Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework

Issue Presented: Should baseline commercial data privacy legislation include a private right of action?

Position Statement: The National Consumers League strongly urges the adoption of privacy legislation that includes a private right of action with statutory damages.

Background and Mission of NCL

The National Consumers League ("NCL"), founded in 1899, is the nation's oldest consumer organization. The mission of the NCL is to protect and promote social and economic justice for consumers and workers in the United States and abroad. The NCL is a non-profit advocacy group which provides government, businesses, and other organizations with the consumer's perspective on concerns including child labor, work place issues, privacy, food safety, and medication information. On behalf of the general consuming public, the NCL appears before legislatures, administrative agencies, and the courts on a wide range of issues, and works for the enactment and effective enforcement of laws protecting consumers. The NCL also educates consumers on ways to protect their privacy and through its National Fraud Center, to avoid fraud in the marketplace.

As part of the NCL's work to protect consumers, the organization advocates on behalf of consumers nationwide. Under the leadership of Sally Greenberg, Executive Director (2007 – present), NCL is focused on numerous key issues facing consumers in the 21st Century including, "How can privacy be effectively protected?" The NCL issues Policy Statements on its various areas of representation, including the issue of privacy. *See* http://www.nclnet.org/policy-statements. In its Statement on Privacy, the NCL argues for the recognition of privacy as a fundamental human right: "As new technologies, products, and services are introduced into the marketplace and workplace, it is increasingly important to consider the privacy implications on consumers and workers. Government must be vigilant in assuring consumers and workers that their personal privacy is protected." The National Consumers League specifically advcoates that:

1. Government at all levels must address the need for a legal framework for basic privacy protection where self-regulatory measures alone are not sufficient;

2. There must be legal requirements to protect particularly sensitive personal information, as well as exceptions for national security, law enforcement or other very narrow circumstances;

3. The right to privacy must be guaranteed in the marketplace, the workplace, and in government;

4. Personal information about individuals should only be collected where appropriate and by fair and lawful means;

5. The collection of personal information, the purpose of such collection, and the uses of that information should be disclosed to the individuals about whom it pertains;

6. Individuals should be able to control whether and how their personal information may be used for purposes other than those for which it was originally obtained and collected;

7. Individuals should have full access to the information that has been collected about them and be able to correct or remove any information that is not accurate, relevant or complete;

8. Those who hold personal information about individuals must develop mechanisms that provide consumers and workers control over how that information is used;

9. Those who hold personal information about individuals must secure it from unauthorized access, disclosure or use, and from loss, destruction or tampering;

10. Individuals must have private rights of action to hold entities accountable for breaches of their privacy; and

11. Public education about the collection and use of personal information and how to assert control over its collection and use is critical in order for individuals to make informed decisions as they participate in the marketplace and workplace.

The NCL issues Policy Statements in other arenas that impact its Privacy concerns:

- As noted in its General Protections for Consumers of Financial Services and Products, consumers "must also be protected against invasions of privacy. Privacy disclosures should explain in plain language the kinds of personal information that are collected for use in developing marketing profiles and how consumers may prevent that use."
- In its statement on Banking and Credit, the NCL calls on banking and credit card companies to create and disclose privacy policies.
- In its Statement on Health Information Privacy issues, the NCL believes "An individual has a right to privacy with respect to individually identifiable health information. The individual should have the right to decide to whom, and under what circumstances, their individually identifiable health information will be disclosed." The NCL calls for informed consent and notice prior to disclosures, security safeguards and penalties, and education as to the importance of privacy security. Finally, in connection with pharmacy

direct-to-patient (DTP) messaging, the NCL invited representatives from public interest organizations, health professionals, the consumer/privacy movement, pharmacy industry trade groups and retailers, pharmacy vendors and pharmaceutical manufacturers to form a Working Group to create a set of voluntary performance-based best practice principles for the pharmacy industry that build upon the requirements contained in the HIPAA Privacy Rule. The Best Practice Principles elaborated, found at http://www.nclnet.org/health/133-privacy/406-advocates-produce-best-practices-for-pharmacy-privacy, bridges the gap between the protections afforded by HIPAA and fair information practices that define the degree of control that consumers should have over the ways their health information is used.

