HOW TO BE A PRIVACY HERO
(AND SAVE YOUR BUSINESS OR JOB IN THE PROCESS)

PRIVACY DESK REFERENCE

Prepared and presented by

Mark McCreary | Fox Rothschild LLP | 215.299.2010 | mmccreary@foxrothschild.com

Fox Rothschild LLP
ATTORNEYS AT LAW

www.foxrothschild.com

TABLE OF CONTENTS

INTRODUCTION

Almost every business in the United States has privacy compliance issues of some sort. Most businesses have undertaken the "bare minimum" approach to protecting private information, rarely complying with the relevant laws and requirements or learning about consequences for failure to comply, which in almost all cases is not enough.

Your business collects protected, private information from employees, has access to or possession of information sensitive to your customers and vendors, and receives information from third parties through your web site or by paper correspondence. Depending on the nature of this information, you owe a duty to the owners of each type of the foregoing information to safeguard and not unreasonably disclose this information.

The purposes of this Desk Reference are to make you aware of issues that exist for your business today and may exist tomorrow, to provide steps you can take now and going forward to make compliance attainable, and to offer advice on what you should do if a problem arises. This Desk Reference should not be considered comprehensive, and any conclusions your business draws should be confirmed by knowledgeable legal counsel considering all facts and circumstances.

Like many aspects of your business, the issues and steps outlined here may only matter when and if something bad happens. Think of privacy compliance efforts as insurance: making sure that if the hacker targets you, the disgruntled employee strikes back or the overnight carrier loses your back-up tapes, you know how to respond, protect the information owners and minimize your exposure.

Be a hero to your business. Protect your business from existing and future threats, plug existing holes and make your business more valuable in the future. Familiarize yourself with this Desk Reference and keep vigilant about the requirements and risks related to privacy and your business.

WHAT INFORMATION IS PRIVATE

Whether information is private depends on the context (*e.g.*, federal or state law compliance, versus breach notification obligations) and the residence of the persons whose private information is involved (*i.e.*, an Ohio business could be subject to North Carolina laws if the latter is the residence of the individual whose personal information is at issue).

Under the Gramm-Leach-Bliley Act (GLBA) discussed herein, "nonpublic personal information" means information on applications to obtain financial services (credit card or loan applications), account histories (bank or credit card) and the fact that an individual is or was a customer. The foregoing interpretation makes names, addresses, telephone numbers, social security numbers and even other fairly innocuous data subject to the GLBA.

From the state law perspective, California law (which is widely regarded as the gold standard in privacy legislation) explicitly includes even more information: first name or initial, and last name with one or more of the following (unencrypted): social security number, driver's license number, credit card or debit card number, financial account number with information such as PIN verification codes, passwords or security codes that could gain access to the account, or medical or health insurance information.

To further complicate efforts to determine what information is covered, more than 10 states have broadened the term to include only one of the above without a name or other identifying information with it. Some states also consider passwords, biometric data, parent's legal surname prior to marriage, digital signatures and email addresses private information.

Generally, the safest approach is to treat all information about your employees and customers as protected, and disclose, safeguard and use that information only in compliance with new and revised laws going forward.

FAIR CREDIT REPORTING ACT

The Fair Credit Reporting Act (FCRA) regulates the collection and use of personal data by credit reporting agencies and their customers. Your business may use credit reports to investigate potential hires, make promotions or other permitted uses under the FCRA, and may only obtain a consumer report for legitimate business purposes or pursuant to a court order.

Before a consumer report may be obtained for employment purposes, the employer must obtain the individual's written consent in a document consisting solely of this notice. If the employee previously gave written permission, the employer need only make sure that the employee receives, or has received, a "separate document" notice that reports may be obtained during the course of his or her employment. Consumers cannot opt-out of the sharing credit report information with affiliates of the employer.

