Today, May 2, 2005, at 42.
[2] Pete Engardio et al., *Outsourcing: Fortress India? Call Centers and Credit-Card Processors are Tightening Security to Ease U.S. and European Fears of Identity Theft*, Bus. Wk., Aug. 16, 2004, at 28 (describing how some Indian call centers require employees to empty their pockets and relinquish bags, cell phones, PDAs, pens, and notebooks before entering the workplace).
[3] *See infra* Part I.
[4] *See infra* Part II.
[5] *See infra* Part III.

mandatory contract language between data exporters and data importers that protects third party victims.

I. Identity Theft, Outsourcing & India

Identity theft occurs when one takes another person's birth date, social security number, or other personal information in order to assume the person's identity when obtaining goods or services in the person's name.[6] A Federal Trade Commission report estimated that approximately 10 million Americans suffered from identity theft in 2003.[7] This same survey reported that identity thieves stole, on average, $10,200 from each victim.[8] The loss to businesses totaled $33 billon.[9]

In the past, identity theft was mostly caused by a lost purse or wallet, or some sort of physical theft.[10] The internet, however, dramatically expands the possible occurrences and impacts of identity theft.[11] Not only may the internet provide access to identifying

---

[6] Timothy H. Skinner, *California's Database Breach Notification Security Act: The First State Breach Notification Law is Not Yet a Suitable Template For National Identity Theft Legislation*, 10 RICH. J.L. & TECH. 1, 10 (2003).

[7] FTC IDENTITY THEFT SURVEY REPORT 4 (September 2003) *available at* http://www.ftc.gov/os/2003/09/synovatereport.pdf. (noting that 4.6% of Americans surveyed in 2003 reported their personal information had been misused to open new credit card accounts, take out new loans, fraudulently renting apartments, or obtaining medical services under their name).

[8] *Id.* at 6 (noting that victims spent average of $500 and 60 hours of own time clearing their name). Although most victims of identity theft cannot believe it happened to them, there are certain demographic factors that make a person a more likely candidate to suffer from such theft. Betsy Broder, Assistant Dir. for the Div. of Planning and Info. of the Bureau of Consumer Prot., FTC, Prepared Statement of the Federal Trade Commission on Identity Theft Before the Committee on Banking and Financial Services (Sept. 13, 2000), http://ww.ftc.gov/os/2000/09/idthefttest.htm #N_3_.

[9] *Id*. Individuals are usually not liable for the losses generated by identity thieves. Laws such as the Truth in Lending Act limit consumer liability in such situations. 15 U.S.C. § 1601 (2000 & Supp. III 2003). For example, the statute limits consumer liability for unauthorized credit card charges up to $50.00. 15 U.S.C. § 1643 (2000).

[10] *See* FTC IDENTITY THEFT SURVEY REPORT 4 *supra* note 7.

[11] Betsy Broder, Assistant Dir. for the Div. of Planning and Info. of the Bureau of Consumer Prot., FTC, Prepared Statement of the Federal Trade Commission on Identity Theft Before the Committee on Banking and Financial Services (Sept. 13, 2000), http://ww.ftc.gov/os/2000/09/idthefttest.htm #N_3_.

information, but it also offers innumerable online merchants from whom a thief can make illegal purchases.[12]

Sending work abroad, once called "offshoring," occurs when a company "hires a foreign company to perform a business function."[13] The internet also facilitates this type of business transaction. Now known as "outsourcing," this practice is touted by American companies who claim that it provides their firms with a "larger skill set and cuts down on production time by freeing up domestic personnel to concentrate on more time-sensitive assignments."[14] The primary motivation to outsource work, however, is actually cost savings.[15] For the salary it would pay an American engineer, for example, a company could obtain engineering services from "three Indians, four Chinese, or five Russian" workers.[16]

In India, "call centers and back-office services are the fastest growing segment in the India's $22 billion technology and outsourcing industry."[17] Such operations have been growing by 50% each year since 2000.[18] These businesses provide twenty-four hour "customer support, online technical help, and telemarketing services" for "airlines, banks, credit card companies, and retail chains."[19] Indian outsourcing firms are expanding into new service areas such as "filing tax returns, interpreting medical reports,