Given the rapid technological changes that threaten consumer privacy in the marketplace and the workplace, NCL has undertaken several projects to address this issue, including:

- Being an active member of a coalition of consumer, public interest and privacy rights organizations advocating in Congress, federal agencies, and the media for stronger privacy protections, including a national Do Not Track rule.
- Contributing to a major white paper addressing the privacy and consumer protection issues surrounding cloud computing services.
- Providing direct assistance to victims of identity theft and other privacy-related fraud via our Fraud Center where we talk with 15,000 consumers each year.
- Educating consumers and thought leaders about the latest issues related to privacy rights and privacy protection via NCL's Fraud.org website and Savvy Consumer blog as well as NCL's Facebook and Twitter presences.

The Need for a Private Right of Action

With consumer dependence on internet and other electronic transactions and the ensuing transfer of their Personally Identifying Information ("PII") consumers have a vested interest in ensuring that violations involving their information are effectively prosecuted. While Federal Government and State Attorneys General actions are beneficial, their number is typically hampered by budgetary and resource concerns. Thus, consumer private rights of action (specifically the class actions) provide both a necessary deterrent effect to corporations providing lax security and oversight over PII and a way to recoup individual losses when such lax security results in data breaches, theft, and fraud.

The Value of Personally Identifying Information

PII not only has extensive quantifiable value to businesses but also has intrinsic value in and of itself. *See* T. Soma, et al., Corporate Privacy Trend: The "Value" of Personally

Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 RICH. J.L. & TECH. *1 (2009). In light of technological advancement, which often threatens the security of sensitive information, privacy ranks among the most important issues facing modern society. Soma, at *2. Fact is a business that collects and stores PII cannot have a 'privacy policy', without reasonable and prudent data security measures and which is in line with industry security standards. *See* ISO 27002, and PCI DSS.[1] While corporations are beginning to realize the importance of data security, the steady rise of data breaches suggests that the groups making internal policy decisions for many of America's companies have yet to grasp or accept a fundamental reality of the modern business world. Id. at *3. In order to continue benefiting from the value of PII as an asset, corporations must recognize and protect the value of their customers' PII privacy interests in a manner similar to the way they treat and protect financial assets or their trade secrets. *Id*.

PII provides a valuable benefit in the way businesses execute transactions, market their wares, and conduct their daily affairs. For many companies, technological advancement has made corporate America dependent upon the electronic storage, transmission, and management of PII. *Soma*, at * 10, 12–15. But with this benefit comes a concurrent obligation to protect such information. As corporate America becomes more dependent upon PII, they must accept the reality that the management and protection of PII demands closer scrutiny and a greater allocation of company resources. *Id.* at *21. Businesses cannot argue that collecting PII makes them more profitable while simultaneously arguing it is unfair to hold them liable when they fail to properly protect such information with reasonable safeguard measures.

By way of background, the United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves can use identifying data such as SSNs to open financial accounts, receive government benefits and incur charges and credit in a person's name.[2] As the GAO Report states, this type of identity theft is the most harmful because it may take some time for the victim to become aware of the theft and can adversely impact the victim's credit rating. In addition, the GAO Report states that victims of

[1] http://en.wikipedia.org/wiki/ISO/IEC_27002 and https://www.pcisecuritystandards.org/organization_info/index.php

[2] *See* http:///www.gao.gov/new.items/d07737.pdf.

identity theft will face "substantial costs and inconveniences repairing damage to their credit records…[and their] good name."

According to the Federal Trade Commission ("FTC"), identity theft victims must spend countless hours and money repairing the impact to their good name and credit record.[3] Identity thieves use stolen personal information such as SSNs for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[4]

Identity theft crimes often include more than just crimes of financial loss. Identity thieves can also commit various types of government fraud, such as: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. Further, loss of private and personal health information can expose the victim to loss of reputation, loss of job employment, black mail and other negative effects.

Additionally, identity theft crimes in today's world include more than just crimes for financial misuse as identity thieves have used Sensitive Information to assist in preparing or committing acts of domestic terrorism.[5] The additional risk of immigration fraud to national security interests cannot be ignored.

---

[3] *See* FTC Identity Theft Site, http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html.

[4] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. §603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id*.

[5] *See* http://www.pueblo.gsa.gov/cic_text/money/preventidtheft/preventing.pdf (stating that identity thieves "may threaten national security or commit acts of terrorism" and noting that the

According to the Federal Trade Commission ("FTC"), identity theft victims must spend countless hours and money repairing the impact to their good name and credit record.[6] Identity thieves use stolen personal information such as SSNs for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[7] A person whose personal information has been compromised may not see any signs of identity theft for *years*. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to one year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the web, fraudulent attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

Because PII is such a valuable commodity to identity thieves, once the information has been compromised, criminals often trade the information on the "cyber black-market" for a number of years.[8] As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, SSNs, and other PII directly on various

---

September 11 hijackers used fake ID's to board their planes); *see also* http://www.msnbc.msn.com/id/5594385 (stating that the September 11 hijackers "liberally used document fraud prior to that date, some to ease entrance into the United States, others to move around once they were here and to obtain drivers' licenses they needed to board the airplanes.").

