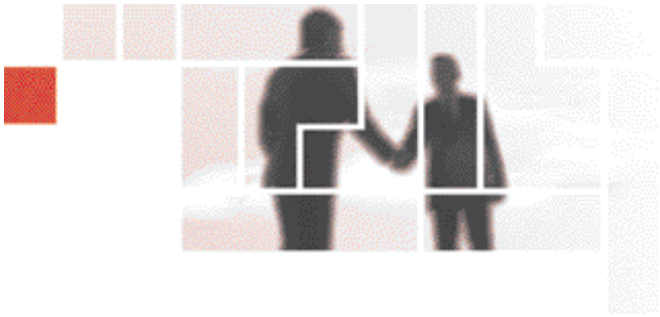


SAI GLOBAL WHITEPAPER

MEETING THE PRIVACY CHALLENGES IN BUSINESS
THE CURRENT PRIVACY LANDSCAPE: PART 1 OF 2

Rebecca Herold, CIPP, CISSP, CISA, CISM, FLMI

Privacy Threats and Responsibilities are Increasing

Never before has there been more concern about privacy than there is right now. And these concerns will only continue to increase – and justifiably so, considering how quickly personal data proliferates.

Consider **the amount of personal information in circulation.** A May, 2009 IDC study reported[1] that 487bn gigabytes (GB) of data exists in the world; if "printed and bound into books, it would form a stack that would stretch from Earth to Pluto 10 times." If this is not amazing enough, then consider that this amount is expected to double in less than one year (i.e. by November, 2010).

The number of ways that **personal information can be collected** compounds the problem. Not only can information be collected and stored in hard copy, but electronic options have multiplied. The same IDC study reported that 70% of data is created by individuals and stored as phone data, e-mails, photos, online transaction data and within many different social networking sites, such as Facebook, MySpace, LinkedIn and Twitter[2]. We are now literally surrounded by these and other endless types of digital recorders.

And now consider the different ways in which **personal information can be stored, processed and shared**. The technologies that brought us smart phones and computers have evolved and expanded to cover a wide variety of digital storage devices so unique and commonplace that one often can't discern the true functionality, i.e. the ability to store and retrieve personal information. When a pen is actually a storage device (see *Figure 1: Examples of USB Storage Devices*, page 2), it's difficult to imagine how to manage the data that people can carry into and out of your organization on a daily basis without anyone else even having a clue about all that data flow.

We've never before been so constantly connected to the outside world, even when within the confines of our employers' facilities. And studies indicate that we expect to access the outside world at all times, no matter where we're located. We want the ability to access personal cell phones, personal e-mail, and our social network sites 24 x 7. Understandably, businesses are concerned about the issue of employee productivity during all this Web 2.0 activity. In a July, 2009 study, Nucleus Research reported that companies allowing access to Facebook:

1. Lose an average of 1.5% in total employee productivity
2. Have 77% of those with a Facebook account access that site during work hours
3. See some employees use Facebook as much as 2 hours per day while at work
4. Serve as the exclusive access to Facebook by one in 33 employees (3%)

Figure 1: Examples of USB Storage Devices

		
A Pen	A Ring	A Battery

Pen: http://www.diytrade.com/china/4/products/5263887/usb_pen_drive_with_digital_wireless_voice_recorder.html

Ring: http://www.theweddingringblog.com/2008/03/article-the-usb.html

Battery: http://blogs.guardian.co.uk/technology/archives/images/usb_batts.jpg

Employee productivity is one issue, however, concerns for information security, privacy and compliance infractions also exist. Employees are increasingly using Web 2.0 sites to post information about their work and their business customers. Consider just a few of the stories that are hitting the news detailing how Web 2.0 use is leaking sensitive information and personal information (see *Figure 2: Stories in the News*, page 3).

Not only are these types of incidents embarrassing for and damaging to the reputations of companies, but regulators are taking notice.

Government oversight agencies are increasingly scrutinizing employee complaints on blogs and social networking sites and using that information as a gauge of an organization's business health. Both the Securities and Exchange Commission (SEC) and Federal Trade Commission (FTC) have expressed concern about the ways in which Web 2.0 use has led to privacy breaches. And bank regulators are concerned with unfair and deceptive advertising and marketing practices.

Privacy is a Global Concern

Privacy as a global concern was demonstrated during the first week in November, 2009 when privacy experts from 50 countries created draft international standards for the protection of privacy and personal data during the 31st International Conference of Data Protection and Privacy. If the standard is adopted, the collection and processing of personal information will only be possible after obtaining the "free, unambiguous and informed consent" of the associated individuals (i.e. the data subjects). Further, the data would need to be deleted when it is no longer necessary. The standards also largely cover the other principles found within the long-standing OECD privacy principles[3], around which most of the existing data protection laws throughout the world are based.

In many parts of the world, privacy is considered a basic human right. As the EU Data Protection Directive (95/46/EC)[4] states, privacy safeguards are "for the protection of the private lives and basic freedoms and rights of individuals." However, it has only been in the past few years that organizations have really started to noticeably address privacy challenges and dedicate the resources necessary to effectively deal with the myriad of privacy issues and requirements. Now that the public is also becoming much more privacy savvy, organizations need to address privacy not only because it is legally required and the right thing to do, but also because it is necessary for keeping customer trust, maintaining customer loyalty and support, and improving the corporate brand.

While organizations are starting to address some privacy issues, there are still significant privacy problems that more and more organizations fall victim to. This is typically because they have simply not recognized certain common vulnerabilities and the complexitites of a growing number of privacy regulations worldwide.

Not only does privacy encompass how business is conducted and the communications made with customers, consumers, business partners, and employees, but it also involves the technology that enables secure business processes. All facets and levels of an organization are affected in a comprehensive privacy program, including business operations, websites and services, back-end systems and databases, outsourced processing, communications with third parties, customers and service providers, and legacy systems. An effective privacy program will not only make your employees and customers happier and maintain their trust, but it will also mitigate your exposure to regulatory noncompliance, lawsuits, bad publicity and government investigations.

How Much is Personal Information Worth?

In today's information economy, personal data is as valuable as currency. The ability to collect, process, analyze and transfer as much personal data as

Figure 2: Stories in the News

- **Februrary, 2009:** Someone from a Wisconsin medical center made an anonymous call to the sheriff to report that a nurse had taken photos of a patient with her cell phone and posted the photos to her Facebook page. Investigation revealed that two nurses each took a photo of an x-ray of a patient that was admitted to the emergency room with "an object lodged in his rectum." The two nurses who took photos were fired. The medical center's reputation was, of course, negatively affected.
- **June, 2009:** A New Jersey federal jury ruled that the managers of a Houston's restaurant in NJ violated the Stored Communications Act and the New Jersey Wire Tapping & Electronic Surveillance Act by intentionally accessing a MySpace page that employees used without authorization, and then firing two employees for derogatory remarks about the management made in MySpace. The restaurant was ordered to pay compensatory and punitive damages for maliciously and without authorization invading a password-protected, invitation-only employee gripe group on MySpace.
- **June, 2009:** City government officials in a Montana town notoriously made the news worldwide for requiring job applicants to provide their IDs and passwords for any online social networking type of site they participate in. Bozeman, MT quickly became the Big Brother mascot for privacy over-zealousness worldwide. Soon after the story broke Bozeman discontinued this practice.
- **August, 2009:** The United State Marine Corps banned the use of Web 2.0 site from and within its networks for security measures and to keep military secrets from leaking out.
- **November, 2009:** It was widely reported that over 1,000 e-mails and several thousand documents from the University of East Anglia's Climatic Research Unit (CRU) in the UK were posted online, first to a Russian FTP site but then quickly copied to many other social media sites throughout the world.

possible is big business. This is not just conjecture; it is a topic that has been greatly analyzed and scrutinized by marketers in every organization concerned about revenue growth. It's clear that organizations require the personal information of consumers in order to conduct business.