If an employer relies on a consumer report in any adverse employment decision, it must:

- Before taking the adverse action, provide a disclosure that includes copies of the individual's consumer report and the FTC's "A Summary of Your Rights Under the Fair Credit Reporting Act."
- After taking an adverse action, give the individual notice that the action has been taken in an adverse action notice, that includes:
  - the name, address and phone number of the credit reporting agency;
  - confirmation that the credit reporting agency did not make the adverse action decision and cannot give specific reasons for it; and
  - notice of the individual's right to dispute the accuracy or completeness of any information the agency furnished, and the right to a free consumer report upon request within 60 days.

The Federal Trade Commission (FTC) and other federal agencies responsible for enforcing the provisions of the FCRA are empowered to declare actions to be in violation of the applicable statute, issue cease and desist orders, and impose statutory penalties for noncompliance with agency orders.

EMPLOYEE INFORMATION

All employers collect covered information about their employees, including for application processing, credit or criminal background check procedures, drug testing, health care benefits processing, direct deposit applications and tax reporting requirements. Questions a business should consider are whether its filing cabinets are secured, if any of the foregoing information is transmitted through "inter-office" mail, and if there are any questions raised and answered in e-mail that regard or contain private information.

More employers are tracking employee Internet usage, as well as reviewing the content of its employees' email. A modern report found that approximately two-thirds of employers monitor employee Internet usage and almost half monitor employee email. Courts have fairly consistently held that employers are entitled to undertake such types of monitoring, *provided* that the employee has been put on notice of these possibilities. Unfortunately, some employers take this comfort further and review personal email accounts accessed on work computers (often by means of browser-stored User IDs and passwords) or email or text messages stored on company-owned mobile phones, PDAs and BlackBerry devices. These latter, further steps may not be permissible, and the employer is treading into dangerous territory when accessing this information.

Many employers are also discovering the convenience and practicality of payroll card accounts. These accounts are established to provide salary to employees (rather than paper checks), and are convenient for employees lacking access to traditional banking options. There are limited compliance requirements for most employers, unless the employee is part of a "payroll card" group that includes a financial institution.

GLBA COMPLIANCE AND PRIVACY NOTICES

The Gramm-Leach-Bliley Act regulates (among other things) the privacy of covered information disclosed to non-affiliated third parties by financial institutions. The GLBA also applies to non-affiliated third parties that receive covered information. A surprising number of businesses are captured in the definition of "financial institution," and *even those not included could be subject merely by the receipt of information from a "financial institution."*

The GLBA requires written or electronic notice of the categories of covered information collected, categories of people to whom the information will be disclosed, (limited) consumer opt-out rights, and confidentiality and security policies. Financial institutions must provide each consumer with a privacy notice when the consumer relationship is established and annually thereafter for the life of the relationship. The privacy notice must identify the information collected, with whom that information is shared, and how that information is used and protected. The notice must also identify the consumer's right to opt-out of the information being shared with unaffiliated parties. Should the privacy policy change at any point in time, the consumer must be notified again for acceptance.

The GLBA also requires administrative, technical and physical safeguards to maintain the security, confidentiality and integrity of the covered information. Unlike the notice requirements above, these safeguards apply to *all parties receiving the covered information*. The Safeguards Rule of the GLBA requires the development of a written information security plan that describes how the company is prepared for, and plans to continue to protect, consumer's covered information. This plan must include:

- Designating at least one employee to manage the safeguards.
- Implementing a thorough loss-risk control system on each department handling the covered information.
- Developing, monitoring and testing a program to secure the covered information.
- Plans to change and update the safeguards as needed with the changes in how information is collected, stored and used.

CLIENT AND CUSTOMER INFORMATION

Businesses collect many different types of information from their individual customers. Even those businesses that use third parties to fulfill orders often receive private information about their customers. Protecting customers' private information is no less important than protecting employee information, and protecting this information is just as often overlooked.

Your business unknowingly may have covered information. In North Carolina, an individual's name, together with an email address, could prompt a notice requirement if your network is compromised or data is improperly copied. It does not take much imagination to see how a stolen laptop or lost BlackBerry device can have absurd results for your business.

Federal and state laws also limit retention of certain types of information. The storage of credit card numbers, security codes, PIN verification codes and the contents of magnetic strips is strictly prohibited except in certain, limited circumstances with customer consent. Various states have requirements that include compliance with certain credit and debit card and social security number storage, truncation and sharing restrictions. For example, California requires most businesses to inform customers upon request with whom their information was shared in the past 12 months.

