





PROTECTING DATA IN A BUSINESS FAILURE

Newscasters and politicians repeatedly stress that the current economic downturn is unlike any other before. It is unique because complexity in financial services has blinded executives to true risk. It is unparalleled for its impact on the savings and investments of the middle class. It is exceptional because of its depth, speed of descent and massive numbers of business failures.

This economic crisis is also exceptional for its threat to personal data. The United States is in the midst of the first severe economic meltdown of the information age – an age where data about consumers, employees, patients and borrowers is maintained on computers for companies large and small. Businesses are obligated by law to protect the personally identifiable information (PII) they retain about people. But when these companies disappear, the data remains in existence, and it is difficult to penalize corporate entities, their officers and their managers for losing or distributing the data – whether intentional or unintentional.

When a business ends, none of its managers have incentive, aside from good ethical values, to protect sensitive private information. Sometimes consumer data may be the only asset a company holds which has enough value to sell for the satisfaction of creditors. In other circumstances, employees may simply abandon a failing business, leaving its databases, printed customer lists and other sensitive information for anyone to find. Occasionally, executives and employees may grab computers and paper records from their dying business to help them as they move to their next positions. In all of these cases, personal information is most vulnerable during a time of transition and confusion. More business failures in this economic downturn means more transition and confusion.

BY THEODORE E. CLAYPOOLE
AND DANIELLE M. BENOIT

If shuttered businesses cannot be trusted to protect sensitive data on their own, then legal obligations may be the only practical incentive to secure our personal information when it is held by a failing company. During bankruptcy proceedings, company trustees may discard private contractual obligations, and are unlikely to impede the reckless actions of business executives who know that, absent broader obligations, a contracting party may only enforce its contract against the dying company that will soon pass from existence. Protective laws and regulations can create broader obligations on a company.

United States data protection law is a wide and varied collection of state statutes, federal legislation and regulations, court decisions and agency interpretations. Businesses handling sensitive, personally identifiable data may be subject to dozens of requirements in information treatment, document retention and disposal, and obligations to provide notice to data owners and government authorities upon loss of data control. The patchwork of data privacy and protection laws includes statutes on the books of at least 44 states that require certain businesses to inform data subjects, public entities and/or credit reporting agencies when personally identifiable data has been placed at risk. These laws were passed to tackle the problem of identity theft, and they address electronic and physical security breaches.

Federal laws protecting data tend to arise around especially sensitive classifications of information. Financial data, both in and out of the banking system, has been regulated for decades, including most famously in the Gramm-Leach-Bliley Act (GLB) and the Fair Credit Reporting Act (FCRA). Medical information is protected by the Health Insurance Portability and Accountability Act (HIPAA), as well as by its subsequent regulations. The Children's Online Privacy Protection Act (COPPA) legally protects data relating to children. At this writing, no omnibus federal act exists in the United States to protect all forms of personally identifiable data or make sense of the widely varying state efforts at data protection. Some of the specific aspects of these American laws are written to be enforced by and against ongoing business, and could affect businesses that are failing or have already failed. Enforcing these rules becomes much more difficult as companies cease operations.



A senior member of Womble Carlyle's intellectual property practice group in Charlotte, THEODORE F. CLAYPOOLE negotiates and prepares data management, business process outsourcing and ecommerce agreements. He is also founder and host of the WombleTech Lunch & Learn series. Claypoole holds a BA in public policy from Duke University and a JD from Ohio State University College of Law. He can be contacted at tclaypoole@wcsr.com.



DANIELLE M. BENOIT is based in Womble Carlyle's Washington, DC office, where she focuses her practice on international data protection matters and advises clients on new media privacy issues. She also maintains an active pro bono practice, representing veterans' appeals in front of the Department of Veterans Affairs. Benoit holds a BA from the University of Richmond and a JD from The Catholic University of America, Columbus School of Law. She can be contacted at dbenoit@wcsr.com.

State Laws Protecting Data Disposal

State data disposal laws require businesses to destroy sensitive customer records when they are no longer necessary for business purposes. For example, certain states have passed requirements concerning the disposition of personally identifiable data when a business has finished using it; however, it could also include when the business ends. California was the first state to adopt comprehensive regulation of data disposal, and other states soon followed with even tighter regulatory requirements. Currently, 27 states regulate the destruction of sensitive consumer information prior to disposal. While the general intent of each statute is to effectively render sensitive, PII unreadable, undecipherable and unreconstructable, a number of factors are highly varied between each statute. These variations make compliance difficult for multi-state corporations — especially when these corporations fail.