But personal information is not just the core of big business for legitimate organizations, it is also irresistibly lucrative for organized criminals. And criminals are finding more and more ways to get their hands on personal information. Consider just one way - through cleverly evolving malware. Malware is increasingly being disguised as security software that lures and tricks victims into clicking on bogus links that take them to sites that contain their credit card numbers and other personal information. Some schemes don't even try to be tricky; personal information is directly requested. The crooks gathering all this personal information then sell it, often hundreds or even thousands of times over. The amount of cash generated by these schemes in a short period of time is staggering when criminals are willing to pay as much as $30 per card[5].

Despite the significant value of personal information, it is rather shocking to see how many organizations provide no or inadequate safeguards to protect personal information. This claim is supported by a recently published Ponemon Institute study[6] that reveals **over half of businesses do not secure personal information**. Some of the more specific findings include:

- 71% do not make data security a top initiative
- 79% have experienced one or more data breaches
- 52% indicated they are not proactive in managing privacy or security risks

It certainly appears that most organizations either don't understand the value of the information itself and the impact that breaches have on an organization, or are unwilling to appropriately safeguard personal information.

A quick look on one of the many breach tracking sites (see *Figure 3: Some of the Sites Listing Data Breaches*) clearly indicates that both the number of breaches and the number of cases of credit card fraud have actually risen year after year despite the enactment of the PCI DSS standard in 2005 as part of an effort to stem the tide of breaches.

Figure 3: Some of the Sites Listing Data Breaches

- http://www.privacyrights.org/ar/ChronDataBreaches.htm
- http://www.datalossdb.org
- http://www.Pogowasright.org

The value of personal information is so high that crooks and insiders are motivated to do just about anything – legal or not - to get their hands on this digital gold. For example, in late 2009 in the U.K., an employee of wireless service provider T-Mobile sold millions of customer database records to data brokers; the biggest breach ever seen in the U.K.

What is "Personal Information"?

What about the fully 50% of organizations surveyed in the Ponemon study that don't safeguard information? Could it be that they don't do so because they don't understand or properly identify "personal information"?

Most businesses handle a huge amount of information about customers, employees, business partners and consumers, and often they view the information they collect and process as being "their" information. Or, they purchase customer lists from marketing vendors and they view those lists as being their own business property.

Business managers need to understand that personal information is, very simply, information that reveals something about specific individuals or groups of individuals. Further, there is not one universal definition of personal information. The definitions applied around the world in different laws and regulations vary greatly. In fact, the definitions vary greatly within the many data protection laws that exist within a single country.

Figure 4 (*Identifying Personal Information,* page 6) represents the various types of personal information covered in a wide range of laws and regulations. Because laws are constantly changing, the information noted here may also change. The ultimate goal of this table is to help you see the wide range of items that are considered "personal information" of some type within various laws and regulations.

Not only do the data protection laws throughout the world differ greatly in the definition of personal information, but the attitudes and views about privacy - and really what privacy means - also vary greatly. While all individuals throughout the world are concerned about privacy, the specific privacy issues of concern differ from continent to continent and from country to country. Let's compare and contrast the attitudes between six different countries.

- U.S.: According to a study released in September, 2009, 66% of U.S. adults do not want marketers to tailor advertisements to their interests.[7] However, individuals who use social media and other "Web 2.0" sites tend to be more nuanced about how they, themselves, view privacy. As a May, 2009 study[8] reported, individuals using social media sites perceive that they are safe, friendly environments and tend to trust the others participating in the same sites.
- Japan: A 2004 research study[9] reveals that Japanese are more risk averse and more concerned about their privacy and online payment security than US citizens.
- India: A 2009 University of California (Irvine) report[10] indicated that workers in India have greater privacy concerns than those in the U.S. For example, workers in India more often want to have privacy management tools available.
- Australia: A 2007 study[11] revealed that an increasing proportion of Australians are willing to provide a wide range of personal information to organizations, but also that a larger proportion do not want to receive unsolicited marketing information and are more concerned about providing information over the Internet.
- Israel: The Israeli desire for national security results in a greater acceptance of government monitoring, but there is still concern about personal freedoms. Furthermore, there is concern about privacy invasive and surveillance technologies as well as the current government consideration to create a biometric registry including fingerprints and digital photographs.[12]
- U.K.: A Ponemon study reported six out of 10 employees in the UK stole data when they left their job in 2008.[13]

To maximize their success, business leaders must be aware of the privacy attitudes of both employees and consumers in all countries in which they operate or market.

Figure 4: Identifying Personal Information[8]

Personal Information Item	HIPAA	COPPA	CA	GLBA	EU	Priv Act	Drivers	FOIA	PIPEDA	Misc
1. First Name or Initial	♦	♦	♦	♦	♦	♦	♦	♦	♦[16]	♦
2. Last Name	♦	♦	♦	♦	♦	♦	♦	♦	♦[15]	♦
3. Geographic subdivisions smaller than a state (mailing address)	♦	♦		♦	♦	♦	♦[17]	♦	♦[15]	♦
4. Dates (excluding year for HIPAA) of:	♦				♦	♦		♦		♦
• Birth	♦	♦			♦	♦		♦	♦	♦
• Admission	♦							♦	♦	♦
• Discharge	♦							♦	♦	♦
• Death	♦					♦		♦	♦	♦
5. Telephone number	♦	♦		♦	♦	♦	♦	♦	♦[18]	♦
6. Fax number	♦	♦[16]		♦	♦	♦		♦	♦[16]	♦
7. E-mail address	♦	♦		♦	♦	♦		♦	♦[16]	♦
8. US Social Security number	♦	♦	♦	♦	♦	♦	♦	♦		♦
9. Medical Records numbers	♦		♦		♦	♦	♦	♦	♦	♦
10. Health Plan beneficiary numbers	♦		♦		♦	♦		♦	♦	♦
11. Account numbers	♦				♦	♦		♦		♦
12. License and Certificate numbers	♦				♦	♦	♦	♦		♦
13. Vehicle identifiers (such as license plate number)	♦		♦		♦	♦	♦	♦		♦
14. Credit Card number			♦		♦	♦		♦		♦
15. Debit Card number			♦		♦	♦		♦		♦
16. California ID number			♦			♦		♦		♦
17. Device Identifiers (such as serial numbers)	♦				♦					♦
18. URLs (Internet Web Universal Resource Locators)	♦				♦					♦
19. Internet Protocol (IP) address	♦				♦					♦
20. Full-face photographic images (and any comparable images)	♦				♦	♦	♦	♦	♦	♦
21. Other uniuqe identifiers that can be attributed to a specific individual	♦				♦	♦		♦	♦	♦
22. Medical care info, such as organ donations, medications, disability info, etc.	♦					♦	♦	♦	♦	♦
23. Any other identifier that the FTC determines permits the physical or online contacting of a specific individual		♦				♦				♦