Point-of-sale software and networks are easily compromised, are rarely adequately secured and often lack controls in place to limit access to only authorized and necessary persons. Over half of all information losses occur in the restaurant industry, with the retail industry accounting for approximately one-fourth of all losses. However, no industry is immune.

The Telephone Consumer Protection Act requires businesses that use the telephone to solicit individuals to provide such individuals with the ability to prevent future telephone solicitations, must maintain and honor lists of individuals who request not to receive such solicitations for 10 years, are prohibited from making unsolicited commercial telephone calls using an artificial or pre-recorded voice without consumer consent, and unsolicited advertisements to facsimile machines are prohibited under this law.

EMPLOYEE ACCESS AND LOSS

The greatest risk of data loss is due to employees. Too often, little is done to inform employees of the types of data they should safeguard, how data should be retained and destroyed, and risky behavior they should avoid.

Often, employees will send covered information to customers by insecure email or online postings. Employees traveling with laptops often access the Internet through insecure wireless points, exposing data on the laptop and creating the opportunity for unauthorized acts from the laptop (or simply lose the laptop).

Employers are often as much to blame as the employee for these risky behaviors. It is common for employees to engage in the following unacceptable practices: using commercial email (*e.g.*, GMail) for work-related email because of poor email systems at work; posting files online because of email attachment size limitations; forwarding all work email to a commercial account because of an email retention policy; using PDAs for email or file storage without remote device "wiping" capability and password protection enabled; using peer-to-peer file sharing services ripe with viruses and malware; and copying sensitive information to unprotected, portable (easily lost) "thumb" drives.

More recently, the significant risks associated with foreign travel with laptops and PDAs have gained attention. It may come as a surprise that Customs and Border Protection does not need reasonable suspicion to inspect and confiscate laptops, PDAs and storage media. Reports are surfacing of these devices either never being returned, or being returned damaged, tampered and (certainly) accessed by unknown persons.

If you suspect that an employee (or third party) has engaged in any wrongdoing regarding your business's covered information, you should approach the situation carefully, avoiding any false accusations. An employee's or a contractor's right to network and facility access must be cut-off immediately upon termination of employment, if not shortly before.

EXTERNAL THREATS

Your business must be concerned with attacks from the outside. Almost all external attacks can be stopped with vigilance and dedication to the protection efforts. Having a firewall typically should not be the end of your vigilance, and redundant firewalls where particularly sensitive information is stored is prudent. Often information technology administrators will keep network ports open, leaving potential points of entry unnecessarily open. It is also often the case that the default passwords on firewalls (among other things) are left unchanged.

Wireless networks are also a continuing source of exposure. A common problem is the failure to engage any sort of security on the wireless network, or failure to employ strong security on the wireless network. Ideally, your wireless network is provided only as a courtesy to your visiting customers and does not broadcast itself. If you must have wireless access at your place of business, then only a cloaked, strongly named network with the strongest encryption available should be used.

Your business should have deployed a strong password policy for all employees that requires combinations of numbers, letters and symbols of several characters in length and not containing English words. Passwords should be changed no less often than every 90 days.

Wireless payment scanners also have been shown to be insecure in many deployments, allowing a person nearby to intercept the data being transmitted. Along the same lines, the use of current technology RFID has raised serious concerns in all industries, despite its ongoing rollout.

What cannot be lost in this discussion is the protection of information contained in paper form. Access to this information must be secured against threats from visitors to your business, including cleaning staff, security guards and former employees that still have access. Does your business have a shredding policy for sensitive documents, or do you engage an outside service to destroy these documents?

DATA SHARING WITH AFFILIATES AND THIRD PARTIES

Generally speaking, there are very few, if any, restrictions on your business sharing covered information with your affiliates. As a matter of best practices, financial information should be excluded from this sharing unless absolutely necessary.

If your business's privacy policy permits the sharing of covered information with third parties (not including financial information), there are limited restrictions on use of that information.