Certain types of personally identifiable information are protected and must be properly disposed of by businesses under state laws; however, what constitutes PII varies between states. Because these statutes were enacted primarily to combat identity theft, protected PII is generally defined as any information capable of being associated with a particular individual through one or more identifiers, but does not include any information generally available to the public. Protected personal data typically constitutes an individual's first or last name, or first initial and last name, in combination with any one of several data elements that can include: address, telephone number, social security number, driver's license number, bank account number, credit or debit card number, passport number and health insurance number, among others. Whether information is protected under a state's data disposal law can also hinge upon whether

such data is encrypted. For example, Hawaii and Texas do not extend data protection to information containing an individual's first name and a data element when the name or data element has been encrypted or redacted, whereas protections in Wisconsin and North Carolina do not hinge upon an extra layer of protection as the presence of a name and data element is sufficient.

Some states treat social security numbers as a specially regulated form of PII and failing companies are required to protect federally issued identification numbers. Nevada and New Jersey specifically require destruction of social security numbers alone to prevent unauthorized

disclosure, and North Carolina requires redaction of social security numbers prior to release or disposal. Five states prohibit — to varying degrees — the sale, lease, loan, trade or rental of social security numbers to third parties. North Carolina permits the sale of social security numbers when reasonable diligence is exercised. South Carolina prohibits the sale, lease or trade of social security numbers containing six or more digits, unless such sale is expressly permitted by law or in cases where the sale is for a legitimate business purpose.

In addition to variation in what PII is protected, the states widely vary on crucial issues like how the data must be destroyed, whether a formal destruction or disposal policy is required, and which types of businesses are exempt from the disposal rules. All states require entities — to varying degrees — to burn, shred, pulverize, redact, destroy, erase or otherwise modify or destroy to render data unreadable, undecipherable or unreconstructable. To this end, some states contain very broad language that permits businesses to destroy records according to commonly accepted industry practices that the business reasonably believes will ensure no unauthorized access to PII while taking into account: the sensitivity of the information, nature and size of the

business and its operations, the available technology and a cost benefit analysis. These laws tend to exclude from required compliance businesses that are under other personally identifiable data regulatory regimes like HIPAA, FCRA and GLB. A few states require businesses to have a written data destruction policy. For example, nine states require that disposal requirements are written into internal company policies. Some states even apply their rules to out-of-state residents conducting business in the state.

Certain states stretch their regulation beyond the business collecting the personal information to the businesses charged with destroying the data on behalf of third parties. New York requires all document destruction companies to register with the state. Several states require a data-collecting business to perform due diligence on third-party document destruction companies before sending PII to be destroyed. Failing businesses in these states would be required to investigate the document disposal firms that would assist in closing the business. For example, Alaska requires entities to conduct an independent audit, back ground investigation and evaluation of all third-party vendor security and privacy policies, including their document destruction procedures.



Despite the differences, some similarities are clear in these state data disposal laws. Nearly all states with applicable laws regulate the destruction of documents by private entities. Fifteen states regulate private entities only and 11 states regulate both public and private entities. Illinois is the only state that requires only public entities to destroy personal data no longer in use, so private companies in decline do not need to follow state protocols on business disposal. In addition, nearly all states require destruction of sensitive, PII, regardless of whether it is in electronic or paper form. Arizona is the only state to specifically exclude electronic documents in its statutory language. Failing Arizona businesses could dispose of their computer hard drives without fear of violating state data disposition laws.

Several state legislatures are debating the extension of existing consumer protection statutes with further data disposal legislation. Connecticut is considering legislation to require persons collecting social security numbers in the regular course of business to create a privacy protection policy. Furthermore, this legislation would require the Connecticut Department of Consumer Protection to adopt regulations prescribing best practices for data disposal. Florida legislators have proposed that all state agencies and private entities collecting personal informa-

tion must adhere to the National Institute of Standards and Technology's "Guidelines for Media Sanitization" when destroying such information, whether in electronic or paper form, and must keep a copy of these guidelines available. Missouri has proposed the most sweeping requirements thus far, applying its data disposal requirements to any business, anywhere in the world, that takes PII from Missouri residents.