Personal Information Item	HIPAA	COPPA	CA	GLBA	EU	Priv Act	Drivers	FOIA	PIPEDA	Misc
24. Information concerning the child or the parents of that child that a Web site collects online from the child and combines with one of the above identifiers		♦								♦
25. Biometric identifiers (such as DNA, finger, iris and voice prints)	♦				♦	♦	♦	♦		♦
26. Body identifier (tattoos, scars, etc.)					♦	♦[16]		♦		♦
27. Employment History				♦		♦		♦		♦
28. Income				♦		♦		♦		♦
29. Payment History				♦		♦				♦
30. Loan or Deposit balances				♦		♦				♦
31. Credit Card purchases				♦		♦				♦
32. Criminal charges and convictions and court records				♦	♦	♦				♦
33. Military history					♦	♦				♦
34. Credit Reports and Credit Scores				♦		♦				♦
35. Existence of Customer Relationship				♦		♦				
36. Financial Transaction information				♦		♦				♦
37. Merchandise and Product Order History				♦[16]		♦				♦
38. Service Subscription History										♦
39. Fraud Alerts				♦		♦				♦
40. "Black Box" Data										♦
41. Video Programming activity information										♦
42. Voting History					♦	♦				♦
43. Conversations (recorded or overheard)					♦	♦			♦[16]	♦
44. Descriptive listings of consumers									♦	♦
45. Education Records						♦		♦		♦
46. Personnel Files								♦		♦

Legend:
HIPAA: Health Insurance Portability and Accountability Act
COPPA: Children's Online Privacy Protection Act
CA: California SB 1386 + AB 1298
GLBA: Gramm Leach Bliley Act
EU: EU Data Protection Directive[14]
Priv Act: The Privacy Act of 1974 (amended)
Drivers: Drivers Privacy Protection Act
FIOA: Freedom of Information Act
PIPEDA: Canada's PIPEDA
Misc: Miscellaneous other laws

Often, combinations of more than one piece of information create personal information. The following, typically when combined with an element from the previous list, are also considered as personal information. Additionally, these are often referenced as "sensitive", "protected" or "confidential" information.
1. Racial or ethnic origin
2. Political opinions
3. Religious or philosophical beliefs
4. Trade union membership
5. Health or sexual activity information
6. Marital status
7. Security code
8. Access code
9. Password

Note: This does not represent legal counsel or legal interpretation. This is provided as a guide to help information security, privacy and compliance professionals to start identifying the many types of personal information referenced within multiple laws that are considered as personal information. Each organization should use this as a starting point to confirm the interpretations as presented here.

Why Should Business Leaders Be Concerned About Privacy?

Why is privacy a general business concern and not just an IT or legal concern? First, there are increasing numbers of laws, regulations and industry standards that can bring business to a complete standstill if they're not properly addressed. Second, there are an increasing number of threats that challenge businesses every day and prompt them to ensure that appropriate safeguards to preserve business, customer and employee privacy are implemented. Some of these include identity theft, new technology weaknesses, disgruntled employees, information thieves, carelessness, mistakes, lack of training, and criminal activity. Effective business leaders should understand that these are significant and important issues, and that their organizations need to have appropriate policies, procedures, technologies and other practices in place to address the associated risks and requirements.

More and More Laws, Regulations and Standards

Lack of adequate protection against personal information threats not only makes personal information vulnerable, it also potentially exposes businesses to lawsuits, criminal prosecution and civil actions. There are growing numbers of laws and regulations with requirements to protect a wide range of personal information.

Just a few of these in the U.S. include:

- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)
- Fair Credit Reporting Act (FCRA)
- Fair and Accurate Credit Transactions Act (FACTA)
- Children's Online Privacy Protection Act (COPPA)
- Telephone Consumer Protection Act (TCPA)

- FTC Act
- Do Not Call lists
- At least 48 state and territory breach notice laws

There are also international data protection laws, such as:

- EU Data Protection Directive 95/46/EC
- F.O.I. Freedom of Information Act 2000 (UK)
- Privacy & Electronic Communications regulation 2003 (UK)
- Canada's Personal Information and Electronic Data Act (PIPEDA)
- Australia's Privacy Act
- Japan's Personal Information Protection Act (IPA), Law No. 57 of 2003

More and More Incidents

Implementing an effective privacy program will help insulate your business against the type of privacy breach that could have substantial impact on revenue, brand and image. Additionally, should a breach occur, an effective program will help prepare your response in the most efficient and effective way possible. And, truth be told, all organizations - even those with the most diligent information security and privacy programs in place – should plan for that expectation just as they plan for other types of crisis management.

Consider the number of mobile users, technologies, customers, and locations that exist today. As that overall number increases, the number of incidents also increases. The Privacy Rights Clearinghouse (PRC) searched US news reports between Feb 15, 2005 and Nov 10, 2009 and logged 1,280 breaches.[19] These breaches cumulatively involved the information of 340 million people. Likewise, the UK Independent Commissioners Office (ICO) noted that between Nov 2007 and Nov 2009, 711 breaches that impacted individuals were reported.[20] And these are just a few data points from the several Web sites that track such breaches. Imagine the totals that aren't included in any easily-discovered list, or the number that aren't reported at all.

The fall-out from such privacy and security incidents can be substantial:

- Civil suits
- Regulatory fines and penalties
- Negative press
- Reduced stock values
- Lost customers
- Devaluation in brand name and reputation
- Diversion of resources (dollars and staff time of marketing, PR, attorneys and others)
- Cost of ongoing credit monitoring for affected customers
- Increased staff necessary to address the incident response activities
- Costs for mailings, phones calls, news releases

The information security and privacy policies that exist within most organizations usually do not cover all the diverse information technologies and use activities that involve data and personal information – powerful databases, global positioning systems, behavioral tracking software, social networking, etc. And how do you draw a line between what employees do at work vs. traveling on company business vs. in their homes? Most organizations draw a line between these activities, and rightly so. But without a comprehensive privacy program,

businesses are, in a very real way, operating with blinders on.

What Should Organizations Know About Privacy?

How should one start to effectively address privacy issues and requirements? Most privacy professionals suggest a look back at the work of the Organization for Economic Cooperation and Development (OECD)[21] which created the principles that form the basis of most worldwide data protection laws.

The OECD grew out of the Organization for European Economic Cooperation (OEEC) that was formed to administer American and Canadian aid under the Marshall Plan for the reconstruction of Europe after World War II. The OECD, with 30 member countries and involvement and input from 70 additional countries, works to (a) discuss, develop and refine various economic and social policies, including recommendations for security and privacy within global economic trade and communications, and (b) encourage a free flow of capital and services. The OECD is well known for what's known as its "soft law" (non-binding, but highly recommended) guidelines for multinational enterprises.

The OECD Privacy Principles[22] were established on September 23, 1980 as the basic principles for addressing international privacy protection. These Principles are listed on the following page (see *Figure 5: OECD Privacy Principles*, page 11).

These forward-looking principles reflect an international consensus and cover the handling of personal information in general as well as guidance on handling various types of media. Additionally, the principles provide the foundation for privacy protection on global networks. Since their publication more than twenty years ago, the OECD has continued to provide privacy guidance to address emerging laws, concerns and technology advances.

The OECD principles can be used as a foundation for a corporate privacy program and the ancillary policies and procedures that support a program. Not only are the OECD principles the widely accepted standard for privacy practices, but many of the legal requirements around the world are based on these principles.