It is common for companies to sell or lease customer information to third parties for marketing to your customers. These arrangements can be very lucrative for your company, and are perfectly permissible as long as the proper disclosures are made to your customers and the information shared is not covered by law prohibiting such sharing.

Opt-out requests received after the information is originally provided by the customer can create issues if that information has been previously disclosed to third parties. Ideally, any agreements with third parties with whom information is shared will have a "claw-back" provision, requiring those third parties to honor subsequent opt-out requests from your customers.

Additionally, any agreements with third parties should have explicit requirements that those third parties are not permitted to further distribute the shared information. Failure to abide by these restrictions should be coupled with meaningful economic consequences for those third parties.

Unfortunately, however, often this shared information is in "the wild," and you will have little control over it. This fact alone may be reason enough for your business to decide not to share covered information with third parties that do not have a need-to-know.

WEB SITE ISSUES AND PRIVACY POLICIES

By now, many businesses have established an Internet presence through a corporate web site. In the rush to get online, many businesses that have no need to have a web site have jumped into the mix without thinking of the implications.

Every web site that collects information from users should have a privacy policy. A privacy policy will inform the visitor why information is collected, how the information will be used, with whom the information will be shared (if anyone) and how the visitor can opt-out of that sharing (if applicable). Some states require a clearly written privacy policy with the foregoing information (among other things) if information is collected from a resident of that state. Even if your business is collecting information only for the purpose of contacting that person, a privacy policy should be in place.

Those businesses that maintain user accounts have several other issues to consider. Businesses should have in place clear terms and conditions that explain the rights of the user and, importantly, the things for which the business is not responsible (information from third parties, misappropriation of login credentials, disclaimer of warranties, etc.). The web site should require strong User ID and password procedures, warn users when they are moving between secure and insecure web sites (maintain the "Chain of Trust"), not permit secure login on insecure web sites, not engage in emailing secure information (*e.g.*, lost passwords), and use SSL connections and encryption.

Web sites that utilize bulletin boards or comment sections also have specialized issues that arise. Prior case law has made it clear that the web site owner has the right to edit and monitor the contents of those items without assuming a heightened duty or (generally speaking) liability for those edits.

There has also been recent discussion from other countries that a visitor's IP address (the set of numbers that identifies the user's computer) may be covered information. While this issue is not decided, you should be mindful of these developments if you have foreign visitors to your web site, or if you record IP addresses of visitors.

The Children's Online Privacy Protection Act generally requires a web site directed at children under 13 years of age to obtain "verifiable parental consent" before collecting personal information online from children. The COPPA regulation defines the term "collects" to encompass providing a child with the ability to have an email account or the ability to post to a chat room, bulletin board or other online forum. COPPA also requires a covered web site to disclose in a notice its online information collection and use practices with respect to children, and provide parents with the opportunity to review the personal information collected online about their children. Unless absolutely necessary, the best approach is to state a policy of prohibiting use of the web site by children under 13 years of age and verify age at the time of creating an account or sending correspondence.

Fact:
The Ponemon Institute issued a report reviewing data breaches by 43 companies involving up to 113,000 records. The costs to handle these breaches ranged from $613,000 to nearly $32 million, with an average of $6.6 million.

PRIVACY POLICIES: CONSISTENCY FOR ONLINE/OFFLINE DATA

If your business uses information collected offline to market to its customers, you still may have to meet many of the online data collection requirements and standards. Until recently, businesses (other than financial institutions) enjoyed a fairly unregulated space when it came to offline data collection. However, the FTC threw that comfortable zone into flux when its agents announced that the stated privacy policies of businesses would be assumed to apply to information collected offline as well. In other words, if a business has an online privacy policy that pledges not to share any covered information to third parties for marketing purposes, the FTC would view this as applying to information collected offline as well and prohibit sharing of information collected offline.

It would appear simple enough to merely adjust your business's online privacy policy to not restrict sharing of covered information with third parties, but your business may only be permitted to apply that policy on a going forward basis. In other word, many experts believe that adjustments to privacy policies to the customers' detriment would not be effective for information already collected, at least not unless further notice was provided to the consumer to disclose the change in policy and permit an opt-out opportunity. The appropriate analysis must be undertaken on a case-by-case basis, and this issue should be on your mind if you make material changes to your privacy policy. Ideally, your business will adopt both an online information privacy policy and an offline privacy policy.

