

Personal Data as Toxic Waste: A Data Protection Conundrum

HOLLY K. TOWLE

The author examines U.S. federal and state data protection laws and concludes that in aggregate, they are having the unintended, counter-productive effect of encouraging or requiring businesses not to know their customers because collection of sufficient data to know them is too dangerous.

Personally identifying information (“PII”) and toxic waste — what do they have in common? The answer is “everything.”

There is only one critical difference, and it creates a conundrum for our times:

- There is no beneficial or common need to use toxic waste, *but*
- Use of PII is *critical* to modern society.

PII:

- Allows distribution of benefits to the right person;
- Allows that person to manage their affairs;
- Allows financial service providers, merchants, and others to avoid dealing with identity thieves; and

Holly K. Towle is a partner with K&LGates LLP, an international law firm, and the cross firm coordinator of the firm’s e-Merging Commerce group. Resident in the firm’s Seattle office, the author may be contacted at holly.towle@klgates.com.

- Prevents the theft of identities and assets.

Given that, we need to ask how can PII be both protected and adequately available at the same time? That is a riddle that local, national, and international legislative bodies (“Legislators”) are not solving in any coherent or realistic manner. Instead, they have enacted and continue to enact a crazy quilt of laws and regulations turning PII into something similar to toxic waste. The message conveyed in modern law for PII is this:

DON’T TOUCH IT — IT GLOWS.

This is the actual message notwithstanding occasional regulatory acknowledgments of the relationship between the ability to collect information and the ability to prevent identity theft and fraud.¹

Before exploring the consequences of this message and the problems it creates, consider the similarities between PII and toxic waste. These principles apply to both:

1. Do not touch it unless you have to;
2. If you have to touch it, learn how or whether to do so – mistakes can be fatal or at least seriously damaging;
3. Do not use normal methods to transport (transfer) it;
4. Attempt to crack the whip over contractor handling it;
5. Do not store some of it at all;
6. Store what you need but in a manner avoiding spills, and limit access;
7. Be alert for suspicious odors and other red flags;
8. Report spills to the relevant people and agencies;
9. Dispose of it only by special means; and
10. Get ready to be sued or incur often unreasonable expenses no matter how much care you take.

To illustrate these points, this article focuses on U.S. federal and state

laws, but similar laws or barriers exist internationally. There is no local, national, or international uniformity. Compliance with the ubiquitous and conflicting rules is unaffordable, unworkable, and impossible. Compliance with one rule set will not comply with others, and even qualifying for a “safe harbor” for one set is meaningless for others. The result is a world in which only criminals are eager to touch PII and they are having, consequently, a field day.

And that is the ultimate irony: if PII really were toxic waste, even criminals would not touch it. However, PII is easily and safely handled by criminals because it is not, really, toxic waste. Only legitimate businesses are required by law or self-defense to *treat it* as toxic waste. Criminals ignore and take advantage of these data protection laws or their excesses and we are all the poorer for it, both in terms of social values and financially. But first, consider the similarities between PII and toxic waste.

PERSONALLY IDENTIFYING INFORMATION – WHAT TO DO AND NOT DO WITH IT

1. Do Not Touch It Unless You Have To

Because modern law makes PII dangerous like toxic waste, the first line of defense for a business is not to collect PII. When it must be handled, the modern message is to treat it as a toxic item that must be handled with extreme care, special systems, and disproportionate liability for the business. This attitude toward PII is the byproduct of modern “data protection” laws, which, ironically, enable identity theft and fraud by making PII so toxic.

Consider Canada, where an employer trying to avoid the possibility of harm conducted a consensual background check on an applicant for a receptionist/petty cash position; a Canadian privacy authority decided in hindsight that the check was not needed and violated applicable privacy law.² It is not as if these kinds of decisions are necessarily irrational, although a reasonable contrary argument can be made. They assume, however, a foreseeability and moderate risk level that does not exist in the real world (or at least in the U.S., the land of class actions). The inevitable

response is to avoid collecting PII (the background check). That is sometimes good and sometimes bad, e.g., in the U.S. a hospital receptionist used the time between registering emergency patients to pluck from their files PII for identity theft. The point is that hindsight is better than foresight and the regulatory lesson to employers is both “do not” and “do” at the same time: they must simultaneously make plausible hires and not step over privacy and regulatory lines that are unknown and ever-shifting in our information economy.³ The employer that is sensitive to data protection laws will try *not* to touch PII, thereby leaving the field clear to applicants bent on ill will.