---

[12] *Id.*
[13] Christopher L. Sorey, *The Hidden Risks of Outsourcing: Is Your IP Safe Abroad?*, 1 Am. U. Bus L. Brief 33, 33 (2005), *available at* http://www.wcl.american.edu/blb/01/2sorey.pdf?rd=1.
[14] *Id.* (citing Scott W. Pink, *Recent Trends in Outsourcing: Understanding and Managing the Legal Issues and Risks*, 781 PLI/PAT 363, 367 (2004)).
[15] A study by the Forrester Research Company estimates that due to such compelling cost-savings, companies will outsource 3.3 million American jobs by 2015. This study also predicted that 70 percent of those jobs would move to India, 20 percent would move to the Philippians, and 10 percent to China. John Schwartz, *Experts See Vulnerability as Outsiders Code Software*, N.Y. TIMES, Jan 6, 2003, § C, at 1.
[16] *Id.*
[17] Saritha Rai, *Indian Outsourcers Move to Fix Security*, INT'L HERALD TRIB., June 17, 2005, *available at* http://www.iht.com/articles/2005/06/16/business/security.php.
[18] *Id.*
[19] *Id.*

and providing legal support for western companies."[20] In the process, the Indian employees of these outsourcing firms have ever-expanding access to the private financial information of American citizens. This leads to the question of what laws protect the consumer whose personal information is subject to this transnational data flow.

II. Privacy & Security Laws

There are two types of victims of identity theft: the actual people whose identities are stolen, and the companies who possess the information when it is stolen. California state law currently protects people whose personal information has been stolen.[21] Companies that wish to go after those who misuse their information have a few federal statutes at their disposal that give rise to subject matter jurisdiction. India, by comparison, has several national identity theft laws. The plaintiff's challenge there, however, lies in urging the Indian government to enforce those laws.

A. American Legislation

The United States does not have comprehensive data protection laws. Currently, there is only a patchwork of federal and state laws governing this area. Congress originally did not appear to recognize a strong need for specific computer crime legislation.[22] In the early 1980s, Congress was concerned that specific computer crime laws might be redundant and federally overreaching.[23] Federal laws initially addressed

---

[20] *Id.*

[21] *See generally* Edmund Mierzwinski, *Preemption of State Consumer Laws: Federal Interference is a Market Failure*, 6 N.Y. ST. B.A. GOV'T L. & POL'Y J. 6 (2004) (noting that California and Vermont adopted omnibus credit reporting and privacy reforms before Congress, and seven states granted consumers right to obtain free annual credit reports).

[22] *See* Joseph B. Tompkins, Jr. & Linda A. Mar, *The 1984 Federal Computer Crime Statute: A Partial Answer to a Pervasive Problem*, 6 COMPUTER/L.J. 459, 471-81 (1986).

[23] *Computer Crime: Hearing Before the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary*, 98th Cong., 1st Sess. 5, 6 (1983) (recording statement of Rep. George Gekas regarding fears of redundancy with existing laws, and statements of Rep. Robert Kastenmeier on Federal overreaching).

particular privacy harms and regulated certain applications of data.[24] The Right to Financial Privacy Act of 1978 and the Electronic Communications Privacy Act of 1986, for example, were intended to prevent the government from violating people's privacy.[25] Both of these acts are less useful for prosecuting thieves who steal identities from databases they are authorized to access via their jobs. The Computer Fraud and Abuse Act of 1984 provides a better foundation for identity theft claims, especially those originating abroad. In addition to these federal statutes, states have also enacted laws governing data protection. Most notably, California's privacy laws have filled some of the gaps left open by the federal statutes.

i. Federal Laws

Two federal statutes that are often cited, but are not particularly helpful to identity theft victims, are the Right to Financial Privacy Act ("RFPA") and the Electronic Communications Privacy Act ("ECPA"). The RFPA only creates a cause of action when a government authority obtains access to or copies of the financial records of a consumer whose information is stored with a financial institution.[26] Thus, this statute cannot be used against those who steal outsourced information because the thieves presumably are not associated with the United States government. The ECPA's usefulness is limited because it does not allow thieves to be prosecuted if they had authorization to view the

[24] Margaret P. Eisenhauer, *Privacy and Security Law Issues in Off-Shore Outsourcing Transactions*, 829 PLI/PAT 777, 784 (2005) (noting privacy harms such as collecting data from children, use of credit card reporting data).
[25] Right to Financial Privacy Act of 1978, 12 U.S.C. § 3402 (2000) (prohibiting government access to financial institution customer records absent consent or judicial subpoena); Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2701(a)(1) (2000) (prohibiting unauthorized access to a "facility through which an electronic communication service is provided"); SECURING PRIVACY IN THE INTERNET AGE (Anupam Chander & Margaret Jane Radin eds., 2005).
[26] 12 U.S.C. § 3402.

information.[27] In *Educational Testing Service v. Kaplan Education Center Ltd.*, a district court in Maryland interpreted the Stored Communications Act to allow information viewed on a computer, memorized, and later published.[28] There, instructors from a test preparation company repeatedly took graduate school admissions exams administered on computers and memorized the questions for use in their classes.[29] The court held that because the instructors were authorized to view the test questions, they did not violate the ECPA. Likewise, the ECPA could not be used to prosecute overseas outsourced employees because they are authorized by their employer to view clients' personal information.