Cross Border Personal Information Data Flows

Establishing policies and procedures to address the OECD privacy principles is a good start but by no means the full story. Organizations also need to comprehensively address the issues surrounding the transfer of personal information across country borders. The transfer of personal information across country borders is a complex issue and has presented significant legal and operational challenges for multi-national organizations ever since EU Data Protection Directive 95/46/EC went into effect in 1998.There are some very important restrictions on how personal information can, and cannot, be sent out of certain countries, as well as restrictions on the countries that cannot receive personal information.

In general, if one country considers the levels of protection for personal information placed by another country to be inadequate, then there may be specific types of activities prescribed for data transfer.

Here are a few important cross border issues that likely require consideration and action:

- Has the personal information data subject specifically given unambiguous consent to transfer the information to the other identified countries?

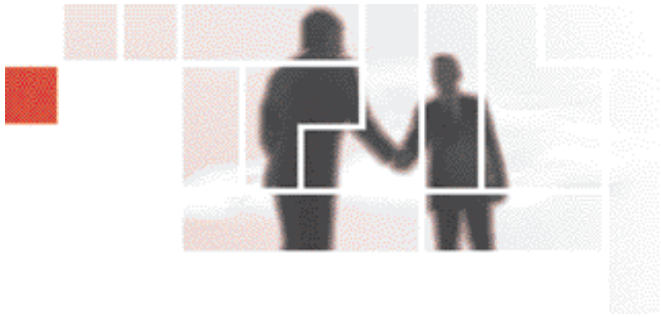


Figure 5: OECD Privacy Principles

- **Collection limitation:** Only personal information that is required to fulfill the stated purpose should be collected from individuals. Treatment of the information must conform to fair information processing practices. Information must be collected directly from each individual person unless there are very good reasons why this is not possible.

- **Data quality:** Every effort must be made to ensure that the personal information is accurate, complete and relevant for the purposes identified in the notice, and remains accurate throughout the life of the personal information within the control of the organization.

- **Purpose specification:** There must be a clearly specified notice describing the purpose for the collection, use, retention, and sharing of personal information. Data subjects should be told this information at or before the time of collection.

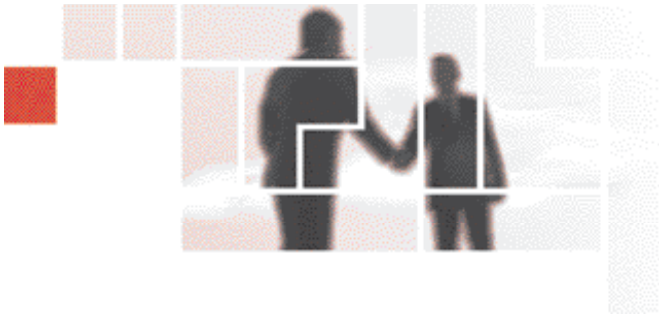
- **Use limitation:** Information should only be used or disclosed for the purpose for which it was collected and should only be divulged to those parties authorized to receive it. Personal information should be aggregated or anonymized wherever possible to limit the potential for computer matching of records. Personal information should only be kept as long as is necessary to fulfill the purposes for which it was collected.

- **Security safeguards:** Personal information, in all forms, must be protected from loss, theft and must prevent unauthorized access, disclosure, copying, use or modification.

- **Openness:** Privacy policies must be made available to personal information data subjects, and the data subjects must be given the ability and process to challenge an organization's compliance with their state privacy policies as well as their actual privacy practices.

- **Individual participation:** Organizations should provide a process for personal information subjects to allow them to ask to see their corresponding personal information and to request the correction of perceived inaccuracies. Personal information subjects must also be informed about parties with whom their corresponding personal information has been shared.

- **Accountability:** An organization must formally appoint someone to ensure that information security and privacy policies and practices exist and are followed.



- Must the personal information be transferred to meet contractual requirements between the personal information data subjects and the organization?
- Must the personal information be transferred to meet the data subject's request?
- Is the transfer of the personal information necessary to meet the contractual requirements of the personal information data subject and a business partner of the organization?
- Is the personal information transfer necessary or legally required?
- Is the personal information transfer necessary to protect the vital interests of the personal information data subject?
- Is the transfer of personal information made from an entity that is legally recognized as being a source that provides information to the public?

There are many ways in which an organization can address these challenges. Some of the most effective and most commonly used ways include:

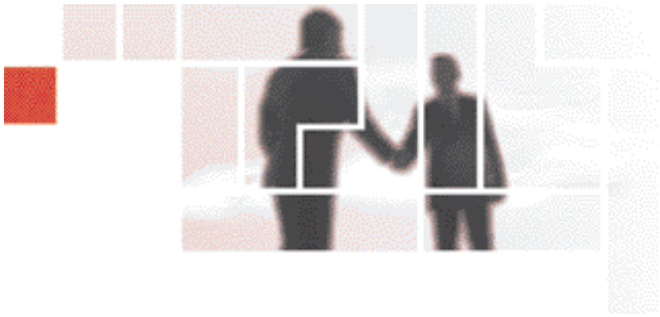
- Model contractual clauses: A form of contract entered into by the parties involved with data transfer that defines how the personal data processing will be managed.
- Alternative model clauses: In the European Union, these apply only to transfers from data controllers to data controllers and result from Decision 2004/915/EC on an alternative set of standard contractual clauses for the transfer of personal data to third countries.
- Binding corporate rules: Yet another alternative means approved by the European Commission which allow businesses to transfer data internationally using their own legally enforceable corporate rules.

In addition to these three briefly described options, some U.S.-based organizations may participate in the EU Safe Harbor program, which establishes a set of data protection rules that have been approved by the European Commission and are administered by the U.S. Department of Commerce. The rules are based on seven privacy principles:

- Notice. Details about data collection (such as the purpose for collecting information) and contact information for questions or complaints must be provided.
- Choice. Data subjects must be able to opt-out of data processing.
- Onward transfer. The notice and choice principles must apply for the disclosure of information to a third party.
- Security. Reasonable precautions must be taken to protect collected data.
- Data integrity. Information collected must only be used for its intended purpose.
- Access. Individuals must be allowed to review the data which has been collected about them and correct, amend or delete any inaccurate information.
- Enforcement. There must be mechanisms for ensuring compliance with the other principles, recourse for adversely affected individuals and consequences for non-compliant organizations.

If a business breaches the Safe Harbor requirements it is subject to action by the Federal Trade Commission. Furthermore, individuals affected by breaches have the right to seek redress.

Think about all the locations in the world where you have offices, personnel, customers, outsourced workers, processing and storage centers. Where is personal information flowing between all these



locations? For example, if you have an employee located in Germany who's looking at data on a monitor in the U.S., does your organization need to ensure all cross border issues have been addressed? Possibly – depending upon many variables – such as:

- Who collected the personal data originally?
- Where was the personal data collected?
- How is the data transferred?
- How is the data stored?
- Is the personal data shared with other entities?

Many U.S.-based organizations have found that participating in the EU Safe Harbor program helps to address many of the cross border personal information data flow issues. But they often need to employ some additional contractual options depending upon specific situations, e.g. if they outsource personal information processing to another third country.

