Protecting Confidential Information and Workplace Privacy in the EU and US

Report Prepared By:

Gary E. Clayton
Privacy Compliance Group, Inc.
8150 North Central Expressway
Suite 1900
Dallas, Texas 75206
214-365-1665
www.privacycouncg.com
gclayton@privacycg.com

Introduction

Requirements for Protecting Workplace Privacy

Rapid growth of technology in the workplace has brought new benefits and challenges to companies around the globe. Increased productivity, instantaneous communications and reduced costs are among the benefits companies are realizing. As companies have grown more dependent upon technology, however, it has become essential to protect computers, databases, e-mails and Internet systems from internal and external risks. Ironically, the very ease of communication fostered by these technologies has created risks to the company's assets, particularly to its confidential and proprietary information. With a click of a mouse an employee can send out an entire customer list or copy of source code or design documents. In order to protect these digital assets, companies should consider implementing and tailoring monitoring of their assets to effectively manage these risks – while carefully avoiding the creation of new risks. During this process, the needs of the company may come into conflict with employees' expectations of privacy – and the rights to privacy imposed by laws in the United States and around the globe.

At the outset, it is important to recognize that effective management of workplace privacy issues requires a multi-faceted approach. One important element is the adoption of technology that can target specific risks while complying with strict policy requirements. The implementation of such technology provides management with an essential tool in dealing with workplace monitoring and privacy issues. The paper will examine:

- Effective Management of Workplace Privacy Risks
- Risks Involved with Workplace Monitoring
- Monitoring in the United States
- Monitoring in the European Union
- Relevant Privacy Legislation Related to Monitoring
    - Recommended Steps to Consider Before Monitoring
    - Transborder Transfers of Personal Data
- How Vontu Effectively Safeguards Employee Privacy
- Grading of Vontu's Safeguarding of Employee Privacy

I. Effective Management of Workplace Privacy Risks

Knowledge, Planning and Technology are Essential

How does a company manage workplace privacy issues when the rules are varied and/or not fully established? Based upon Privacy Compliance's Group's expert's experience in working with Fortune 500 companies for over a decade, the starting point is to understand your company's use of data and the general principles that impact the data. Understanding the use of personal data involves determining the "who, what, when, where and how" of data processing:

1) Who is processing/collecting the data?
2) What data is being collected?
3) When is the data being collected?
4) Where is the data being collected and processed?
5) How is the data being collected and processed?

With this information in hand, the next step is to understand that even though there are many distinctions between the laws of the U.S. and those of the E.U., there are a number of general principles that apply throughout the United States, the European Union and many other regions of the world that have based their privacy laws upon those of the E.U. These general principles are:

a. Respecting employees' expectation of privacy;
b. The principle of proportionality;
c. Compliance with company policy;
d. Limitations on the use of data that are collected; and
e. Compliance with the fair information practice principles.[1]

[1] The fair information practice principles were first articulated in a comprehensive manner in the United States Department of Health, Education and Welfare's seminal report entitled *Records, Computers and the Rights of Citizens* (1973). In the three decades that have elapsed since the HEW Report, a canon of fair information practice principles has been developed by a variety of governmental and inter-governmental agencies in the United States and around the globe. A number of countries have added additional principles; however, they are basically just variations of those contained in the HEW Report. The fair information practice principles set forth in the HEW Report are: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and, (5) Enforcement/Redress. In addition, this paper has included the principles of "onward transfer" and "proportionality" from the European Union because they have such significance for companies that process personal data from the European Union. The concept of onward transfer also has a place in U.S. law with such laws as the Gramm-

Employees' Expectation of Privacy

One of the major differences between the U.S. and E.U. regulation of workplace privacy relates to employees' expectation of privacy. In the United States, employers face a myriad of federal and state laws that protect the privacy of communications at work. These laws often limit how and when an employer can monitor as well as what can be monitored. But generally, even without prior and express employee consent, U.S. employers can monitor workplace communications and activities. As a result, employers are often advised to notify employees that they have no reasonable expectation of privacy in their communications while in the workplace. In the European Union, however, data protection officials frequently state that employees do not leave their rights to privacy at home when they come to work. E.U. employees are afforded much greater workplace privacy rights and protections than their counterparts in the United States.