2. If You Have to Touch It, Learn How or Whether to Do So — Mistakes Can Be Fatal or at Least Seriously Damaging

Radioactive waste and air pollution emissions are not handled identically. However, what is obvious in the context of toxic waste is not obvious for most PII. This is particularly true in the United States, which has a tradition of viewing information that is not truly private as in the “public domain” or “stream of commerce” and as critical to the free flow of information and a democratic society.

What some PII laws preclude will not surprise anyone, e.g., a Missouri statute precluding employers from requiring an employee “to have personal identification microchip technology implanted into an employee.”⁴ The surprise for that kind of statute is that Missouri felt it necessary to pass it at all, given traditional privacy and employment laws.

Laws regarding other types of PII, however, can catch attorneys and their clients unaware. For example, some courts are now pretending that everyone ought to know that a U.S. social security number (“SSN”) is “private” and, thus, should be handled like toxic waste, but that is simply not the case.⁵ For decades SSNs have appeared in public records and have been required on governmental and other forms from which they are only recently being redacted or banned; they also continue to be critical to legitimate commerce.⁶ The point is not that SSNs or other personal information should be handled carelessly. The point is that it is a *change* to have PII (including SSNs) viewed by society as toxic waste, and that

change means that some of the new laws catch many by surprise.

To illustrate, for years drivers licenses or employee identification numbers have been commonly used for identification in various circumstances, yet now, for legitimate transactions:

- There are laws restricting *copying* a drivers' license;⁷
- There are laws restricting "swiping" the magnetic data tracks on a drivers' license;⁸
- There are laws prohibiting writing the license number down, such as on a credit card slip to enhance identification;⁹
- There are laws requiring truncation of employee identification numbers and restricting uses of them;¹⁰ and
- There are laws restricting when a fingerprint or scan can be taken to ensure a financial institution or school is dealing with the correct person.

Regarding the last point and as recently explained by the Illinois legislature, members of its public "are weary of the use of biometrics when such information is tied to finances and other personal information." That is another way of saying that some of the public longs for the days when PII could be taken without a lot of fuss in order to enhance identification in significant circumstances. But those days are gone. With its new law, the Illinois legislature has so increased the "weariness" quotient for use of biometrics for identification, that biometrics should disappear in Illinois.¹¹ Chalk one up for the criminals.

Each of these laws is or will become the subject of litigation and that is when most businesses will learn that these very specific, nonuniform, and often contradictory laws, and myriad others, even exist. How then may a business seek to prevent identity theft? What PII can be used in all 50 states for identification when identification is necessary or desirable and what can be stored to prove that identification was obtained but not retained? If little can be retained, how can the business prove compliance with "know your customer" laws or concepts, and also prove who engaged in the transaction when the counterparty claims, truthfully or fraudulently, "it wasn't me?"

These are good questions to which there is no answer. Ask the same question internationally and there also is no answer. Chalk another point up for the criminal team.

Recently, the U.S. Federal Trade Commission (“FTC”) recommended that Congress adopt national standards for authentication so that businesses will be forced to collect sufficient PII to know with whom they deal¹² — good idea, but worthless unless any such standards preempt state law and provide safe harbors against second-guessing by regulators and litigators (and that is not a good bet, if past experience is a guide).

Even more recently, the FTC decided to skip waiting for Congress. Acting on a signal buried in its report to Congress, the FTC brought an enforcement action under its new theory that failing to have reasonable verification and authentication procedures is, along with other theories previously alleged in private enforcement actions, an unfair act or deceptive practice.¹³ Even if the FTC is empowered to make its own data protection code, businesses cannot authenticate and verify when compliance requires handling toxic waste they are *strongly* encouraged not to touch.