Like the ECPA, the Computer Fraud and Abuse Act ("CFAA") provides civil remedies for certain types of computer crimes.[30] This Act covers computers used by the federal government, financial institutions, or computers located outside the United States used in a manner that affects foreign commerce.[31] Notably, unlike the ECPA, the CFAA does not permit improper uses of information merely because the thief at one point had authorization to view the information.[32] The CFAA creates a cause of action when the thief's conduct causes a loss to one or more people of $5000 or more, within one year.[33] A person harmed by a violation of the statute can receive compensatory damages and injunctive or other equitable relief.[34]

---

[27] ETS v. Stanley H. Kaplan Educ. Ctr., Ltd., 965 F. Supp. 731, 740 (D. Md. 1997).
[28] *Id.* (interpreting Act to apply when "the trespasser gains access to information to which he is not entitled to see, not those in which the trespasser uses the information in an unauthorized way").
[29] *Id.* at 733-34.
[30] 18 U.S.C. § 1030 (2000 & Supp. III 2003).
[31] 18 U.S.C. § 1030(e)(2) (2000 & Supp. III 2003).
[32] 18 U.S.C. § 1030(a)(2)(C) (2000 & Supp. III 2003); Theofel v. Farey-Jones, 359 F.3d 1066, 1078 (9th Cir. 2004) (holding that subpoena asking ISP to disclose "all copies of emails sent or received by anyone" and not limited to subject of trial violated authority warranted by subpoena under CFAA).
[33] 18 U.S.C. § 1030(a)(5)(B)(i) (2000 & Supp. III 2003).
[34] 18 U.S.C. § 1030(g) (2000 & Supp. III 2003).

Aside from statutes specifically aimed at data theft, Congress has also enacted other statutes that contain language about data protection. One, the Gramm-Leach-Bliley Privacy and Safeguards Rule ("GLB Act"), regulates information held by U.S. financial institutions.[35] Another, the Health Insurance Portability and Accountability Act ("HIPAA"), protects health information processed by healthcare providers, health plans, and information clearinghouses.[36] "To the extent the company has posted privacy statements (or otherwise made representations to consumers or employees) about privacy and security," the GLB Act and HIPAA require the company to comply with those statements.[37] The GLB Act and HIPAA do not "address the issue of trans-border data flows directly."[38] As a result, some state legislatures have worked towards passing bills aimed at regulating private information.[39] "At least 32 states considered over 127 bills to restrict outsourcing "— mostly the outsourcing of state data processing.[40] Other bills focus on general privacy.

ii. California Laws

California is a nationwide leader in protecting the use of personal information over the internet.[41] The California Online Privacy Protection Act requires any company, wherever located, that gathers personal information from Californians online, to post

---

[35] 15 U.S.C. §§ 6801-6827 (2000) (covering non-public personal financial data possessed by financial institutions).
[36] 45 C.F.R. §§ 164.302-.318 (2005).
[37] Eisenhauer, *supra* note 24, at 785 (noting privacy harms such as collecting data from children, use of credit card reporting data).
[38] *Id.* at 784.
[39] *Id.* at 785; *see, e.g,.* Virginia's Computer Crimes Act, VA. CODE ANN. §§ 18.2- 152.1-.16 (LexisNexis 2004 & Supp. II 2006) (prohibiting access to protected information on computers).
[40] Eisenhauer, *supra* note 24, at 790.
[41] Kelly D. Talcott, *California Leads the Way: Rash of New Laws Helps Protect Personal Data of E-Consumers*, N.Y. LAW J., Oct. 19, 2004, at 5 (discussing California Consumer Protection Against Computer Spyware Act, Security Act, Online Privacy Proteciton Act, Direct Marketing Act); *see also Identity Thieves' Secret Weapon*, N.Y. TIMES, Apr. 15, 2005, at A18 (describing Californian consumers as playing "the canary in the data mines").

privacy notices.[42] Another law, the California Security Act, requires businesses that own or license the personal information of California residents, to implement and maintain reasonable security measures to protect the information from unauthorized access or disclosure.[43] The California Database Protection Act ("CDPA"), in turn, requires companies that suffer a security breach of personal information of California residents to disclose that breach provided that the personal information includes the person's name and other identifying number such as social security number, driver's license number or financial account information.[44]