[6] *See* FTC Identity Theft Site, http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html.

[7] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. §603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id*.

[8] Companies, in fact, also recognize Sensitive Information as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation's Norton brand has created a software application that values a person's identity on the black market. Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html; *see also* Soma, at *3-4.

Internet websites essentially making the information publicly available. One study found hundreds of websites which displayed stolen PII and that none of these websites were blacklisted by Google's "Safe Browsing list." As the study concluded:

> It is clear from the current state of the credit card black-market that cyber criminals can operate much too easily on the Internet. They are not afraid to put out their email addresses, in some cases phone numbers and other credentials in their advertisements. It seems that the black market for cyber criminals is not underground at all. In fact, it's very "in your face."[9]

Additionally, with health-care related identity theft fraud, a recent report sponsored by Experian indicated that the "average total cost to resolve an identity theft-related incident … came to about $20,000."[10] Moreover, more than half of the victims said they had to pay out-of-pocket costs for health care they did not receive in order to restore coverage. Almost 50 percent said they lost their health care coverage as a result of the incident, while nearly one-third said their insurance premiums went up after the event. Finally, 40 percent of consumers said they were never able to resolve their identity theft. Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.[11] It is this temporal element of identity theft and data risk, namely the time spent repairing or monitoring credit, which is greatly overlooked as an element of damages that the regulations must address.

Compensating the Victims of Identity Theft

The cost to individuals, businesses, and the economy from data security failures and breaches is staggering. In 2006, the cost of fraud was an estimated at $55.7 billion. *Soma*, at

[9] http://www.stopthehacker.com/2010/03/03/the-underground-credit-card-blackmarket/

[10] http://news.cnet.com/8301-27080_3-10460902-245.html

[11] *See, e.g.*, Soma, *supra*, at *3-4.

*44. Victims of privacy breach and identify theft "estimate[d] the total value of all charges on fraudulent accounts in their name" at $87,303 on average. *Id.* Individual consumer estimates ranged from $50 to $500,000 per act. *Id.* Resolution of privacy breaches takes the consumer significant time and funding. *Id.* While it is estimated that the consumer spends ninety-seven hours to repair the damage when an existing account has been used to affect fraud, if a new account has been created in the victim's name, resolution of the breach increases to 231 hours. *Id.* In 2006, the average consumer's out-of-pocket costs to resolve breaches for existing or new accounts averaged $1,884 and $1,342, respectively. *Id.* Not surprisingly, "theft or loss of personal and financial information is the No. 1 concern of consumers worldwide (64 percent)." *Id.*

Many of these losses will never be addressed by administrative enforcement. If private rights of action are afforded, the consumers can attempt to recoup some of the cost borne by them.

Deterring Misconduct

The adequacy of a statutory remedy is also judged by whether it will generally prevent the misconduct at which it is aimed. While no remedy will create perfect behavior, a remedy that has little or no impact on the behavior at which it is aimed is inadequate. Without a private right of action, the remedy proposed by this legislation is incomplete.

Statutory damages would further promote the kind of data security practices that data collectors should be practicing. Fair and Accurate Credit Transactions Act (FACTA), which amended the Fair Credit Reporting Act (FCRA), mandates that organizations are no longer allowed to print the full credit card number on printed receipts. *See* 15 U.S.C. §1681c. Failure to do so may result in civil penalties equal to "actual damages sustained by the consumer as a result of the failure or damages of not less than $100 and not more than $1,000." *See* 15 U.S.C. § 1681n. The practice of printing no more than the last four digits of financial account numbers is certainly now widely spread and therefore, it is arguable that this deterrent created the solid progress and compliance found across the industry.

A private right of action providing for statutory damages in the area of identity theft is not unprecedented. The Identity Theft Enforcement and Restitution Act (ITERA)[12] allows victims to recover costs associated with identity theft such as lost wages due to time taken off work to deal with identity theft damages and money spent to restore credit and identity issues. This criminal statute allows a private right of action to make identity theft offenders "pay an amount equal to the value of the time reasonably spent by the victim in an attempt to remediate the intended or actual harm incurred by the victim from the offense." *See* 18 U.S.C.A. §3663(b)(6). By this comment, we merely ask that a similar private right of action be extended in the civil arena.