Legal Requirements for Privacy

I've talked with literally hundreds of information security and privacy professionals in recent years and there is one common question: "How can I keep up with everything I have to do to legally comply with privacy requirements?" Staying up to date can certainly be an overwhelming challenge, but it's something that organizations cannot dismiss or wait to address at some later day.

Organizations need to continuously monitor legal compliance, new laws and regulations, and update programs as necessary. The number of laws and regulations that govern how personal information must be handled continues to grow worldwide. Organizations, and the personnel handling personal information, must understand and comply with the requirements and laws for all the locations in which personal information is handled.

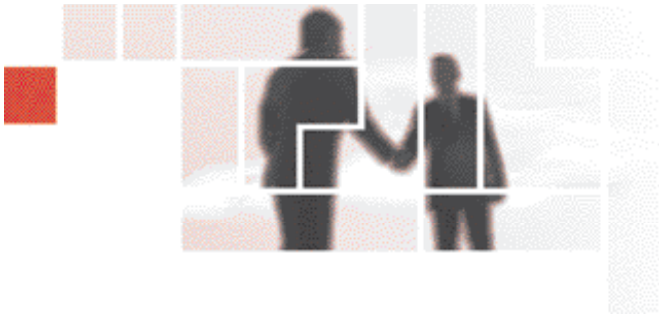
The continuous flow of new laws, regulations and standards address the increase in privacy breaches and information security incidents as well as the specific breaches themselves. As discussed earlier in this whitepaper, the increase can be attributed both to a preponderance of new technologies and lack of awareness on the part of individuals using them – often resulting in bad decisions with bad outcomes. And a poor economy generally only exacerbates insider threats.

The complexity of this ever-expanding regulatory landscape presents organizations with significant challenges when it comes to complying with multi-jurisdictional privacy laws and regulations. Organizations that store, process, and transmit personal data across national borders can no longer ignore the need to gain and maintain a better understanding of their industry and the jurisdictions in which they operate. Let's take a look at a few of these many legal requirements.

U.S. laws are highly decentralized

In contrast to most other countries in the world, the United States data protection laws are highly decentralized. Even the U.S. Federal Trade Commission (FTC) recognized this by stating in its 1998 Report to Congress that "American privacy law can best be described as sectoral, consisting of a handful of disparate statutes directed at specific industries that collect personal data." Of course, since 1998 there have been numerous state and federal level laws enacted that address privacy, all of which still attack the issue of protecting personal information in a very disjointed and disparate way.

Because the U.S. has historically relied less on government regulation and more on self-regulation by businesses, lawmakers have been reluctant to



impose the type of comprehensive privacy laws that can be applied across the board. The result is a huge patchwork of federal and state laws directed at specific industries or, increasingly, developed as a response to reported incidents. The financial and healthcare sectors are two of the most heavily governed but most industry experts expect that, with the increase in privacy incidents, more federal bills will be written to address data protection in general and across industries. For example, the HITECH Act provisions within the ARRA indicate how U.S. federal lawmakers have recently addressed the problem of privacy breaches involving health information across industries.

It is important for every organziation to identify all the international, federal, state and local laws and regulations that govern both their handling of personal information and their responses to personal information breaches. Organizations must identify all their contractural requirements including internal privacy policies that are posted to Web sites. If businesses do not identify these laws and contractural requirements, they are at risk of non-compliance, possible large fines and penalties, civil suits, and potentially business-ending damage due to reputation and brand. And, because international, national and local law and regulations are being overhauled at an incredible pace, organizations must remain diligent when addressing legal requirements.

Making sense of legal requirements

It's helpful when looking at all the laws, regulations and standards to ask the following six questions:

1. Why was the law created?
2. Who must comply with the law? Even if compliance isn't required, would following the requirements represent best practice and help in a civil suit?
3. What information is covered?
4. What actions are required?
5. What agencies enforce the law and where do I find compliance guidance?
6. What are the penalties?

Appendix A lists a few U.S. laws with brief commentary and analysis (page 18).

International laws are generally centralized

Over 90 countries have their own laws and the laws of any one country sometimes conflict with those of others. Differences complicate business and restrict the flow of personal information around the world. And a failure to address these requirements not only disrupts personal information flows but could result in serious damage to a business.

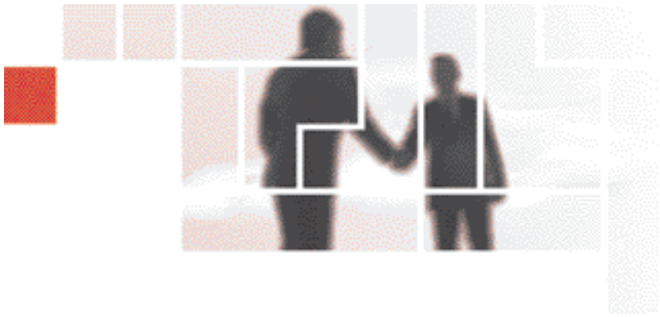
If your company has global consumers or business partners, you must know and understand which of these laws apply to you and how your organization is working to be in compliance.

Figure 6 on the following page (*Sample International Data Protection Laws*) provides just a few of the laws and related issues. As with the U.S. laws, be sure to work with your legal counsel to discuss these legal issues as well as to identify other laws that may apply to your organization.

When determining compliance procedures internally, you must understand both the requirements of applicable laws and your organization's data handling processes. Keep in mind that most international laws have requirements built around the OECD privacy principles discussed earlier.

Workplace privacy

With all the emphasis on customer and consumer privacy, don't forget to address privacy issues surrounding your own employees. In some areas the privacy requirements are even more stringent for personnel than they are for consumers.

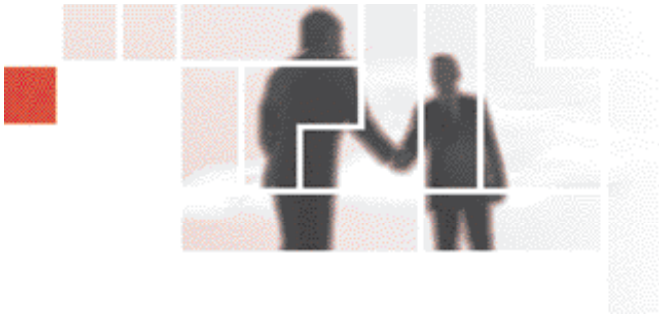


Here is a high-level framework for addressing workplace privacy:

1. Address workplace privacy
    - Before employment occurs
    - How is privacy protected within procedures around job applications and interview questions?
    - What type of employee candidate testing and background checks do you perform?
2. During employment
    - How is HR data protected and managed?
    - Why kind of workplace monitoring occurs? For example, closed circuit television, phone call recording, keystroke monitoring, Web site log-ins and so on?
    - What types of investigation procedures are in place for employee misconduct? Are privacy issues addressed?
3. After the employment relationship ends
    - Do your termination procedures address the privacy of the details involved with the individual?
    - Are privacy issues addressed within transition management and ongoing obligations for the individual?
    - What privacy issues could arise from post-termination claims?
    - How will you address privacy concerns related to document retention and destruction?