3. Do Not Use Normal Methods to Transport (Transfer) It

For sensitive PII, statutes regulating its transmission prohibit or make inadvisable the use of e-mail or unencrypted transmissions over the Internet. For example, Nevada precludes transmission of “personal information” unless the transmission is encrypted or faxed.¹⁴ The Nevada definition of “personal information” includes a name plus a “sensitive” number such as a driver’s license number, a social security number, or a bank account or payment card number in combination with any required access code (consider a Nevada employer e-mailing PII to headquarters in another state). Several states prohibit anyone from requiring entry of an SSN over the Internet absent encryption;¹⁵ Michigan prohibits internal, unencrypted transmissions of SSNs;¹⁶ and a National Automated Clearinghouse rule can be read to allow faxes but not those utilizing Internet based services such as VOIP.

So what is a person to do? Illustrating the presence of competing societal goals in this area, some businesses are adopting defensive solutions

favoring carbon emissions and tree harvesting by using postal or courier services (paper, delivery trucks, airplanes and gas). Encryption is also an option, but it is an example of a favorite Legislative solution that, in practice, can prove impractical, technologically unworkable, or too expensive.

4. Attempt to Crack the Whip Over the Contractor Handling It

Many data security statutes require the business controlling the data to contract with their service providers to provide similar protection.¹⁷ This forces alteration of contracts with those contractors, possibly in a manner they will not accept. It also assumes that every business has the power and choice among contractors to force the required result and to force contracts containing particular language or “certifications.” Good luck with that.¹⁸ Again, the point is not to ignore service providers or to allow them to run wild, but the inflexibility created by some Legislators can create counterproductive results, such as by forcing the business into noncompliance (because the business cannot obtain the required certification or take or prove that the business took required “reasonable” steps); by forcing the business to forego use of a service provider more knowledgeable than the business (because the service provider refuses to assume the liability requested by the business at the price being paid for the limited services); or by forcing the business to take the second best contractor or the one with nothing to lose (the one that cannot afford to respond to a judgment so will sign anything).

5. Do Not Store Some of It at All

For PII, an example of this concept is provided by the Payment Card Industry (“PCI”) Standard for Data Security.¹⁹ It precludes any storage of some payment card data such as the “CVV2” (the little security code on the back of some cards); data that can be stored must be stored in compliance with the standard. Minnesota has codified a conflicting and/or ambiguous version of the PCI standard,²⁰ thereby creating more confusion and imposing liabilities that would not exist under traditional damage allocation principles. Other states are attempting to follow Minnesota into this black hole of legislation that ignores and upsets the complex balances

already established in payment system laws, standards and contracts, and also ignores the whip-saw impact that these kinds of statutes have on merchants already endeavoring, at significant expense, to comply with PCI and federal law.

Some states seem to delight in taunting their merchants with these new laws and parcel them out a tidbit by tidbit. For example, just about the time merchants and service providers nationally incurred the expense of reprogramming systems to come into compliance with a federal statute dictating truncation of account numbers on credit card receipts *delivered to customers*, these states changed, or are trying to change, the rules again. This time the legislation requires reprogramming for the receipt retained *by the merchant*.²¹ Most merchants do not even know about this change and are targets for class actions, even if they carefully store the retained information in compliance with PCI standards. Granted, merchants can also commit fraud, but one wonders how honest merchants will meet their obligations to prove with whom they dealt or respond to other obligations (such as to prove their compliance with consumer protection rules for disputed transactions). Again, chalk one up for the identity thieves and for customers willing to claim they did not make purchases they actually made. These costs of continual reprogramming and fraud are borne by honest consumers who must subsidize the chaos created by Legislators and regulators.

6. Store What You Need But in a Manner Avoiding Spills, and Limit Access

PII data security obligations abound. Some are *general*, such as Federal Trade Commission enforcement actions taking the approach that a failure to take adequate care of PII is an “unfair practice”²² and state statutes imposing general data security obligations.²³ Some security statutes are *industry specific*, such as the federal Gramm Leach Bliley Act (“GLBA”) and state statutes enhancing it for “financial institutions” (a broadly defined term in the GLBA); some are *data specific* such as for payment card data and various, random state statutes. Examples are a New York statute imposing duties of care for *truncated* social security numbers,²⁴ and a Maine statute creating a security obligation for allowed