Some believe that because of "California's size and leading role in the high tech industry, SB 1386 'could create a de facto national disclosure policy' even absent the passage of federal legislation on the subject."[45] This is because a company that experiences a breach and must disclose the breach to its Californian clients would be hard pressed to justify not disclosing the breach to its clients in other states.[46] Not only that, but it may be cheaper and easier to disclose to all of its customers at once.[47] These theories have proven the test of reality, as demonstrated by the ChoicePoint incident. In February of 2005, ChoicePoint, a data brokering firm, announced that it had divulged files on over 145,000 customers to thieves posing as legitimate small businesses.[48] The

---

[42] CAL. BUS. & PROF. CODE § 22575 (West 2006).
[43] CAL. CIV. CODE § 1798.81.5 (West 2003).
[44] CAL. CIV. CODE § 1798.82 (West 2003) (the California legislature passed this act after a computer hacker broke into a state-operated data storage facility and gained exposure to the personal information of all 265,000 state employees); RISK MGMT. ALLIANCE, WHITE PAPER: CAL. DATABASE PROT. ACT OF 2003, 1 (2003), http://www.cybersure.com/documents/seminar/database_protection.pdf.
[45] *See* Skinner, *supra* note 6, at 14; Jane Strachan, *Cybersecurity Obligations*, 20 ME. B.J. 90, 90, 94 (2005); Robert Vamosi, *Security Watch: Congress Loves Identity Thieves*, CNET, Nov. 11, 2005, http://reviews.cnet.com/4520-3513_7-6381707-1.html (describing California law as "gold standard").
[46] Skinner, *supra* note 6 at 24.
[47] Kevin Poulsen, *California Disclosure Law Has National Reach*, SECURITYFOCUS, Jan. 6, 2003, http://www.securityfocus.com/news/1984.
[48] Michael Rasmussen, *ChoicePoint Security Breach Will Lead to Increased Regulation*, CSO ONLINE, Mar. 3, 2005, http://www.csoonline.com/analyst/report3416.html.

company initially only disclosed this information to its California clients, because it had no obligations to clients of other states that lacked laws requiring disclosure of breaches of information security.[49] ChoicePoint soon divulged the breach to customers in other states, however.[50] Although the ChoicePoint disclosure was not the first made under the CDPA, it made enough headlines to spur federal legislators to action.[51]

Some argue, however, that notifications of breaches in data security may be unnecessary and may in fact exacerbate the damage.[52] Notification provides hackers the notoriety they crave, and credit card companies argue that their consumers are protected by zero liability provisions in consumer contracts and need no such notice.[53] Also, the language of the CDPA may provide loopholes that would make it undesirable as a template for federal legislation.[54] For example, companies need not disclose a breach if data had been stored in an encrypted form.[55] If data has been encrypted with weak technology and a hacker is able to break the encryption, the CDPA may not be triggered.[56]

Some have argued against such state-specific privacy and security laws because, although it may be easy to comply with the California law, businesses would run into

---

[49] Because of the CDPA, ChoicePoint notified between 30,000 and 35,000 California residents that their personal information may have been accessed by "unauthorized third parties" but the company chose not to notify customers in other states of the breach. Bob Sullivan, *Database Giant Gives Access to Fake Firms*, MSNBC, Feb. 14, 2005, http://www.msnbc.msn.com/id/6969799/.
[50] Rasmussen, *supra* note 48.
[51] *Id.* (noting that Wells Fargo made at least three disclosures from when Congress enacted CDPA to when ChoicePoint made its disclosure).
[52] *Id.*
[53] Visa "Zero Liability," http://www.usa.visa.com/personal/security/visa_security_program/zero_liability.html (last visited Sept. 30, 2005) (noting in fine print footnote that "[f]inancial institutions may impose greater liability on the cardholder if the financial institution reasonably determines that the unauthorized transaction was caused by the gross negligence or fraudulent action of the cardholder — which may include your delay for an unreasonable time in reporting unauthorized transactions").
[54] *See* Poulsen, *supra* note 47.
[55] CAL. CIV. CODE § 1798.82(a) (West Supp. 2006).
[56] *See* Poulsen, *supra* note 47.

problems if other states passed similar legislation.[57] Each state might have different requirements and penalties, which would mean that companies conducting business over the internet in different states would be burdened the most.[58] Also, conflicting laws might result in consumer confusion.[59] In light of these problems, Congress is considering several information security bills, although some of them provide consumers with less protection than the CDPA.[60]

B. Indian Laws

India has several laws upon which an identity theft plaintiff could base her claims, provided the thief was operating in India. The Indian Contract Act and the Specific Relief Act regulate contractual arrangements and impose civil sanctions. The Information Technology Act and the Indian Penal Codes impose criminal sanctions on thieves who use computers to commit their crimes. However, despite the presence of these helpful laws, a plaintiff might choose to sue in America simply because India lags in the area of enforcement.