Federal Data Laws and Regulation

Federal regulators also protect personally identifiable data when a business fails. For example, at the end of the technology boom in 2000, when the internet retailer Toysmart.com ceased doing business, The company's trustee in bankruptcy contemplated selling its customer list — complete with contact information — to raise money for the company's creditors. The US Federal Trade Commission (FTC) stepped in, claiming jurisdiction to regulate unfair and deceptive acts perpetrated on the public. The FTC claimed that since Toysmart.com's online privacy policy informed customers that the retailer would not sell or otherwise transfer personal information obtained from customers, that selling their personal information in bankruptcy would be unfair and decep-

When mapping out your business, it helps to use a legend.

Voted best law firm in Canada two years in a row.
2008 and 2009 *International Legal Alliance Summit & Awards*.

Business Law | Litigation | Intellectual Property | Employment and Labour Law
CANADIAN LAWYERS | MONTREAL | OTTAWA | QUEBEC | TORONTO | LONDON
OGILVY RENAULT LLP ogilvyrenault.com

OGILVY
RENAULT

tive. The FTC was able to stop the data sale. "Customer data collected under a privacy agreement should not be auctioned off to the highest bidder," said Jodie Bernstein, director of the FTC's Bureau of Consumer Protection.

The FTC has subsequently developed additional authority to address the improper sale or disposal of personal data. The Fair and Accurate Credit Transactions Act of 2003 (FACTA), which amends the long-

ACC Extras on...Data Protection

ACC Docket

- *Trust, but Verify: The Reality of Data Protection in an Information-Driven World (May 2008)*. Consumer data is everywhere and just as convenient to access, making it necessary to protect and verify this data. www.acc.com/docket
- *Edata and Discovery: Protecting Your Company from Avoidable Risk (Jan./Feb. 2007)*. This article discusses how to prepare your organization to effectively respond to an electronic data request. www.acc.com/docket
- *Defining Data Security Measures that Protect Your Company and Customers (Dec. 2007)*. Find out how to strengthen your company's current policy on data security, or find out how to get one in place. www.acc.com/docket
- *Three Crucial Questions and Answers for Protecting IP in a Deal (March 2005)*. This article explains how to assess the IP aspects of a proposed transaction; conduct and complete due diligence; and draft the provisions of the purchase agreement relating to the transfer of rights. www.acc.com/docket
- *Keeping Secrets: The Growing Challenge of Protecting Data in Outsourcing and Service Provider Arrangements (Nov. 2004)*. Here, the authors identify the most common data protection issues created by outsourcing and similar service provider arrangements, and suggest practical solutions for addressing them. www.acc.com/docket

Sample Form & Policy.

- *FAQ Data Privacy (March 2006)*. A sample of FAQ's and answers regarding data privacy of a company. www.acc.com/legalresources/forms

InfoPAKSM

- *Data Protection – A Practical Guide to Personal Data Transfer Laws in Asia/Pacific Region, Canada, Europe and the United States (Aug. 2006)*. This InfoPAK provides a general overview of the key issues US businesses need to be aware of when requesting information about individuals (whether employees of subsidiaries or in third-party databases) to be transferred from Europe or Canada into the United States. www.acc.com/infopaks

Quick Reference

- *Resources for Preventing and Assessing Information Security Incidents Checklist (Dec. 2007)*. Check out this

checklist for preventing and assessing information security incidents. www.acc.com/legalresources/quickreferences

Program Material

- *Data and Information Security: What Are the Rules and Can Technology Help with Compliance? (Oct. 2008)*. Is a data theft or breach one of your company's worst nightmares? This presentation provides a summary of the current law, a discussion of who the laws apply to and the types of data that have to be protected and a description of the technology that can be used to help compliance. www.acc.com/legalresources/resource.cfm?show=162024

Education Materials

- *The 2009 Annual Meeting*. Need more information on handling company data in the face of a closure? Join us at ACC's 2009 Annual Meeting, October 18-21 in Boston, for session 1004 Business Bankruptcy Basics for the Generalist. Plus check out the track, Meeting Economic Challenges, for additional information on managing your law department during these tough economic times. Register today at <http://am.acc.com>.

Alliance Partners

- *Trust IntraLinks for Secure Information Exchange*. For secure online workspaces, ACC Alliance partner IntraLinks offers corporate legal departments a better way to manage the exchange and storage of their company's confidential and sensitive information. ACC members receive a 20 percent discount on all new subscription contracts. Visit www.intralinks.com/accalliance for more information.