Along the same lines, problems arise with businesses that "mix" online and offline collected information. Your business should always be in a position to demonstrate how and where information was obtained in case of a dispute. There is no obligation to have identical online and offline privacy policies.

RESPONSE IN EVENT OF BREACH

If the unthinkable happens, no matter what your efforts to prevent it, your business needs to be prepared to deal with an improper disclosure. The following are the top 10 things your business should know about breaches:

1) Timely notification to those persons affected is crucial. While there is no magic number of days that your business may wait (although some statutes do set time periods), each passing day increases the risk of improper data use.
2) Having a breach notification plan in place will assist you with a timely and complete notification, and the plan also may help your company in any litigation or regulatory action that may follow.
3) Currently, there is no comprehensive federal breach notification law other than a recently passed (Obama Administration) notification requirement dealing with medical information, but currently 44 states, D.C. and Puerto Rico have breach notification requirements. Some states permit private rights of action.
4) Recovery is generally denied for speculative losses, but your company may be responsible for individuals' actual costs incurred.
5) The method of notice must be appropriate for the individual's state of residence and include any language required by that state. A breach, no matter the size, requires a state-by-state analysis and notification to all appropriate agencies.
6) Contracts with third parties can control the parties' liability, so that your service provider must indemnify and defend you for losses.
7) Losses can be caused by a third-party carrier, who may offer special services or reimbursement rights if there is a loss.
8) Your business may be covered under existing insurance policies, and your business should now consider purchasing coverage.
9) Federal or state agency involvement may open unwarranted investigations in unrelated matters.
10) Generally liability will rest where the breach occurs, but can be contractually altered. (Regardless, every party that potentially has liability tends to get brought into the litigation.)

Depending on your industry, you may have been through a SAS70 (or equivalent) review of your data collection, retention and securitization. These reports will analyze your computer network, storage practices and access implementations, and they will also include recommended corrections and fixes appropriate for your industry. The GLBA also has accompanying published safeguards and best practices for the financial industry. While these safeguards and best practices may not be required for your business, they are certainly a great first step in your review of what can and should be done to improve your business's practices.

If one is not already in place, your business should have a written data retention policy that is followed and practiced. Not only will this limit potential exposure for your business in the event of a breach, but also may be beneficial if you find your business involved in unwanted litigation. The topic of document retention standards for various types of data is too broad for this Desk Reference, but you should be aware that almost every category of information has different retention requirements (both legally and from a best practices point-of-view), and data covered includes both paper and electronic formats (*e.g.*, saving email)

As discussed earlier, controlling your employees' access to information and your computer network and hardware is crucial. Your business should have policies (or technological "blocks") in place to prevent installation of unwanted computer programs by employees, physically block certain web sites (or all web sites that are not work related), prevent email forwarding rules, block peer-to-peer traffic, and install and maintain up-to-date virus and malware prevention software.

The Fair and Accurate Credit Transaction Act of 2003 (FACTA) added new sections to the FCRA, intended primarily to help consumers fight the growing crime of identity theft. Businesses that use consumer reports,

must adopt a plan to detect, prevent and mitigate identity theft. The plan must be approved by the company's board of directors or senior management. The rules identify certain indicators of actual or attempted identity theft, but each company is left to establish plans based upon a risk assessment of its own operations. Indicators identified by the agencies as warranting increased scrutiny include:

- Consumer's notation on a credit report such as a fraud alert, active duty alert or credit freeze
- Unusual patterns in the consumer's use of credit, such as a recent increase in inquiries or new credit accounts, changes in the use of credit or accounts closed
- Suspicious documents that appear to be alerted, forged or reassembled, or documents that include information that is inconsistent with the person applying for credit
- Suspicious social security numbers, for example one that has not been issued or is listed on the Social Security Administration's Death Master File
- Suspicious address or phone number
- Use of an account that has been inactive for a "reasonably lengthy period of time"
- Mail sent to the account holder is returned while transactions continue
- Notice from the account holder or law enforcement that identity theft has occurred

FACTA also requires that credit card expiration dates not be printed, which includes "printing" on electronic receipts.