The Principle of Proportionality[2]

In the E.U. and increasingly in the U.S., employees, Congress and the courts apply the principle of proportionality to determine the legitimacy of surveillance. The principle of proportionality means that workplace monitoring is justified only if:

- It is *necessary* to protect the legitimate business needs of the employer; and
- The monitoring goes no further than is necessary to meet that need.

Essentially, therefore, proportionality involves a balancing act between the needs of the employer and the rights of the workers. The main consideration in both the U.S. and the E.U. is the extent to which

---

Leach-Bliley Act and the Health Insurance Portability and Accountability Act where contractual safeguards are required for the transfer of covered data to third parties.

[2] Proportionality has evolved from the notice and choice principles. Courts and governmental enforcement officials look at a company's privacy notice and the reasons set forth relating to the purpose for collecting data. While companies are not required to state with complete specificity all data that is being collected, they are required to give general descriptions of the types of data being collected. The principle of proportionality applies a relevancy test to determine if the information collected is reasonably related to the stated purpose and if so, is it necessary to achieve that purpose. In the United States, this principle has been implemented in HIPAA. The HIPAA Privacy Rule generally requires covered entities to make reasonable efforts to limit the use or disclosure of, and requests for, protected health information to the *minimum necessary* to accomplish the intended purpose. HIPAA Privacy Rule, 45 C.F.R. §164.502(b).

monitoring will intrude into employees' private lives or capture information which they could reasonably regard as confidential or sensitive. As a practical matter, this balancing act is also impacted by the effect that monitoring has on employee morale. The less focused and more widespread the monitoring, the more adverse the impact is likely to be on employee morale.

Compliance with Internal Policies[3]

In order to meet the principle of proportionality, any monitoring performed should be the least intrusive possible, the information collected should be targeted, and the use of information collected should be limited. This means that companies are advised to put in place policies regarding the collection and use of personal information during monitoring. These policies should advise employees what will be monitored and how the monitoring will be performed. Additionally, the policies should advise employees about the use of information that is gathered during monitoring.

The purpose of such policies is not to arm employees with the information needed to avoid monitoring; rather, it is to ensure that employees understand what privacy rights they should expect and understand the consequences if they violate company policies. Corporate policy should include provisions that clearly state the following:

- Employees are being put on notice that the computer, modem, telephone and e-mail systems are the property of the employer.
- Use of these systems is strictly for business purposes.
- If personal use of the systems is permitted, certain limits are imposed.
- The company reserves the right to monitor, review or inspect the employee's e-mail and other communications.
- A warning that any such review of monitoring or inspection is to be conducted as part of the company's ordinary course of business.

The implementation of such policies will ensure that employees are fully informed about the company's position. Having such policies also

[3] Internal policies provide "notice" to employees. One of the fundamental principles of privacy protection is that individuals must receive notice before personal information is collected. As seen by the Federal Trade Commission's privacy enforcement actions, companies most frequently get into trouble for having notices or policies that state something different than what the company's actual practice is. In the area of employment law, written policies are often necessary to reduce the risks associated with enforcement or termination actions against employees who violate stated policies.

imposes obligations upon the employer. Once a company states its policy regarding monitoring, it must generally comply with that policy. This means that the company must have in place processes, procedures and technology than can ensure compliance with the stated policies.

Limitations on the Use of Data Collected

Information collected during monitoring should be used *only* for the stated purposes. This means that data gathered during monitoring should be closely controlled and safeguards put in place to ensure that the information is used only for legitimate purposes. There should be controls placed on who can access the data and how it can be used. There should also be audit procedures put in place to ensure that all aspects of the collection and use of the information are carefully recorded. Finally, companies should ensure that personal or non-relevant information is carefully protected and its use limited.

Another significant aspect of limiting the use of data is ensuring that only the data regarding the violation of policy is collected and used. There are several factors involved with this aspect of limitation:

1) The technologies used to monitor should be configured to collect only communications and work tasks that violate policy.
2) Secondly, the monitoring should avoid "false positives." False positives arise when the monitoring technology incorrectly determines that a message violates policy and collects the information in the message. Correctly identifying and collecting only messages that violate policy are important aspects in limiting risks to the company.
3) Only employees with proper security access and a need to know should be able to view and remediate violations.