Statutory damages related to data breach events should reflect the time spent and expenses incurred by victims who must monitor, protect, repair and restore their identities and credit ratings if such damages are to be a true deterrent. Instead of placing all the burden on the individuals whose data is compromised, statutory damages could compensate individuals affected by data breach events for their time and expenses paid, with a nominal minimum amount similar to the structure in the FCRA's at 15 U.S.C. § 1681n.

Companies with access to PII, should be deterred from created hollow security protections. It is important for a company to create and enforce proper security protocols on which individuals can rely when they hand over their sensitive personal information. It also important to ensure that whatever industry or FTC guideline on security exists, are actually followed. The consequences of the omission of a private right of action are that companies have no real threat when they do not take the steps needed to protect PII. And when PII becomes public, the vast majority of individuals that are harmed will have no legal redress. In short, companies mandate the provision of PII, its electronic storage and transmission but have no real incentive to ensure that the PII is kept safe.

In today's world, it is easy to create protections for sensitive, personal information. Proper guidelines that detail the treatment of PII that are enforceable by both administrative entities and consumers will go a long way to protect individuals' privacy and avoid the possibility of litigation.

[12] http://www.govtrack.us/congress/billtext.xpd?bill=h110-5938

State of Privacy Litigation

In order to create accountability and deter the negligent mishandling of individuals' PII, any commercial data privacy legislation must include a private right of action. Such a provision would also allow for an individual, whose PII has been negligently exposed, to receive some compensation for the damaged to their property and for the disregard of their privacy. While attempts have been made through private litigation to penalize wrongdoers and provide remedies to data breach victims, those lawsuits have been based on state common law and have had all but no success. To effectively provide legal redress for victims of data breaches, a federal right of action must be created.

Presently, individuals only have a private right of action against the federal government for data breaches. *See* 5 U.S.C. § 552a; *In re Dep't of Veteran Affairs (VA) Data Theft Litig.*, MDL 1796 (D.D.C.) (settlement of data breach allegation after laptop theft). While some states are moving towards providing a private right for individual's whose *medical* PII has been compromise to seek redress, [13] that limited allowance has not trended towards a broader right in the state fora. In fact, many courts denied entry to the judicial system itself to victims of data breaches on the basis that they lack standing. A few are: *Allison v. Aetna, Inc.*, 2010 WL 3719243 (E.D. Pa. Mar. 9, 2010); *Amburgy v. Express Scripts, Inc.*, 671 F. Supp. 2d 1046 (E.D. Mo. 2009); *Giordano v. Wachovia Sec., LLC*, 2006 WL 2177036 (D.N.J. July 31, 2006); *Key v. DSW, Inc.*, 454 F. Supp. 2d 684 (S.D. Ohio 2006); *Hammond v. The Bank of New York Mellon Corp.*, 2010 WL 2643307 (S.D.N.Y. June 25, 2010).[14] Only **two** cases have survived summary judgment-- and only for those with instances of actual identity theft as opposed to an increased risk caused by the negligent release of PII. *See Stollenwerk v. Tri-West Health Care Alliance*, 254 Fed. Appx. 664, 667 (9th Cir. 2007) (claim upheld for consumer alleging identity theft yet

[13] *See, e.g.*, Cal. Civ. Code §§56-56.16, *et seq.* (Confidentiality of Medical Information Act); 215 ILCS 5/1001, *et seq.*. (Illinois Insurance Information and Privacy Protection Act).

[14] One Circuit has denied standing to litigants alleging increased risk of identity theft, *Lambert v. Hartman*, 517 F.3d 433, 437 (6th Cir.2008), while two Circuits have recognized standing for such litigants. *Pisciotta v. Old National Bancorp*, 499 F.3d 629 (7th Cir.2007); *Krottner v. Starbucks Corp*. 2010 WL 5141255 (9th Cir. Dec. 14, 2010). While finding standing, both Circuits have nevertheless denied plaintiffs a cause of action for their claim. *Pisciotta, supra* (Indiana law); *Krottner v. Starbucks Corp.*, 2010 WL 5185487 (9th Cir. Dec. 14, 2010) (Washington law); *see also Ruiz v. Gap, Inc.*, 380 Fed. Appx. 689 (9th Cir. May 28, 2010) (California law).

denied for consumers alleging increased risk of identity theft) and *Kuhn v. Cap. One Fin. Corp*., 2006 WL 3007931, *4 (Mass. App. Ct. 2006).