Fact:
The nonprofit Identity Theft Resource Center® reports that 656 data breaches were reported in 2008, up from 446 in 2007. This includes only those breaches reported by businesses.

CREDIT CARD ACCEPTANCE AND INFORMATION STORAGE

The Payment Card Industry Data Security Standard (PCI DSS) was developed by major credit card companies like MasterCard® and Visa to ensure consumer confidence when using credit cards. The PCI DSS applies to all merchants, financial institutions, service providers and others that use, store, process or transmit payment cardholder data. The foregoing parties must take due care and diligence to prevent credit card fraud, identity theft and hacking. The standard has 12 requirements designed to ensure the confidentiality and integrity of customer information.

Overall compliance with PCI DSS is very low, setting the stage for those non-complying businesses to face uphill battles in the event of a breach, and serious consequences from the major credit card companies and merchant processors for failing to comply. Most of these requirements are routine components of any information security program that are (or should) already be in place in any organization that handles sensitive information.

Build and maintain a secure network

1. Install and maintain a firewall configuration to protect data.
2. Do not use vendor defaults for passwords and other security.

Protect cardholder data

3. Protect stored data. Storage of cardholder data must be kept to a minimum time with data storage and retention policies. Authentication data, such as magnetic strip or chip data, validation codes, or PIN verification values, must not be stored *at all* subsequent to authorization. Cardholder data must be rendered unreadable, encrypted, anywhere it is stored.
4. Encrypt cardholder and sensitive data across public networks.

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software or programs.
6. Develop and maintain secure systems and applications.

Implement Strong Access Control Measures

7. Restrict access to data by business need-to-know. User-level controls must restrict individuals' access to only data required for their work.
8. Assign a unique ID to each person with computer access. User-IDs must be authenticated with at least one factor (passwords, tokens or biometrics). Remote access should employ two-factor authentication.
9. Restrict physical access to cardholder data. Facility entry controls must limit and monitor physical access to areas containing systems that store, process or transmit sensitive data. Media backups must also be kept in controlled locations.

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data. Audit trail (activity logging) mechanisms must be available to record critical system events and link all events to an individual user (without the possibility of being altered). Audit trail data must be reviewed daily, and retained "for a period that is consistent with effective use, as well as legal regulations" (i.e., a minimum of three months).
11. Regularly test security systems and processes.

Maintain an Information Security Policy

12. Maintain a policy that addresses information security for employees and contractors. Organizations must "establish, publish, maintain and disseminate" a formal security policy that meets all the PCI DSS requirements. An annual risk assessment and policy review/update is required. Operational security procedures consistent with the policy must be put in place. A security incident response plan must be established, documented and periodically tested.

E-MAIL MARKETING ISSUES

Privacy laws affect your business's email marketing efforts, including laws dealing specifically with email marketing. The most significant "email" law is the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act. CAN-SPAM contains, among other things, the following:

- **Bans false or misleading header information**. The "From," "To" and routing information in the email, including the originating domain name and email address, must be accurate.
- **Prohibits deceptive subject lines**. The email subject cannot mislead the recipient about the contents or subject matter.
- **Requires that email contain an opt-out method**. The email must contain a return email address or another Internet-based email method that allows the recipient to unsubscribe from future mailings. All opt-out mechanisms must be capable of accepting opt-out requests for at least 30 days after the email is sent. Once an opt-out request is received, your business must stop sending email to that email address within 10 business days. It is illegal to sell or transfer the email addresses of people who have opted-out.
- **Requires that commercial email be identified as an advertisement and include the sender's valid physical postal address**. The email must contain clear and conspicuous notice that the message is an advertisement or solicitation, that the recipient can opt out of receiving commercial email from your business, and your business' valid physical postal address.

Your business must make sure its email marketing is consistent with your privacy policy. Likewise, your privacy policy should not state that it applies to affiliates if the companies have different information sharing practices.