Fair Information Practice Principles

The United States and the European Union have entered into a "safe harbor" framework as a way to avoid interruptions in the transfer of data with the E.U. Companies that certify under the safe harbor will assure that they provide "adequate" privacy protections, as defined by the E.U.'s Data Protection Directive. Joining the safe harbor program is purely voluntary, but organizations that join must agree to comply with seven safe harbor principles. Regardless of whether or not your company belongs to the safe harbor program, these principles underlie many of the U.S. and European privacy laws and serve as a useful roadmap for

companies in the processing of employee data. The six principles require the following:

1) **Notice**: Companies must notify individuals about the purposes for which they collect and use information about them. Companies must provide information about how individuals can contact the company with any inquiries or complaints, the types of third parties to which it discloses the information and the choices and means the organization offers for limiting its use and disclosure.

2) **Choice**: Companies must give individuals the opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with original purpose for which it was collected or subsequently authorized by the individual. For sensitive information, affirmative or explicit (opt in) choice must be given if the information is to be disclosed to a third party or used for a purpose other than original purpose or the purpose authorized by the individual.

3) **Access**: Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete the information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individuals' privacy, or where the rights of persons other than the individual would be violated.

4) **Security**: Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.

5) **Data Integrity**: Personal information must be relevant for the purposes for which it is to be used. An organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete and current.

6) **Enforcement**: There must be readily available and affordable mechanisms to resolve disputes and complaints and to ensure compliance with the principles.

These general principles apply to the workplace and the collection of personally identifiable information on employees. Absent specific legislation, these principles (and the specific principles of the E.U. Data Protection Directive) provide guidance for determining how to effectively protect information gathered on employees. As previously noted Europeans workers are generally aware of their privacy rights and have a high expectation that their personal data – including data collected during monitoring – will be protected. The failure to comply with the general principles discussed in this section can result in liability for the company and have a negative impact on your company's culture.

II. Risks Involved in Workplace Monitoring: An Overview of U.S. and E.U. Requirements

Network Monitoring for Risk Management

For more and more companies, issues involved in workplace monitoring[4] must be assessed in light of global human resource privacy laws. Two trends have combined to expand the application of such global rules to more than the Fortune 500: the globalization of the U.S. economy and the growing reach of the data protection laws of the E.U. These trends have combined to raise a series of complex regulatory requirements for companies operating internationally, whether with a full service office located in Europe, or with European sales or customer service and development offices. The processing, storage, transfer and monitoring of personal information on employees are regulated by many of the United States' most important trading partners, particularly those in the European Union.

European privacy and data protection laws can affect U.S. companies in a number of distinct respects:

- A European subsidiary must comply with the privacy laws in the countries where they have operations, and as discussed below, such countries can have laws that are significantly more restrictive than those in the United States.
- The transfer of personal information can be blocked under E.U. laws unless specific requirements are met.
- Countries around the globe are adopting laws similar to those of the E.U. due in part to the global reach of the E.U. privacy laws.

The next section of the paper will examine and compare the workplace privacy laws of the U.S. and the European Union. It is important for companies in the United States to understand that they are affected by workplace privacy issues even if they are not operating internationally. The next section will discuss the data protection issues that impact most U.S. companies.

[4] Privacy laws may apply to all types of monitoring: network communications, e-mail, Internet, telephone, CCTV and audio monitoring. A number of laws also regulate monitoring systems that intercept communications, such as e-mails or telephone calls in the course of their transmission. This paper uses the term "monitoring" to cover all such communications, regardless of whether they are intercepted during transmission or monitored while in storage. Under European and U.S. laws, such communications contain personal information and, therefore, are regulated by privacy laws.