copies of drivers' licenses.²⁵

As for access, some businesses have long imposed access controls so that only employees with a "need to know" or with certain authority levels can access PII, and more are doing so as their awareness of modern threats increases. Unbeknownst to most businesses, the FTC has begun to define as law, what access controls are, or are not, adequate. Recent enforcement actions concern allegedly inadequate access controls and one went beyond the business' own systems to require on-site visits to examine *customer* systems.²⁶ Envisioning the practical realities of any such requirements in a global economy is stunning. Chalk one up here for mega-businesses: only they will have any hope of being able to conduct and afford necessary due diligence and of having the power to make necessary contracts – given the current economy, small businesses are the certain losers here and even megabusinesses have, realistically, little hope.

7. Be Alert for Suspicious Odors and Other Red Flags

For PII, federal regulations require "financial institutions" and "creditors" to establish Identity Theft Prevention Programs and consider at least 26 "red flags" portending possible identity theft.²⁷ "Creditors" is a broadly defined term that, according to regulators but not necessarily the law, covers traditional creditors as well as "automobile dealers, mortgage brokers, telecommunication companies, and utility companies"²⁸ and, according to an FTC "guide," anyone who sends a bill to a customer instead of demanding prepayment or immediate payment such as by credit or debit card.²⁹ Way to encourage economic recovery and eliminate standard, beneficial, business practices! Part of these regulations cover "users" of consumer reports (e.g., employers ordering credit reports or background checks) – they must establish procedures to respond to notices of discrepancies in addresses.³⁰

8. Report Spills to the Relevant People and Agencies

For PII, many state and federal statutes require notice if a data security breach occurs.³¹ Sometimes notice is to the "data subject" and sometimes

it is to regulators or another business “owning” the data. The statutes or notices are not uniform so compliance requires review of each that applies. For example, some cover every person or business with a particular tie to a state while others cover data or information brokers or state agencies. Some cover computerized data while others cover data on paper too. Some require notice automatically while others use a threshold such as reasonable potential of harm to a data subject. And some contradict others. For example, the Massachusetts statute says notice of security breach “shall not include the nature of the breach or unauthorized acquisition or use or the number of residents of the commonwealth affected by said breach or unauthorized access or use;”³² other statutes expressly require at least a general description of the breach.³³

9. Dispose of It Only by Special Means

For PII, some states impose general duties to dispose of PII and associated hardware securely, essentially so that it cannot be read, used, or reconstructed, and some require particular internal policies.³⁴ Other laws tie to the particular kind of PII at issue, such as information derived from a credit report or background check.³⁵ As with toxic waste, these disposal statutes require special handling.

10. Get Ready to be Sued or Incur Often Unreasonable Expenses No Matter How Much Care You Take

The Illinois statute mentioned earlier creates a private right of action and authorizes a prevailing party to recover for *each* violation, liquidated damages of \$1,000 or \$5,000 depending upon whether the violation is negligent, intentional or reckless, plus attorneys’ fees and costs.³⁶ The federal Driver’s Privacy Protection Act requires no actual damages to reap a statutory award. In *Kehoe v. Fidelity Federal Bank & Trust*,³⁷ Fidelity paid \$5,656 for 565,600 names used for mailing an offer to refinance auto loans. It did not know, however, that the State of Florida had not properly complied with the Act; Fidelity’s exposure under the resulting action was \$1.4 billion, \$2,500 per violation with no actual damages. The case

settled for a “mere” \$50 million — a wonderful return for the class action plaintiffs’ lawyers who did not have to prove any damages — at all — to anyone. The Minnesota “PCI” statute mentioned earlier awards to financial institutions only, damages that courts have been striking down as not awardable to them under traditional principles of damage awards or payment system contracts.

What about expenses regardless of litigation? Consider the plight of a nonprofit administrator/service provider for student scholarships. It carefully met the request of a multinational college scholarship provider to eliminate social security numbers from the scholarship applications – this multinational corporation was intent on not handling toxic waste. Good idea, only it was not waste. The schools to whom the scholarship funds were sent viewed the SSNs as critical for internal matching purposes and would not accept checks without them. There were at least three losers here: (1) the administrator whip-sawed between the scholarship provider and the universities, (2) the students who never got a scholarship because “their” funds were spent on reprogramming, reprinting, re-collection, and re-training instead; and (3) society as a whole, which benefits from educated citizens. Had the scholarship provider not viewed SSNs as toxic waste, it would have been willing to take the risk of collecting them in the first place.