Figure 6: Sample International Data Protection Laws[23]

The E.U. Data Protection Directive 95/46/EC	Requires all twenty-five member countries to enact data protection laws that comply with the Directive's principles. Additionally, companies doing business in the member countries must comply with the country-specific laws (based on the Directive) in each country in which they have operations.
Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)	Must establish rules to govern the collection, use and disclosure of personal information for purposes that a reasonable person would consider appropriate in the circumstances. Built largely around the OECD privacy principles discussed in this paper.
Japan's Act on the Protection of Personal Information	Must, among other things, provide individuals with notice concerning the purposes for which the information will be used, maintain the accuracy of the information, allow individuals to access and request corrections to their information, and obtain consent before disclosing personal information to third parties. With respect to data security, covered entities must supervise employees and others who handle personal data, institute "necessary and proper" measures for preventing unauthorized disclosure, loss of or damage to personal data, and ensure that third-party contractors protect data security.
Australia's Privacy Act	Establishes information privacy principles, built largely around the OECD privacy principles discussed in this paper, for all government agencies and privacy sector organizations.



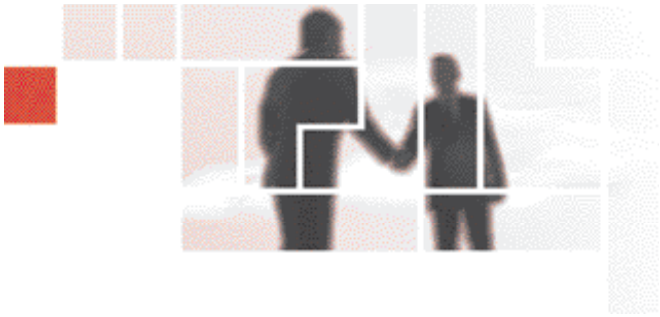
Most businesses find that someone in the organization needs to understand and be accountable for keeping up to date with and managing the applicable workplace laws, the associated privacy implications, and the organization's privacy practices.

U.S. laws typically emphasize employer duties with a focus on the security surrounding personnel data. The U.S. laws generally allow continuous and multi-dimensional employee monitoring. Aggressive background checks are also typically allowed and in fact are increasingly required for certain types of positions. Employee expectations are very limited. For more information on a number of US laws that specifically address different aspects of employment see Appendix B.

Organizations with employees outside the U.S. must address very different legal privacy requirements with the emphasis in most countries on the rights of the employees. For example, within the European Union privacy concerns of workers predominately govern the use of workers' personal information. Monitoring is only permitted with specific, limited legal justification. There are very limited allowances for background checks. Additionally, employees have very broad expectations and rights for privacy. Figure 7 lists some of the distinctive privacy requirements outside the U.S.

Figure 7: Worldwide Employee Privacy Rights[23]

Country/Region	Issues
European Union (E.U.)	• Employee data covered by the E.U. Data Protection Directive, each country's data protection laws and distinct labor laws • Broad regulation of "personal data" (including name and work address) with additional rules for "sensitive data" • Restrictions on both local processing and cross-border transfers • Must consult with "Works Councils" • Must notify Data Protection Authorities (DPAs) • Detailed notices to employees who have right to object to certain grounds
Argentina	• E.U. style privacy laws greatly influenced by Spain's laws • Continuous and multi-dimensional employee monitoring is okay
Canada, Australia and New Zealand	Within all three countries there are very similar E.U. style laws, but significant exemptions for employee data, no transfer prohibition and no government filings
Hong Kong	More commerce-friendly than E.U. law but the Hong Kong DPA has issued substantial guidance regarding employee data
Japan	The 2005 law includes employees, stresses notice and consent for data sharing



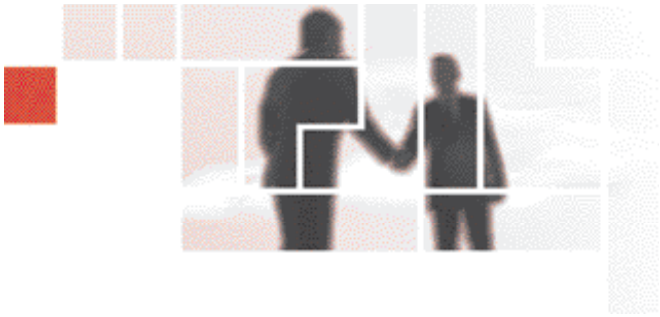
SAI GLOBAL WHITEPAPER

Business Needs Effective Privacy Management

This whitepaper presents a very wide range of data protection issues that organizations around the world must address. To complicate the issue, the public and the media have tended to lump many separate issues under the heading of "privacy." However, each of the issues of privacy, confidentiality and data protection are complex and require an understanding of laws and regulations, fundamental human rights, business practices and processes, contractual obligations, information security, technology, trends in using new social media, and personnel expectations. In addition to this understanding, organizations must also analyze and determine how to most effectively mitigate the risks involved with each issue.

Addressing all these growing privacy risks goes beyond the mere implementation of technology. No matter what a software or hardware vendor may say, privacy requirements and risks cannot be effectively addressed and resolved simply by implementing a new application or system. Although technologies address a small portion of privacy issues, ensuring privacy and compliance with all the legal privacy requirements throughout the world is largely a human issue. Organizations must ensure they have the policies, procedures, supporting training, and ongoing awareness communications and activities in place.

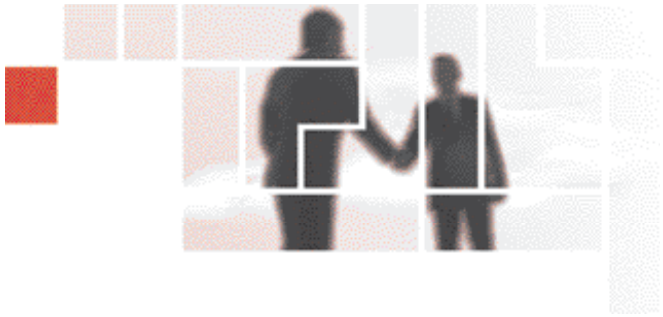
Organizations often lack the knowledge, information and tools to effectively and efficiently manage privacy across the enterprise. Privacy and data protection management requires an understanding of technology, business processes and the political and legal environment of multiple jurisdictions, along with proactive and insightful business leadership. Our next whitepaper on this subject provides the guidance to create an efficient and effective privacy management program to better manage privacy risk and achieve data protection compliance.



Appendix A: Samples of U.S. Laws and Demonstrated Accompanying Analyses[23]

The following selection of laws and accompanying analyses are provided as a sample of how you can do analysis within your own organization. These particular laws impact a large number of businesses due to their scope. Be sure to work with your legal counsel to discuss these legal issues as well as to identify other laws that may apply to your organization.