The common set of circumstances surrounding the typical data breaches militate giving some sort of control over the situation to the victim via a private right of action. In most data breaches, a victim has been forced to turn over its PII to a business in the first place as a requirement of their employment, *see Starbucks* or *Aetna*, or a requirement of the employment application process, *see Gap*, or a prerequisite to a financial transaction or account, *see Pisciotta*. Employees, applicants, and consumers are left with no way to protect their PII themselves and are forced to trust the businesses themselves to do protect it. Jonathan J. Darrow and Stephen D. Lichtenstein, "Do You Really Need My Social Security Number?" Data Collection Practices in the Digital Age, 10 *North Carolina Journal of Law & Technology* 1 (2008) (suggesting that when a merchant requires a consumers PII, the relationship is, or should be a fiduciary one). Once a business has negligently leaked an individual's PII, a victim is again left without the tools to protect itself from further harm and limit the exposure of its PII.

Victims of data breaches are forced to continue to give up control of the PII during the data breach aftermath to those that there negligent with it in the first place. A frustrating example of this is the case of *Amburgy v. Express Scripts, Inc.*, 671 F. Supp. 2d 1046 (E.D. Mo. 2009), where thieves not only deliberately hacked into a negligently protected database that contain insurance customers' (medical and financial) PII, the thief then blackmailed the company for millions of dollars with the threat of publishing the victims' PII. Not only did the company fail to adequately protect its customers' PII, it then failed to properly investigate the data breach ***and*** even denied the extent of the data breach for months. Thus, data breach victims were unable to even determine whether or not their PII/PHI had been stolen and attempt to mitigate any potential future harms as a result. Despite this, the court denied the consumers standing and a cause of action. Had a victim of the *Express Scripts* data breach been able to bring a claim under a federal private right of action, then it would have at least been able to uncover the nature of the breach and the extent to which the PII was exposed. Similarly, in *In re: RBS Worldpay, Inc., Customer Data Sec. Breach Litig.*, MDL 2035 (N.D. Ga.), hackers sat on RBS' servers for an undetermined amount of time, downloaded PII, *and* stole approximately $49 million dollars in a

worldwide scheme touching on cities from New York to Rome. Yet the court denied plaintiffs a claim under state law.[15]

In addition, public policy favors allocating the risk of loss to corporations like Gap, Starbucks or Express Scripts, who are best able to prevent the loss or spread the loss. The corporations are clearly the only parties in the facts at issue here who could have prevented the loss to millions of its customers by taking the necessary measures to maintain the security of the sensitive information it was entrusted with. There is nothing the customer could have done to prevent this loss. In addition, if such a loss could not have been prevented, then surely these large corporations, who benefits immensely in the financial sense from its customers' business and employees' services, should be requiring to internalize the costs of this security breach, instead of spreading and externalizing the cost to millions of hapless consumers.

The law, as it has been applied to date, has permitted defendants to externalize on its hapless customers all the costs and burdens of its own negligence and breach of contract by failing to keep the customers' and employees' PII access information safe. While Courts have tried to fashion a remedy with the current law available, data breach victims are still left without recourse. It is time for a legally created redress that an individual can use to protect their PII and recoup their losses from those at fault for the data breach.

15 The only limited relief obtained by average consumers have come in only 4 cases where the defendant opted to engage in early settlement (perhaps for public relations purposes) rather than attack the complaint in court. These settlements have provided data breach victims: reimbursement of for out-of-pocket expenses and time spent to curb the potential losses sustained by stemming from the data breach (such as fees for new bank account checks, long distance phone charges to financial institutions that handle a victim's accounts, fees incurred when ordering new identification, etc.), identity theft insurance policies, and identity theft restoration services. *Lockwood v. Certegy Check Serv., Inc.*, No. 8:07-cv-01434-SDM-TGW (M.D. Fla.); *In re TJX Cos. Retail Sec. Breach Litig.*, MDL 1838 (D. Mass.); *In Re: Countrywide Fin. Corp. Customer Data Sec. Breach Litig.*, No. 3:08-MD-01998-TBR (W.D.K.Y. 2008) (final approval of settlement is currently on appeal); *In Re: Heartland Payment Sys., Inc. Data Sec. Breach Litig.*, MDL 2046 (S.D. Tex.) (final approval still pending).