The Indian Contract Act awards compensatory damages to a party that has suffered a breach, but it does not award damages for any remote or indirect loss.[61] An American business could use this Act to sue the company it outsourced to if the latter were to violate a contractual requirement to hold information confidential. Indian courts are reluctant, however, to enforce large liquidated damages or unlimited penalties, though they will usually enforce the compensatory damages described by the parties in the

[57] *See* Talcott, *supra* note 41.
[58] *Id.*
[59] *Id.*
[60] *See infra* Part III.A.
[61] Indian Contract Act, 1872, No. 9, Acts of Parliament, 1872, *available at* http://indiacode.nic.in/ichome.asp (follow "act year" hyperlink; then enter "1872" as year).

contract.[62] Indian courts will typically disregard penalties such as higher interest rates in the event of default, and re-compute them at reasonable rates.[63]

The Specific Relief Act, along with the Contract Act, could be used to enforce provisions in outsourcing contracts.[64] For example, if an outsourcing contract requires an off-shore service provider to destroy all imported data, and it refuses to do so, the outsourcer could use the Specific Relief Act to enforce that part of the contract.[65] In the face of imminent danger to data security, outsourcers may use the Specific Relief Act to seek a temporary or perpetual injunction.[66]

The India Penal Code assigns a prison term of two years, a fine, or both, for a person who dishonestly misappropriates or converts to his own use any movable (corporeal) property.[67] Crimes such as forgery or cheating have been interpreted as affecting corporeal property.[68] Data, however, "being incorporeal, may not fall within the interpretation of [movable] 'property' under the IPC."[69]

The Information Technology Act addresses computer crimes such as hacking,[70] breach of confidentiality,[71] and damage to source codes.[72] The Act imposes up to three

---

[62] Chetan Nagendra, *A Suitable Law is Not Ready Yet*, THE FIN. EXPRESS, June 28, 2005, *available at* http://www.financialexpress.com/archive.html (enter date of article; last article listed under the title "FE INSIGHT").
[63] *Id.*
[64] Specific Relief Act, 1963, No. 47, Acts of Parliament, 1963, *available at* http://indiacode.nic.in/ichome.asp (follow "act year" hyperlink; then enter "1963" as year).
[65] Nagendra, *supra* note 62; *see* Specific Relief Act, 1963, No. 47, Acts of Parliament, 1963 *available at* http://indiacode.nic.in/ichome.asp (follow "act year" hyperlink; then enter "1963" as year).
[66] Nagendra, *supra* note 62; *see* Specific Relief Act, 1963, No. 47, Acts of Parliament, 1963 *available at* http://indiacode.nic.in/ichome.asp (follow "act year" hyperlink; then enter "1963" as year).
[67] INDIA PEN. CODE § 403 (1994).
[68] Nagendra, *supra* note 62.
[69] *Id.*
[70] Information Technology Act, 2000, No. 21, § 66, Acts of Parliament, 2000 (defining hacking as when person, "with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means").

years in prison for hacking and damaging source code, and up to two years for breach of confidentiality.[73] All three actions expose the wrongdoer to fines.[74] The Act specifically states that it applies to offenses committed outside of India "by any person if the act or conduct constituting the offense involves a computer, computer system, or network located in India."[75] The Act also states that

> [i]f any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium . . . he shall be liable to pay damages by way of compensation.[76]

Notably, the Information Technology Act established the Cyber Regulations Appellate Tribunal to adjudicate cyber crimes.[77] The Act grants this Tribunal the same powers that are vested in a civil court, such that it may subpoena individuals to appear before it, require discovery, and receive evidence on affidavits.[78] Parties may appeal a Tribunal holding before the India High Court. The Tribunal operates a website, in English, that allows a victim of identity theft to email a grievance directly to the Cyber Crime Investigation Cell of the Mumbai police.[79] Although this initial act of

---

[71] *Id.* § 72 (defining breach of confidentiality as when a person, "has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned [and] discloses such…material to any other person").
[72] *Id.* § 65 (defining computer source code as, "the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form").
[73] *Id.* §§ 66, 65, 72.
[74] *Id.*
[75] Information Technology Act, 2000, No. 21, § 75, Acts of Parliament, 2000.
[76] *Id.* § 43(b).
[77] *Id.* § 48.
[78] *Id.* § 58.
[79] Cyber Crime Investigation Cell, http://www.cybercellmumbai.com/cyber-crimes/ (last visited Nov. 19, 2005) (noting that cybercell investigates such crimes as cyberstalking, child pornography, virus dissemination, credit card, net extortion, and internet fraud).

investigation is easy for an American to start at home, the actual trial still requires the parties to physically appear in court in India.[80]