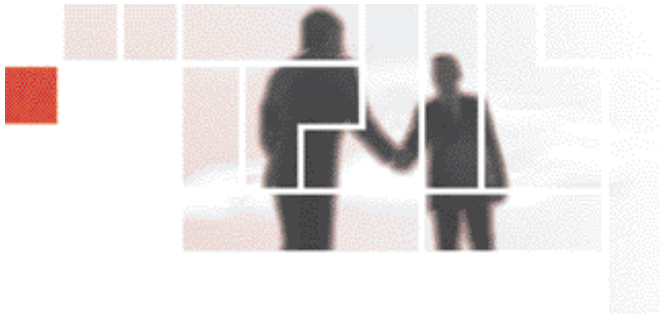
U.S. Fair Credit Reporting Act (FCRA)	
Why was the law created?	To mandate accuracy, access and correction and to limit use of consumer reports to permissible puposes. The FCRA was amended in 1996 with provisions for non-consumer-initiated transactions and standards for conusmer assistance. It was amended again in 2003 with provisions related to identity theft within the Fair and Accurage Credit Transactions Act (FACTA).
Who must comply with the law?	• Entities that compile consumer reports • Persons who use consumer reports
What information is covered?	A consumer report is basically any information that pertains to credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living, and that is used, in whole or in part, as a factor in establishing a consumer's eligibility for credit, insurance, employment, or other business purpose.
What actions are required?	• Third party data used for substantive decision-marking must be appropriately accurate, current and complete • Consumers must receive notice when third party data is used to make adverse decisions about them • Consumer reports may only be used for permissible purposes • Consumers must have access to their consumer reports and have an opportunity to dispute/correct any errors • Must comply with all other requirements on users and furnishers of consumer information
What agencies enforce the law?	• Federal Trade Commission (FTC) • State attorneys general • Private right of action exists
What are the penalties?	• Civil and criminal penalties • In addition to actual damages, violators are subject to statutory damages
U.S. Gramm-Leach-Bliley Act (GLBA)	
Why was the law created?	As a modernization statute to revamp the banking and insurance industries and to address privacy concerns resulting from the consolidation of financial data.
Who must comply with the law?	U.S. based financial institutions, defined as "…any company significantly engages in financial activities."



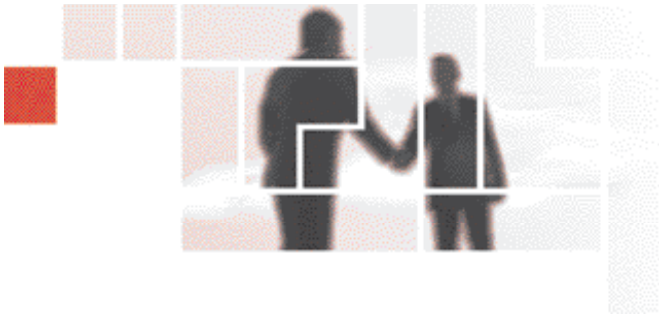
What information is covered?	"Non-public personal financial information" which includes any information: • Provided by a consumer to a financial institution (FI) in order to obtain a financial product or service • Resulting from a transaction involving a financial product or service between a FI and a consumer • That the FI otherwise obtains in connection with providing a financial product or service to a consumer

What actions are required?	• The GLBA Financial Privacy Rule requires:
	  • Initial and annual privacy notices to customers
	  • Nine categories of information to be protected
	  • Process to allow customer to opt out within 30 days
	  • Share with other third parties only if any exception exists or no opt-out is received
	  • Ensure that service providers will not use the data for other purposes
	• The GLBA Safeguards Rule requires
	  • Administrative security
	  - Program definition and administration
	  - Manage workforce risks, employee training
	  - Vendor oversight
	  • Technical security
	  - Computer systems, networks and applications
	  - Access controls
	  - Encryption
	  • Physical Security

What agencies enforce the law?	• FTC and financial institution regulators • State attorneys general
What are the penalties?	• Enforcement actions and possible private lawsuits • No private right of action, but failure to comply with a notice is a deceptive trade practice, actionable by state and federal authorities. Some states do have private rights of action for unfair and deceptive trade practice violations.
U.S. Health Insurance Portability and Accountability Act (HIPAA)	
Why was the law created?	To protect health insurance coverage from employer to employer, as well as to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers. It also addressed the security and privacy of health data.
Who must comply with the law?	• Covered entities (CEs) include health care providers, health plans and health care clearinghouses • "Business associates" and others who use or disclose protected health information (PHI) from CEs are now also responsible for following HIPAA requirements under the expansions resulting from the HITECH Act.
What information is covered?	• The Privacy Rule covers PHI transmitted or maintained in any form • The Security Rule covers PHI in electronic form



What actions are required?	Covered entities may not use or disclose PHI except as permitted or required by the Privacy Rule and the Security Rule.
What agencies enforce the law?	• The U.S. Department of Health & Human Services (HHS) • State attorneys general
What are the penalties?	• Civil and criminal penalties with fines of up to $50,000 per violation to a maximum $1,500,000 for all violations of an identical provision and/or 10 years imprisonment • Does not pre-empt stronger state laws
The U.S. Children's Online Privacy Protection Act (COPPA)	
Why was the law created?	Created in response to large numbers of Web sites collecting personal information from young children to regulate unfair and deceptive acts and practices in connection with the collected data.
Who must comply with the law?	Commercial Web site operators
What information is covered?	Collection and use of information on children under the age of 13 years via a commercial Web site.
What actions are required?	With a few exceptions, Web site operators must obtain verifiable parental consent before they can collect personal information from children
What agencies enforce the law?	FTC and state attorneys general
What are the penalties?	• Unlimited fines and penalties from the FTC and state attorneys general • Civil actions



SAI GLOBAL WHITEPAPER

Appendix B: Samples of U.S. Laws Addressing Aspects of Employment[23]

A few U.S. laws that prohibit discrimination – which result in limiting inquiries for personal information – include those below.

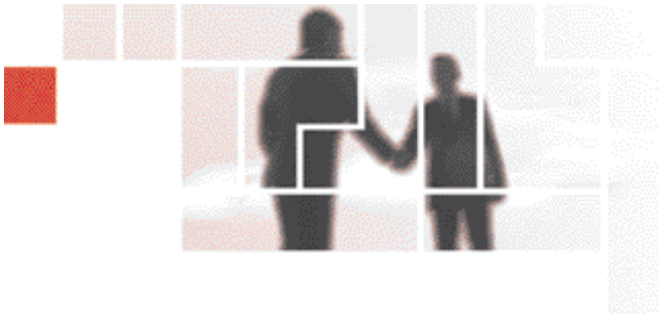
Laws Addressing Discrimination

Law	General Description
The Civil Rights Act of 1964	No discrimination due to race, color, religion, sex, national origin
Pregnancy Discrimination Act	Adds pregnancy, childbirth and related medical conditions
Americans with Disabilities Act of 1990 (ADA)	No discrimination against qualified individuals with disabilities
Age Discrimination Act of 1967	Protects individuals over 40 years of age
Equal Pay Act of 1963	Prohibits gender-based wage discrimination

Some of the U.S. Laws that regulate employee benefits management and which often mandate the collection of medical information include those listed below.

U.S. Laws Addressing Personnel Benefits Management

Law	General Description
The Health Insurance Portability and Accountability Act (HIPAA)	Privacy and security rules regulate protected health information (PHI) for self-funded health plans
Consolidated Omnibus Budget Reconciliation Act (COBRA)	Requires qualified health plans to provide continued coverage after termination to certain beneficiaries
Employee Retirement Income Security Act (ERISA)	Ensures that employee benefits programs are created fairly and administered properly
Family and Medical Leave Act (FMLA)	Entitles certain employees to leave in the event of birth or illness of self or a family member



There are many other U.S. laws with employee privacy implications and requirements for data collection and record keeping. A few of these include those listed below.