III. Monitoring in the United States

Notice is Key for Employee Monitoring

In the United States, most employment law treatises usually describe the situation in the U.S. with the general rule that employees who have been notified of the employer's monitoring no longer have a reasonable expectation of privacy and can be deemed to have granted complied consent by continuing to attend work at will. A review of the significant legislation, however, reinforces the principle that employers should provide notice and where possible, obtain informed consent from employees before undertaking monitoring. Perhaps the most significant legislation regarding privacy in electronic communications is the Electronic Communications Privacy Act of 1986 (the "ECPA"). The ECPA amended what was commonly referred to as the Federal Wiretapping Statutes. Under the ECPA the intentional interception of any wire, oral or electronic communication is prohibited. An offender can be liable for various civil and criminal penalties. Significantly, the ECPA allows individual states to enact their own laws regarding electronic privacy, as long as those laws are at least as protective as the ECPA.

The ECPA clearly protects privacy rights although it is ambiguous regarding those rights in the workplace. Employers generally have relied upon certain exceptions to the ECPA to stay out of the reach of the legislation. The ECPA provides a "business exception", which permits interceptions when telephone or telegraph components are used in the ordinary course of business and for legitimate business purposes (18 U.S.C. 2510(5) (a)). To the extent that courts find that modems and computers qualify as telephone components, employers can certainly assert legitimate business reasons for monitoring employee e-mail communications in order to exempt themselves from the Act. Another important exception exists when one of the parties to the communication has given prior consent to the interception or access. (18 U.S.C. 2511(2) (d)).

Courts interpreting the ECPA have generally found in favor of the employer where the company could point to a legitimate business reason for monitoring. Companies that have clearly identified a legitimate business need for monitoring and have then limited the monitoring to meet those needs typically have been found to fall outside the scope of the ECPA.

Bottom Line under the ECPA: Identify a legitimate business reason for monitoring and then employ technology that limits monitoring to meet those needs. Notify employees in writing that monitoring will take place and obtain consent.

Companies should also be aware that employees have relied on the fourth amendment of the Constitution as the basis for an invasion of privacy claim for monitoring in the workplace. A number of cases have addressed the question of whether employees have a "reasonable expectation of privacy" in the use of computers, e-mail and the Internet in the workplace. In cases where clear notice was given to employees or where there were splash screens notifying employees when their computers were turned on, courts have found that the employees' expectation of privacy was diminished and dismissed their claims.

Courts are insisting that employers provide clear notice to employees before monitoring takes place. Courts have denied employer claims of employee consent where the policy had not been stated with sufficient clarity. In *Williams v. Poulas,* 11 3d 271, 280-281 (1st Cir. 1993), for example, the court rejected an employer's consent defense on the ground that the employee was not "informed" "of the manner in which the monitoring was conducted." In *Deal v. Spears,* 980 F.2d 1153, 1158 (8th Cir. 1992), the Eighth Circuit Court of Appeals rejected a defense based upon consent when the employee was not informed "that [the employer was] monitoring the phone, but only [that the employer] *might* do so…". (Emphasis added).

Companies should implement a policy regarding the use of e-mail and the Internet. The policy should outline both the employer's rights and the employee's rights. Such a policy will help ensure that the company's practices fall within the business exception and prior consent exception of the ECPA. It should also help protect against fourth amendment claims by reducing employees' expectation of privacy.

In addition to development of an effective policy, the company should deploy technology that effectively targets messages or information that violates policy. The monitoring technology should maintain an audit trail of the information collected. The information should be adequately protected and used only for the purposes stated in the policy.

IV. Monitoring in the European Union

Stricter Privacy Rules in Europe

While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the E.U. has taken a different approach to privacy from that taken by the United States. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self regulation. The European Union, however, relies on comprehensive legislation that, for example, requires creation of government data protection agencies, registration of data bases with those agencies, and in some instances prior approval before personal data processing may begin.

Companies that operate internationally must understand the different privacy requirements between the United States and the European Union. The collection, storage and transfer of confidential information on employees are controlled by many of the European Union's Member States. Simple steps like monitoring e-mail or sending employee information to the United States can violate the privacy laws in Europe. Unfortunately, although the Member States of the European Union have adopted a Data Protection Directive in an effort to "harmonize" their privacy and data protection laws, there are still significant differences that must be understood by U.S. companies operating in Europe.