India convicted its first cyber criminal in February of 2003, when a Delhi High Court sentenced a call center employee for online cheating.[81] The defendant stole an American citizen's credit card information to order a color television and a telephone.[82] However, this incident has not spurred many other computer crime cases. In general, India has been criticized for its lack of enforcement of the Information Technology Act.[83] By November of 2003, India had charged eleven individuals with violating the Act, but only fully prosecuted two.[84]

III. Redress

Companies that partake in transnational data flow for outsourcing must understand the various laws that may apply to a data breach. They must determine if domestic laws, both federal and state, will regulate data post-transfer.[85] They must also comply with state laws that may protect the consumer whose personal information they are transferring. Companies must also determine whether the laws of the country to which the data is transferred give rise to any additional liabilities.[86] Individual victims of identity theft must determine if they have standing under various state, federal, or foreign statutes, and then decide where to bring a suit.

---

[80] Indian Bare Acts, http://helplinelaw.com/bareact/index.php?dsp=cyber-reg (last visited Nov. 19, 2005).
[81] *See* Eisenhaur, *supra* note 24 at 793.
[82] *Id.*
[83] *Id.* Each year the United States Trade Representative publishes a "Special 301" review of the adequacy and effectiveness of intellectual property rights in 90 countries. This document notes that due to inadequate laws and inefficient enforcement, India remains on the priority watch list. UNITED STATES TRADE REPRESENTATIVE, 2005 SPECIAL 301 REPORT 1 (2005).
[84] David Lazarus, *Credit Agencies Sending Our Files Abroad*, SAN FRANCISCO CHRON., Nov. 7, 2003, at A1, *available at* http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2003/11/07/MNG4Q2SEAM1.DTL.
[85] Eisenhauer, *supra* note 24, at 784.
[86] *Id.*

This paper argues against enactment of the currently proposed federal identity theft legislation for two reasons. First, state law provides superior remedies to consumers against companies who may lose their information in data breaches as compared with proposed federal legislation. Second, the federal CFAA already provides companies with a cause of action against persons outside the United States who either misappropriate or misuse the company's data. If Congress does enact federal consumer protection legislation, it ought to, at the very least, mandate disclosure of breaches in security and provide consumers a private cause of action against those who traded their data.

A. California Law Provides Better Consumer Protection Than the Proposed Federal Law

As the ChoicePoint fiasco demonstrated, state law does function to notify and protect consumers in the event that a corporation that holds their personal information suffers a data breach.[87] If Congress passes no federal legislation in this area, then over time the California standard would become the de facto standard outside California.[88] For many reasons, this may provide stronger protection for potential identity theft victims in the future than would future federally enacted legislation.[89]

California is known as a state focused on consumer protection; as it stands, the California identity theft statutes are fairly rigorous.[90] Seeing the importance of these

[87] *See supra* text accompanying note 49.
[88] Eisenhauer, *supra* note 24.
[89] Tom Zeller, Jr., *Data Security Laws Seem Likely, So Consumers and Businesses Vie to Shape Them*, N.Y. TIMES, Nov. 1, 2005, at C3.
[90] *See* Barry A. Abbott & Clayton T. Coon, *Financial Privacy and the California Experience*, 23 ANN. REV. BANKING & FIN. L. 411, 411 (2004). *See generally Identity for Sale? Protecting Consumers from Identity Theft Before the Senate Judiciary Comm.*, 109th Cong. 5 (2005) (statement of Gail Hillebrand, Senior Attorney, & Susanna Montezemolo, Policy Analyst, Consumers Union), *available at* http://www.consumersunion.org/pub/0413%20identity%20theft%20statement%20final.pdf. Since 2000 California has had an Office of Privacy Protection within its Department of Consumer Affairs. CAL. BUS. & PROF. CODE § 350 (West 2004).

laws, legislators have introduced more than a dozen bills on data security to Congress this year.[91] While this may appear, on its face, to be a step in the right direction, these laws are actually dangerous to consumers.

Representative Clifford Stearns of Florida is the chief sponsor of H.R. 4127, known as the Data Accountability and Trust Act ("DATA").[92] Amongst the various bills before Congress, DATA appears the most likely to be enacted.[93] At first blush, this bill appears tough on data theft. Similar to how California's CDPA protects Californian citizens, DATA would require a company that had suffered a breach to notify any individual in the United States if his personal information was at risk.[94]

Critics, however, argue that this bill would actually cover up data theft more than prevent it.[95] The most problematic element of DATA is its definitions section.[96] DATA defines a "breach of security" as the unauthorized acquisition of electronic data when there is a "significant risk" of identity theft.[97] How a company decides if the data is at this significant risk is up to them. One reporter noted that, "[i]f the House bill were law, Bank of America may have decided there wasn't a 'significant risk' to the 18,000 customers whose names, addresses and Social Security numbers were left on a