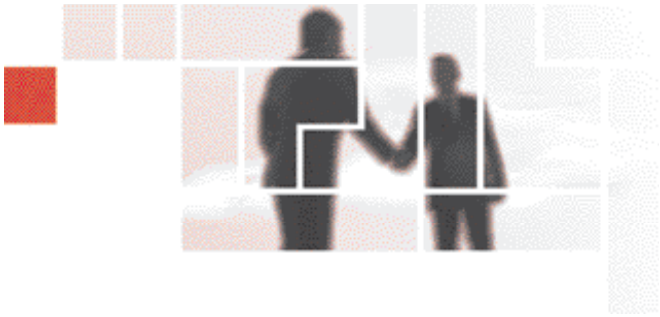
U.S. Laws Impacting Employee Information Collection

Law	General Description
Fair Credit Reporting Act (FCRA)	Regulates the use of "consumer reports" in the background checks of employees
Fair Labor Standards Act (FLSA)	Establishes a minimum wage and sets standards for fair pay overall
Occupational Safety and Health Act (OSHA)	Regulates workplace safety and record keeping practices
National Labor Relations Act	Sets standards for collective bargaining
Immigration Reform and Control Act	Requires employment eligibility verification

U.S. federal employers also must consider many other laws impacting personnel information, such as those shown below .

U.S. Laws Covering Federal Employers

Law	General Description
The Privacy Act of 1974	Requires privacy notices and limited collection of data
The Whistleblower Protection Act	Protects federal employees who report violations of law
The Fourth Amendment of the U.S. Constitution	Sets limits on search and seizure of items



SAI GLOBAL WHITEPAPER

Footnotes

[1]Accessed on November 10, 2009 from http://www.guardian.co.uk/business/2009/may/18/digital-content-expansion

[2] All trademarks of their respective owners

[3] More information about the OECD privacy principles is available at http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

[4] More invormation about the EU Data Protection Directive is available at http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm

[5] November 1, 2009 citation from http://eval.symantec.com/mktginfo/enterprise/white_papers/b-symc_report_on_rogue_security_software_WP_20100385.en-us.pdf

[6] Ponemon Institute study: http://news.cnet.com/8301-1009_3-10360639-83.html?tag=mncol;title

[7] "Americans Reject Tailored Advertising: And Three Activities That Enable It." September 29, 2009. J Turow, J King, CJ Hoofnagle, A Bleakley, M Hennessy. Accessed November 10, 2009 from http://graphics8.nytimes.com/packages/pdf/business/20090929-Tailored_Advertising.pdf

[8] "'Big Yellow Taxi': The Erosion of Personal Privacy within Social Media." May 8, 2009. A Boyd, K Williams, R Chin, S Densten, D Diamond, C Morgenthaler. Accessed November 10, 2009, from "Americans Reject Tailored Advertising: And Three Activities That Enable It." September 29, 2009. J Turow, J King, CJ Hoofnagle, A Bleakley, M Hennessy. Accessed November 10, 2009 from http://graphics8.nytimes.com/packages/pdf/business/20090929-Tailored_Advertising.pdf

[9] "Trust and loyalty: A cross-cultural comparison." C Bonanni, D Cyr. Proceedings for the International Conference of Business, Economics and Management Disciplines. (2004). Pg 3.

[10] "Comparing Privacy Attitudes of Knowledge Workers in India and the U.S." INTERACT 2009. S Patil, A Kobsa, A John, D Seligmann. Accessed November 10, 2009 from http://www.ics.uci.edu/~kobsa/papers/2009-Cult&Tech-kobsa.pdf.

[11] "Community Attitudes to Privacy 2007." Wallis Consulting Group. Accessed November 10, 2009 from http://www.privacy.gov.au/aboutprivacy/attitudes.

[12] "Israeli attitudes on privacy." S Bennett. "The Privacy Advisor." The International Association of Privacy Professionals. October 2009; pg. 1.

[13] "Truly depressing": GFI laments lack of insight into current IT needs from UK SMEs" Accessed November 27, 2009 from http://www.infosecurity-magazine.com/view/1318/truly-depressing-gfi-laments-lack-of-insight-into-current-it-needs-from-uk-smes

[14] Personal data is defined very broadly as any "information relating to an identified or identifiable natural person (data subject). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number, or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."

[15] Excerpted from "The Privacy Management Toolkit" by Rebecca Herold, published by Information Shield; http://www.informationshield.com/privacy_main.html.

[16] Does not include the name, title or business address or telephone number of an employee of an organization

[17] While this law does not explicitly list this item, it is possible that using this item could be considered as violating the law because the way the law is written it could include this item. It could depend upon the judge, jury, and the other policies, contracts and documents the organization has published or provided.

[18] Excluding the 5-digit US Zip Code

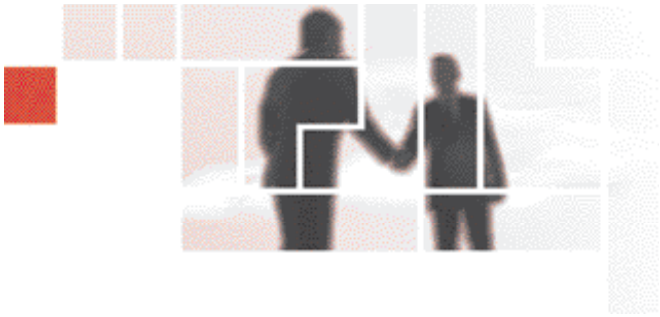
[19] For additional details about breaches, refer to http://www.privacyrights.org/ar/ChronDataBreaches.htm

[20] Accessed on November 28, 2009 from http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/breach_notification_spreadsheet_nov09.pdf

[21] More information is available on the OECD Web site http://www.oecd.org.

[22] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, © OECD 2002 All rights reserved. This term was originally published by the OECD. However, this reproduction does not necessarily reflect the official views of the Organization or of the governments of its member countries.

[23] This table is taken from in-sites classes provided by Rebecca Herold & Associates, LLC. Up-to-date and on-demand guidance is also available through SAI Global's Privacy Knowledgebase.



SAI GLOBAL WHITEPAPER

SAI Global

SAI Global is one of the world's leading business publishing, compliance, training and assurance organizations with operations in North America, Europe and Asia Pacific. The Compliance Division of SAI Global works with organizations worldwide helping to build a culture of compliance. Using our international experience, we deliver effective solutions to help manage risk, achieve compliance and promote ethical behaviour. We offer a flexible range of risk and compliance solutions and services, which engage staff at all levels of an organization.

About the Author

Rebecca Herold, CIPP, CISSP, CISM, CISA, FLMI, has provided information security, privacy and compliance training, services, tools and products to organizations in a wide range of industries throughout the world for over two decades. Rebecca has been named one of the "Best Privacy Advisers" multiple times by Computerworld magazine and one of the "Top 59 Influencers in IT Security" by IT Security magazine. She is also an author and adjunct professor for the Norwich University Master of Science in Information Assurance (MSIA) program. rebeccaherold@rebeccaherold.com; www.privacyguidance.com.

Americas
101 Morgan Lane, Suite 301, Plainsboro, NJ, 08536, USA
Tel: +1-877-470-SAIG (7244), Fax: +1 609 924 9207
e-mail: info.americas@saiglobal.com

Europe, Middle East and Africa
42 The Square, Kenilworth, Warwickshire CV8 1EB, UK
Tel: +44 (0)1926 854111, Fax: +44 (0)1926 854222
e-mail: info.emea@saiglobal.com

Asia Pacific
224-226 Normanby Road, Southbank, Melbourne, VIC 3006,
Australia, Tel: +61 3 9278 1555, Fax: +61 3 9278 1556
e-mail: info.asiapac@saiglobal.com

www.saiglobal.com/compliance