THE CONUNDRUM

Data protection laws become a joke when data is so protected by law that it becomes too risky to touch.

This is an excellent outcome for criminals and plaintiffs’ class action counsel, but a very sad result for anyone seeking actual data protection. The more Legislators convert PII into toxic waste, the less true data protection will exist.

The apparent hope of Legislators is that every business can and will be able to create systems to navigate through the toxic wasteland that PII laws have created: radioactive data here, contaminated data there, and mercury here, there, and everywhere. Every business, large and small, is mandated to figure it out for 50 states, nationally and internationally, and then, under

some regimes, create perfect systems. Impossible, impractical, unaffordable, and counterproductive.

Even businesses spending millions on this quest ultimately discover several things:

- The laws create an incomprehensible and conflicting maze;
- Perfect systems do not exist;
- Mistakes happen, inevitably;
- Not every “bad” employee³⁸ can be stopped or accurately predicted and, as we know from Canada, punishment will flow from attempts to predict or prevent; and
- Once the business has battened down every hatch, it will be very difficult, if not impossible, to conduct business.

Worse and increasingly, many of the new laws do not even give points for trying and instead impose penalties regardless of fault or damage.

In the meantime, relatively little Legislative energy is focused on law enforcement against criminals and identity thieves, and they know it – spring is here in criminal circles.

PII has been converted to toxic waste. This is intended by some Legislators and in part they are right: if a business has no need for PII then it should not take it — turning PII into toxic waste delivers that message well.

However, that conversion goes too far. Its costs are reflected in increased prices and fraud which are borne by honest consumers and businesses. Society is also diminished by the withdrawal of much beneficial or necessary PII from the “public domain” and by the inability to avoid identity theft by knowing and be able to prove with whom one is dealing. The realistic solution for businesses is:

DON'T TOUCH IT — IT GLOWS.

And there you have it, the conundrum for our time:

Too Much/Too Strict PII Legislation = Toxic Waste = Fraud & Identity Theft & Other Societal Harms

THE SOLUTION?

One solution is litigation, e.g., some of the state statutes that give preference to certain technologies or specifications may violate preemptive federal law; some should violate the U.S. First Amendment or similar precepts in other countries; and some should violate the Dormant Commerce Clause by attempting to regulate interstate commerce. But no one (except the class action bar) likes litigation.

A better solution is nonconflicting, uniform laws that reasonably protect PII, *allow its reasonable use*, require actual damages and fault, and quit assuming that all legitimate data holders are evil. The criminals are the bad guys and they include all of us, i.e., some businesses with lax practices, organized crimes rings, and yes, even the very data subjects these laws protect: all of our friends, neighbors, and co-workers make mistakes, and many of them violate company policies or law in order to sell data, seek revenge, or to commit identity theft. The case law is replete with examples of such identity thieves.

The nation does not need more laws pointing the finger at only one player in this drama (businesses) and it needs fewer laws converting PII into toxic waste. Actual data protection laws, and amendments of existing laws, that create practical and affordable protection for *all* victims of identity theft, i.e., data subjects as well as legitimate businesses are needed. For those who believe our current laws do that, I respectfully dissent.

NOTES

¹ See, e.g., *Staff Summary of Comments and Information Received Regarding the Private Sector's Use of Social Security Numbers* (Nov. 2007), available at <http://www.ftc.gov/bcp/workshops/ssn/staffsummary.pdf>; see also "Security in Numbers *** ** ** SSNs and ID Theft", FTC Report to Congress (12/08) at <http://www.ftc.gov/os/2008/12/P075414ssnreport.pdf>.

² See <http://www.oipc.ab.ca/ims/client/upload/Investigation%20Report%20P2005-IR-008.pdf>.

³ See, e.g., Massachusetts regulation 201 CMR 17.03(g) requiring persons to limit “the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected.” Given that, as they say in the song, one man’s ceiling is another man’s floor, it is not possible to know in advance what is “reasonable,” “necessary” and “legitimate” for purposes of effecting compliance with such a rule, yet foreign Legislators love this concept (perhaps because class actions have largely not yet reached their shores).