---

[91] Zeller, *supra* note 89 (noting bills introduced by Senator Jeff Sessions, R-Alabama, Senator Charles E. Schumer, D-New York, and Representative Clifford B. Stearns, R-Florida). Senators Specter, Leahy, and Feingold introduced S. 1332, 109th Cong. (2005), "Personal Data Privacy and Security Act of 2005," Congressman Cox has introduced H.R. 1817, 109th Cong. (2005), "To Authorize Appropriations for Fiscal Year 2006 for the Department of Homeland Security, and for other purposes," and Congresswoman Bono has introduced H.R. 29, 109th Cong. (2005), "Securely Protect Yourself Against Cyber Trespass Act."
[92] Data Accountability and Trust Act, H.R. 4127, 109th Cong. (2005).
[93] Vamosi, *supra* note 45 (questioning what happened to significantly better bills introduced last April).
[94] H.R. 4127 § 3(a)(1).
[95] Loren Steffy, *Identity Theft Legislation Provides Easy Way Out*, HOUS. CHRON., Nov. 8, 2005, *available at* http://www.chron.com/disp/story.mpl/business/steffy/3448269.html.
[96] Other problems with DATA are that it "does not set a time period within which a company must disclose a breach," and appears to "only target companies that do business across state lines." Jaikumar Vijayan, *Critics Hit Proposed Data Breach Notification Law as Ineffective: If Enacted, It Would Override Tougher Laws at the State Level*, COMPUTER WORLD, Nov. 10, 2005, http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,106116,00.html.
[97] H.R. 4127 § 5(1).

consultant's laptop computer that was stolen from his car."[98] Conversely, the CDPA requires disclosure of a breach regardless of the degree of risk of identity theft.[99] Clearly the California law is stricter on data brokering firms than DATA.

Another drawback with DATA is that it does not allow for a private cause of action.[100] The CDPA, on the other hand, explicitly provides consumers a private right of action to provide monetary and injunctive relief against companies that do not comply with the notice requirements.[101] Interestingly, DATA explicitly preempts any state laws that require data breach notification.[102]

If Congress passes toothless bills that preempt state statues, not only will the current California laws no longer protect California citizens, but the California laws will no longer protect other American citizens indirectly. This would be a giant step backwards in identity theft protection for the United States.[103] Rather, Congress ought to adopt federal legislation that provides at least as much protection as the CDPA.

Of course, an American victim of identity theft could file suit in India. India's Information Technology Act allows for suits in civil court.[104] This is likely to be an expensive proposition, however, because it would probably involve hiring an Indian attorney and appearing in Indian court. The appealing aspect of this venue, however, is that in the event that the Cyber Tribunal finds in the plaintiff's favor, the defendant must

---

[98] Steffy, *supra* note 95; *see also* David Lazarus, *Data Theft Bill a Step Backward*, SAN FRANCISCO CHRON., Nov. 6, 2005, at J1, *available at* http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2005/11/06/BUGP0FJ17S1.DTL ("This really is a case of the fox guarding the hen house.").
[99] CAL. CIV. CODE § 1798.82(a) (West Supp. 2006).
[100] H.R. 4127 § 6(b)(1). ("No person other than the Attorney General of a State may bring a civil action under the laws of any State if such action is premised in whole or in part upon the defendant violating any provision of this Act.").
[101] CAL. CIV. CODE § 1798.84 (West Supp. 2006) (noting in section (c) that customer injured by willful, intentional, or reckless violation of this title may receive up to $3000, and otherwise may receive $500).
[102] H.R. 4127 § 6(a).
[103] Lazarus, *supra* note 98.
[104] Information Technology Act, 2000, No. 21, § 46(5)(b), Acts of Parliament, 2000.

pay "by way of compensation not exceeding one crore rupees to the person so affected."[105] One crore rupees equals approximately $219,178. Were a victim able to convince the Cyber Tribunal that his presence were unnecessary, and retain a local attorney with a lower billing rate than in America, suing in India might not be such an unappealing option.

B. Federal Law: Identity Theft Victims Should Prosecute Extraterritorial Data Thieves Under the CFAA

Apart from its usefulness to private citizens, state law is not as helpful to the corporation wishing to sue a data thief. This is due primarily to an absence of such legislation. Instead, corporations rely on federal law to prosecute extraterritorial data thieves.