Email addresses purchased from third parties can be very risky for your business. Unless your business purchases the list from a reputable party, you cannot be assured that the information was obtained in a permissible manner. Third-party email service providers that supply email addresses should undertake liability for non-compliance with privacy laws.

ASSET SALE AND BANKRUPTCY CONSIDERATIONS

Businesses commonly overlook how privacy policies and practices affect the purchase and sale of businesses. Whatever representations were made to customers when that information was collected stay with that data, no matter who possesses the data.

Assets that your business may acquire from time to time will most likely include customer information. You can imagine your disappointment if you are restricted in how you can use that information, or even worse, your unwitting, improper use of that information puts your business in the crosshairs of federal or state agencies (or even private actions).

When it comes to the sale of your business, savvy purchasers will require representations regarding the source, integrity and usability of customer information being purchased from the business, and possibly from the shareholders, resulting in potential personal liability for misrepresentations, possibly even inadvertent misrepresentations.

Avoiding these messy scenarios is possible with thorough planning and protections in advance and at the time of the acquisition.

Another risky scenario can be the purchase or licensing of customer information from bankruptcy debtors. Typically, bankruptcy transactions come with few or no representations regarding the customer information acquired. This is not always because of the nature of the bankruptcy, but because principals of the debtor are not available, records are scattered or unavailable, and trustees tend to avoid unverified representations.

Before you make use of any assets that include customer information that are purchased or licensed through bankruptcy proceedings, you must be fully aware of the risks involved and the possibility that your use of such customer information may be limited to your internal business needs.

The European Union Directive (the Directive) is a wide-ranging law that affects more and more United States businesses. Article 3 of the Directive reads in part: "[t]his Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system."

Personal data is a broad phrase, covering any information relating to an identified or identifiable natural person. One of the key requirements of the Directive is that personal data can only leave the European Union under certain conditions, notably where the receiving country has adequate privacy protections. It has long been unclear whether and when the United States and other countries have such adequate protections, and thus it has been potentially unlawful to transfer personal data to the U.S.

Not only does the Directive apply to the electronic receipt and transmission of personal data from European Union citizens, but also appears to cover the transfer of personal data by business travelers carrying laptops containing personal data from the European Union to the United States. Arguably, business travelers are required to give notice to each name and address in their laptop or PDA before leaving the European Union, and register the laptop with European Union countries that require registration of databases.

The Directive has also caused problems in civil litigation, pitting the Directive's prohibitions on disclosure against the broad discovery disclosure requirements of the United States' Federal Rules of Civil Procedure.

Consent by individuals covered by the Directive may overcome this quagmire, but such consent must be prospective and unambiguous.

STATE PRIVACY LAWS

Information protected by state laws varies widely, as do the notification obligations and liabilities in the event of an improper disclosure. For example, a court in California held that consumers have the right to opt-out of the sharing non-consumer report information between affiliates, which is contrary to the federal laws FCRA and GLBA. A business may be subjected to several state laws if it collects covered information from customers or employees in multiple states.

Most states also have common law (case law, not statutory, rights) theories of invasion of privacy (a disclosure where the consumer has a reasonable expectation of privacy), public disclosure of private information, defamation or libel (disclosures of inaccurate personal information), and breach of a duty of confidentiality.

Computer crime statutes in many states (as well as federal law) prohibit the tampering with computers or accessing certain computerized records without authorization. These statutes can apply to unauthorized access from both personal *and* work computers.

Fact:
With more businesses and individuals posting data to the "cloud," the risks of exposing or losing that data increase dramatically. Google recently notified some users that their documents had been inadvertently shared with more persons than those given permission. What if these documents included trade secrets, employees' personal information or competitive analyses? Unfortunately, few are taking the necessary time to assess, understand and take preventative action.

About the Author:

Mark McCreary is a partner in the firm's Corporate Department. His practice focuses on Privacy, Licensing, Intellectual Property and Internet law. Mark may be reached at (215) 299-2010, or email him at mmccreary@foxrothschild.com.

Fox Rothschild LLP
ATTORNEYS AT LAW
www.foxrothschild.com