⁴ See Missouri Stat. 285.035(2008).

⁵ For a discussion of this issue, see Holly K. Towle and Raymond T. Nimmer, *The Law of Electronic Commercial Transactions* at ¶ 12.14[3] (2003-2009 A.S. Pratt & Sons).

⁶ See FTC Staff Summary, *supra* note 1.

⁷ See, e.g., ME LEGIS 568(2004) (“A person commits a Class D crime if that person ... reproduces ... without the written consent of the Secretary of State a paper or document in the form of a ... driver’s license Notwithstanding this subsection, a person may photocopy without the written consent of the Secretary of State [listed exceptions]”).

⁸ See Cal. Civ. Code § 1798.90.1; see also NH Rev. Stat. § 263.12(X) (prohibiting as a misdemeanor any person to knowingly scan, record, retain or store electronically, personal information unless authorized by the department).

⁹ See Cal. Civ. Code § 1747.08 (2007).

¹⁰ Cal. Labor Code § 226(a) (2004) (restricting certain uses of employee identification number to one showing no more than last four digits).

¹¹ See IL ST CH 740 § 14/5 (2008).

¹² See report in note 1, *supra*.

¹³ See *USA (for the FTC) v. Rental Research Services, Inc.*, FTC File No. 072 3228 (2009).

¹⁴ See, e.g., 2005 NV S.B. 347, § 29 (2005).

¹⁵ See, e.g., Cal. Civ. Code § 1798.85.

¹⁶ See, M.C.L.A. § 445.84 (2004).

¹⁷ See, e.g., Holly K. Towle and Raymond T. Nimmer, *The Law of Electronic Commercial Transactions* at ¶ 16.08[1] (2003-2009 A.S. Pratt & Sons).

¹⁸ See, e.g., Massachusetts regulation 201 CMR 17.03(f), which originally required persons to contract with their service providers and also to do this: “Prior to permitting third-party service providers access to personal

information, the person permitting such access shall obtain from the third-party service provider a written certification that such service provider has a written, comprehensive information security program that is in compliance with the provisions of these regulations.” Given the ambiguities in the regulation and its incorrect assumptions about what compliance is possible, no rational service providers would provide such an unqualified certification. Apparently someone pointed this out so the certification was removed and an amended version requires the business to take:

...all reasonable steps to verify that any third-party service provider with access to personal information has the capacity to protect such personal information in the manner provided for in 201 CMR 17.00; and [take] all reasonable steps to ensure that such third party service provider is applying to such personal information protective security measures at least as stringent as those required to be applied to personal information under 201 CMR 17.00.

See 201 CMR 17.00: Standards for The Protection of Personal Information of Residents of the Commonwealth (copy as of 2/09 available at <http://www.mass.gov/Eoca/docs/idtheft/201CMR17amended.pdf>). This doesn't really solve the problem in that no one can “ensure” anything with respect to data security, but this version creates at least a theoretical possibility for compliance.

¹⁹ *See, e.g.*, (1) Payment Card Industry (“PCI”) Data Security Standard (PCI-DSS), including “Information Supplement: Requirement 6.6 Code Reviews and Application Firewalls Clarified (Internet-facing applications)”;

(2) PCI PIN Entry Device (PED) Security Requirements; (3) the Payment Card Industry (PCI) Encrypting PIN PAD (EPP) Security Requirements; and (4) the Payment Application Data Security Standard (PA-DSS). *See also* ACH (Automated Clearinghouse) rules for direct debit and credit banking information.

²⁰ *See* 2007 Minn. Sess. Law Serv. Ch. 108 (H.F. 1758), creating Minn. Stat. § 325E.64. For a discussion of this statute, see Holly K. Towle and Raymond T. Nimmer, *The Law of Electronic Commercial Transactions* at ¶ 16.11[3][a] (2003-2009 A.S. Pratt & Sons).

²¹ *See, e.g.*, Cal. Civ. Code § 1747.09 (as amended) and AS 45.48.750(c).