Ordinarily, courts may not presume that acts of Congress apply extraterritorially unless Congress states otherwise.[106] A federal district court in Connecticut, however, has interpreted the Computer Fraud and Abuse Act to apply extraterritorially. In *United States v. Ivanov*, the defendant, a Russian citizen, hacked into the computer system of the company Online Information Bureau ("OIB").[107] OIB processed credit card data for internet merchants.[108] After the defendant hacked into the system and obtained the key passwords to control the financial data, he contacted OIB, threatened to destroy the data, and demanded $10,000 for his services to secure the system.[109] The defendant conducted the hacking and authored the extortion emails while situated in Russia.[110] The District

[105] Information Technology Act, 2000, No. 21, § 43(h), Acts of Parliament, 2000.
[106] Sale v. Haitian Ctrs. Council, Inc., 509 U.S. 155, 188 (1993).
[107] United States v. Ivanov, 175 F.Supp.2d 367, 369 (D. Conn. 2001).
[108] *Id.* at 368.
[109] *Id.* at 369.
[110] *Id.*

Court held that despite the presumption that Congress intends its acts to apply only within the United States, "there is clear evidence that the statute was intended by Congress to apply extraterritorially."[111] The Court also held that the plain language of the statute clearly meant it to apply to "interstate or foreign commerce or communication."[112] The Court also noted that the legislative history of the act supported the plain language reading.[113]

This legislative history explains that Congress passed the CFAA as a response to growing fears about computer hackers.[114] When it found that some data crimes were due to thieves "on the inside," Congress amended the CFAA to focus on deterring such white collar crime.[115] Although that particular amendment did not achieve such deterrence,[116] it is now better situated for prosecuting identity thieves who work for outsourcing firms abroad and who may have limited authorization to access sensitive information.

C. Suggested Future Reforms

There are several steps Congress could take to provide American citizens better protection against international identity theft. As discussed in Part III.A., California's CDPA provides superior consumer protection than the proposed federal DATA. Congress should pass a bill that more closely resembles the CDPA; one that does not

[111] *Id.* at 373.
[112] *Id.* at 374 (quoting 18 U.S.C. §1030(e)(2)(B) (2000)).
[113] *Id.* (noting that prior versions of the act did not cover foreign communications despite the fact that hackers are often based abroad).
[114] Dodd S. Griffith, Note, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem*, 43 VAND. L. REV. 453, 463-64 (1990) (explaining that legislatures intended access alone to trigger liability).
[115] *Id.* at 486; *see* H.R. REP. NO. 98-894, at 4-6 (1984), *as reprinted in* 1984 U.S.C.C.A.N. 3689, 3690-92.
[116] Griffith, *supra* note 114, at 486.

grant companies discretion in when they disclose identity revealing security breaches, and one that does provide consumers a private cause of action.

Another action the United States government could take to protect consumers is to create mandatory contractual language for outsourcers. Since June of 2001, the European Union ("E.U.") has provided outsourcers with a set of standard contractual clauses to use when establishing ties with companies outside of the E.U.[117] The purpose of these clauses was "to facilitate data flows from the Community . . . under a single set of data protection rules."[118] This allows E.U. countries to transfer data to countries outside the E.U. while adequately safeguarding the data.[119] This contractual language provided consumers with significant rights by holding the data exporter and the data importer jointly and severally liable in the event of a breach.[120] The E.U. amended this language in 2004 to limit consumers' rights, by changing to a proportionate liability scheme between the data exporter and importer.[121]

Although this particular amendment is not as consumer-friendly as prior versions of the Directive, it is nonetheless worthy of an American counterpart. Certainly American data-exporting firms contract with foreign data importing firms regarding the event of a breech. These contracts, however, are not designed to protect the third party — the individual whose personal information has been compromised. Like the European Union Commission, Congress should pass a bill mandating that such contractual language protect individual consumers. Such a bill would not only complement the

[117] Commission Decision 2004/915, 2004 O.J. (L 385) 74, ¶ 1 (EC).
[118] *Id.*
[119] *Id.*
[120] *Id.* ¶ 5.
[121] *Id.*

normative values of California's CDPA, but would also provide American citizens the same protections as their European counterparts in the global marketplace.

Conclusion

As identity theft becomes increasingly more common, legislators are inclined to sponsor legislation that is tough on those crimes. Politically, these bills are easy to pass because everyone, in theory, supports stronger laws to deter such theft. Upon closer scrutiny, current state law better protects consumers than proposed federal laws. Rather than preempt the state law with weak federal statutes, Congress should pass a bill similar to California's CDPA that requires disclosure of data breaches and allows for private causes of action. In addition, Congress ought to focus on adopting mandatory consumer protection language for use between firms exporting and importing information. These actions would help reduce the number of American citizens receiving unexpected bills for flat screened TVs they supposedly bought in Kolkata, and provide redress for the occasion such theft does occur.