ACC's Value Challenge

- Find related resources in ACC's Value Challenge Resources webpage at www.acc.com/valuechallenge/resources and share ideas on IT practices by emailing us at accvaluechallenge@acc.com. One resource, "How to Use Technology to Strengthen Partnering," can be found at www.acc.com/legalresources/resource.cfm?show=39833.

ACC has more material on this subject on our website. Visit www.acc.com, where you can browse our resources by practice area or use our search to find documents by keyword.

standing FCRA, established additional requirements and procedures for the collection, processing and use of personally identifiable information by consumer reporting agencies, to prevent identity theft. While the FCRA and FACTA specify permissible uses of such information, require notice and disclosure of the rights and obligations of consumer reporting agencies and resellers, and set forth procedures for breach prevention and notification, these statutes did not meaningfully address the disposal and destruction of personal data by entities. So the FTC, pursuant to FACTA, adopted the “disposal rule” rule to supplement the already established FACTA consumer protections.

The FACTA disposal rule, effective June 1, 2005, governs disposition of information contained in and derived from consumer reports collected and used by businesses. The rule does not mandate specific procedures or disposal methods; rather, to protect against unauthorized access or use, the rule requires covered entities to properly dispose of consumer reports using “reasonable measures” once the records are no longer necessary for business purposes. The rule is very broad and covers any business, organization or even individuals who request a consumer report for the provision of goods or services, such as a landlord seeking to rent an apartment or a family looking to hire a nanny.


Under FACTA, covered people and businesses should be mindful of what constitutes consumer information or consumer reports, proper disposal methods and reasonable measures of disposal, as FACTA, and the subsequent disposal rule, are frustratingly ambiguous. For instance, the FTC regulations loosely define the “consumer information” to be protected, which leaves room for inclusion of data elements that are not inherently identifying, such as an email address. Furthermore, the disposal rule does not specify data destruction methods. Rather, the FTC provides a short list of approved practices, many of which are already mandated by various state data disposal statutes. Such measures include: physically destroying the document or rendering it unreadable by either pulverizing, burning, shredding or otherwise modifying the report; establishing data disposal and compliance procedures; and conducting due diligence with third party vendors used to dispose of sensitive information. Faltering companies that hold consumer information will be expected under current law to dispose of that information appropriately.

The FTC enforces its disposal rule against US companies of all types. For example, in 2008, the FTC filed a complaint against huge pharmacy retailer CVS Caremark, claiming that CVS pharmacies were throwing trash into open dumpsters that contained pill bottles

with patient names, addresses, prescribing physicians’ names, medication and dosages; medication instruction sheets with personal information; computer order information from the pharmacies, including consumers’ personal information; employment applications, including social security numbers; payroll information and credit card and insurance card information. The FTC claimed that such actions violated the disposal rule, as well as certain requirements under HIPAA. CVS Caremark signed a consent decree in this matter, paid \$2.25 million to the federal government and agreed to future compliance monitoring audits.

In 2007, the FTC reached a similar consent order for \$50,000 with a much smaller business, American United Mortgage of Illinois, based on the company’s practice of dumping loan documents with consumers’ sensitive personal and financial information in and around an unsecured dumpster. The American United Mortgage settlement requires the company to pay every two years for 10 years for professional audits of the company’s data management and disposal practices.

While current enforcement efforts and the laws in the United States protect various types of personally identifiable information from disclosure and improper destruction, they do not address the most significant practical problem faced by individual Americans whose data is held by a failing business: how to enforce the laws and other data protection obligations against the officers and managers of the faltering business. Unfortunately, without the ability to hold individuals responsible for treatment of company data, federal, state and personal enforcement efforts will fail against a corporate entity that has no money to pay fines and no ongoing operations to attach. Even with a strong infrastructure of obligation in place, obligations cannot be enforced against a company otherwise preoccupied with its very existence. Once the company is gone, personal data still remains vulnerable.

The American businesses and government are beginning to understand new implications of protecting data in the information age. Many of the state and federal rules for protecting information are relatively new, and interpretive opinions and case law have not yet been written or published. Much uncertainty still exists in the final status of US data protection law and its ultimate interpretation by regulators and courts, especially with respect to data disposal. As business failures mount, the fate of data within these faltering companies will test the current laws, and may demonstrate the need for additional protections and clarifications. 

Have a comment on this article? Email editorinchief@acc.com.