²² *See, e.g.*, *In the Matter of BJ's Wholesale Club*, FTC File No. 0423160 (copy available at www.ftc.gov/opa/2005/06/bjswholesale.htm); *see also In the Matter of DSW Inc.*, File No. 052 3096 (Dec. 2005), <http://www.ftc.gov>.

gov/opa/2006/03/fyi0616.shtm; *In the Matter of Guidance Software, Inc.*, *supra*; *In the Matter of CardSystems Solutions, Inc., and Solidus Networks, Inc., Doing Business as Pay by Touch Solutions*, File No. 052 3148 (Feb. 2006), http://www.ftc.gov/opa/2006/02/cardsystems_r.shtm; *In the Matter of Goal Financial, LLC*, FTC File No. 072-3013 (2008) <http://www.ftc.gov/os/caselist/0723013/index.shtm>; *In The Matter of The TJX Companies, Inc.*, FTC File No. 072-3055, <http://www.ftc.gov/os/caselist/0723055/index.shtm>.

²³ *See, e.g.*, Cal. Civ. Code § 1798.81.5(a).

²⁴ NY McK. Gen. Bus. Law § 399-dd(1) as added by L.2006, c. 676 (“social security account number” shall include the number issued by the federal social security administration *and any number derived from such number*. Such term shall not include any number that has been encrypted”).

²⁵ ME LEGIS 568 (2004) at 4(d).

²⁶ *See In the Matter of Reed Elsevier Inc. and Seisint, Inc.*, FTC File No. 052-3094; *see generally* <http://www.ftc.gov/opa/2008/03/datasec.shtm>; Complaint at No. 10 for list of allegedly inadequate controls, <http://www.ftc.gov/os/caselist/0523094/080327complaint.pdf>. *See also In the Matter of Premier Capital Lending, Inc.*, FTC File No. 0723004 (Complaint at No. 14, <http://www.ftc.gov/os/caselist/0723004/081106pccmpt.pdf> — based on Gramm Leach Bliley Act but illustrating FTC allegations of inadequate security at customer level).

²⁷ Various regulators have issued parallel rules. For the FTC rule, *see* 16 CFR Part 681; for a discussion of the red flag rules, *see* Holly K. Towle and Raymond T. Nimmer, *The Law of Electronic Commercial Transactions* at ¶ 15.06[3][c][ii] (2003-2009 A.S. Pratt & Sons).

²⁸ *See* 16 CFR 681.2(b)(5) (FTC rule).

²⁹ *See* 2009 “Fighting Fraud with the Red Flags Rule: A How-To Guide for Business,” at 9, <http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus23.pdf>.

³⁰ *See* 16 CFR Part 681.1 (FTC rule).

³¹ For a list and discussion of data security breach statutes, *see* Holly K. Towle and Raymond T. Nimmer, *The Law of Electronic Commercial Transactions* at ¶ 16.08 (2003-2009 A.S. Pratt & Sons).

³² 2007 Mass. H.B. 4144 (NS) at § 3(b).

³³ *See, e.g.*, NC Gen. Stat. § 75-65(d) (notice must include description of the “incident in general terms”) and Hawaii and New Hampshire (same); *see also, e.g.*, Mich. S.B. 309 (notice must “describe the security breach in general terms”).

³⁴ *See, e.g.*, AS Sec. 45.48.530(2008). For a discussion of data disposal

statutes, *see* Holly K. Towle and Raymond T. Nimmer, *The Law of Electronic Commercial Transactions* at ¶ 16.12 (2003-2009 A.S. Pratt & Sons).

³⁵ *See* FCRA disposal rule at 16 CFR Part 682 (applies to “any person who maintains or otherwise possesses consumer information for a business purpose”).

³⁶ *See* IL ST CH 740 § 14/20.

³⁷ *Kehoe v. Fidelity Federal Bank & Trust*, 421 F3d 1209 (2005).

³⁸ Although studies go both ways, many conclude that insiders are a major source of identity theft. *See, e.g.*, “2008 Study on the Uncertainty of Data Breach Detection” (Oct 2008) (Compuware and Ponemon Institute: insiders were the number one cause of all data breaches with hackers ranking “a distant fifth”), http://www.compuware.com/pressroom/news/2007/7185_ENG_HTML.htm.