This section will examine the privacy laws of a number of the major E.U. Member States. This section will also examine the E.U. Data Protection Directive and the potential limitation it places on the export of personal data to locations outside of the E.U. This is important for companies that (1) operate in the European Union; (2) have affiliates or subsidiaries in the European Union that collect personal information; (3) have employees residing in the European Union; (4) otherwise collect personal information from the European Union.

United Kingdom

U.K. Information Commissioner has implemented Code

This section is important for companies that are U.K. based as well as those with offices or employees located in the United Kingdom. In the United Kingdom, workplace monitoring is regulated by the Data Protection Act of 1998 as it generally involves the processing of personal data. However, the Information Commissioner has set out detailed guidance for

companies as to how the legislation applies to workplace monitoring. The Information Commissioner's office has published its Employment Practices Data Protection Code to regulate workplace monitoring. The Code expressly recognizes the need to "strike a balance between a worker's legitimate right to respect for . . . private life and an employer's legitimate needs to run its business." Under the Code, employers are required to carry out an impact assessment to establish whether any planned monitoring is necessary to address a legitimate business need, and goes no further than is necessary to meet that need.

The U.K Information Commissioner is responsible for enforcement of the Employment Practices Data Protection Code and the Data Protection Act of 1998. This does not prevent individual employees or potentially other interested parties from pursuing claims against employers who do not comply with the law. Any company that collects or processes personal information on employees located in the U.K. should carefully review and understand the Information Commissioner's codes.

Bottom Line under U.K. Law: A detailed impact assessment must be performed to document a business need for monitoring, and the method of monitoring must be targeted and the least intrusive possible. Written notice must be provided to employees providing clear information on how monitoring will be conducted, what information will be collected and the reason for the monitoring.

France

Provides among the strictest limits on workplace monitoring in Europe

In France, both the legislation and the case law provide greater privacy protections than in the U.K. The French Labor Code recognizes the employer's right to monitor the proper performance of work tasks by its employees, provided that such monitoring does not violate the employee's fundamental rights and freedoms. (Art. L.120-2). Network monitoring of employees is thus permitted, subject to the protection of the employee's rights.

In France, all monitoring systems must be registered with the French Data Protection Authority (*la Commission Nationale de L'Informatique et des Libertes (CNIL)*) prior to implementation. The CNIL is also responsible for enforcing the privacy laws in France. The registration process requires the employer to indicate clearly the process, scope and purpose of the monitoring. Additionally, before any monitoring activities are set in place, employees must be notified of any such procedures that may affect them

(Labor code, Art. L. 121-8). Such notification must be made in writing such as an internal memorandum, statement in the company rules and regulations or in the terms of the contract of employment.

The French law also discusses when monitoring is justified. If the company has reason to believe that, in view of the duties and responsibilities held by an employee, he or she could potentially undermine the integrity of company systems or otherwise act against the company's interests such as by making it vulnerable to a security breach affecting confidential data, inflicting damage on the computer systems, causing technical disruptions or exposing it to the risk of incurring liability toward third parties as a result of a data transfer. (Labor Code, Art. L. 120-2), then monitoring is justified.

If the monitoring will involve personally identifiable information, making it possible to identify employees directly or indirectly, the employer must comply with the provisions of the French law on data protection and privacy.

Bottom Line under French Law: French law specifically applies the principle of proportionality: workplace monitoring is justified only if it is necessary to protect the legitimate business needs of the employer; and goes no further than is necessary to meet that need. The French laws are important for those companies established in France or with offices or employees in France. The laws also apply to U.S. companies that receive and process employee information of affiliates or subsidiaries in France.

Germany

Historical antipathy to monitoring

Data processing in Germany is generally governed by the Federal Data Protection Act (the "FDPA") and by the federal constitution. The FDPA applies to all types of data processing activities that are carried out in Germany, including those in the workplace. The FDPA contains no specific references to privacy in the workplace and, as a result, privacy in the workplace is to a large extent shaped by the case law of the labor courts which have, through a series of individual cases, outlined the general principles of "employee data protection."

The employer is generally entitled to monitor the use of the company's network, the Internet and e-mail. The employer's right to monitor, however, must be weighed against the employee's privacy rights. The employees should generally be informed from the beginning of the type, purpose and extent of monitoring that will take place. (Section 81(1) German Works Constitution Act). It is sufficient to generally announce that monitoring is to be expected in the workplace. For business e-mails, monitoring is generally permissible to the full extent so that the employer

is able to monitor the activities of the employees. For private e-mails, the employer is allowed to monitor the contents of private e-mails only if there is substantial suspicion of breach of contract, misuse of company assets or a criminal offense.

In Germany, the role of the Works Councils[5] must be considered. A Works Council is legislatively created entity comprised of a group of employees with whom management of companies with over more than 150 employees must inform and consult regarding certain decision affecting employees. Not all companies have works council, but where they are established in Germany, they have the right of co-determination with respect to the introduction and use of technical systems that monitor employees. If there is no Works Council in a particular company, then consent must be obtained from employees before monitoring can take place.

Bottom Line under German Law: Information obtained during monitoring must only be used for specific purposes and must be limited to what is necessary to accomplish the legitimate purposes for monitoring. Under German law it may be necessary to involve the Works Council in the decision to employ monitoring technology and, therefore, it is important to be able to demonstrate that the monitoring is effective and is subject to safeguards that protect an employee's privacy.

Other European Countries

Very little case law to guide employers

In a number of European countries, the employee's right to privacy is enshrined in the country's constitution and such a fundamental right limits the employer's ability to monitor in the workplace, primarily where e-mail content is concerned. In addition, employers must often have regard to the rights of workers representatives to be consulted regarding the introduction of any monitoring.

In a number of the E.U. Member States, there is very little case law or established practice regarding workplace monitoring. In Sweden, the monitoring of e-mails is regulated by the Penal Code and the Data Protection Act. In Italy, workplace monitoring is regulated by the Personal

[5] Works councils were implemented pursuant to Council Directive 94/45 on the establishment of a European Works Council or a procedure in Community-scale undertakings and Community-scale groups of undertakings for the purposes of informing and consulting employees.

Data Protection Code. In Sweden, the Netherlands, and Denmark, monitoring with certain conditions is lawful.

If there is no specific legislation governing workplace monitoring, then the country's general data protection legislation will control. Each Member State is required to enact data protection legislation in compliance with the E.U. Data Protection Directive. This Directive has established general principles for privacy that are common throughout the European Union, including the newest Member States.

In the absence of clear legislative guidance, companies should consider the take steps to protect themselves before undertaking monitoring.

Table 1 below provides a checklist that should be considered by companies considering monitoring in Europe.

Table 1

Recommended Steps to Consider Before Monitoring

#	Recommended Step	Comment
1	Draft a policy that allows the company to monitor employee's network communications such as e-mail, Web mail, or instant messaging, if certain conditions are met.	Ensure that policy is carefully written and specific. Companies normally set forth the purpose for monitoring in a "Network Use" policy, and "Employee Privacy Policy," a "Customer Data Privacy Policy" or other similar policies. It may also be included in an employee handbook.
2	Consider obtaining specific employee consent to monitoring.	While it may not be legally required to obtain consent, obtaining it should give full legitimacy company's practices.
3	The notice should provide a clear description of the purposes for monitoring and why it is necessary.	State that the network, Internet and e-mail are company assets provided uniquely for work purposes and which, therefore, should not be used for any other purpose.
4	The notice should generally describe how monitoring will be performed.	Information such as this is important for an employee's consent to be "informed" consent.
5	Management should understand how the monitoring technology works and what audit trails, if any, are provided.	Among unions in Europe, there has been concern raised that if employer's monitor employee's e-mail without the presence of a workers' representative or independent third party, this would permit employers who want to get rid of certain employees to "fabricate" evidence of improper use of e-mails. Providing an audit trail and securing the data captured during the monitoring is an important step in addressing this concern.

Transborder Transfers of Personal Data

One of the more controversial aspects of the E.U.'s Data Protection Directive is the limitation imposed by Article 25. Article 25 provides that Member States shall ensure that personal data can be transferred to third countries (such as the United States) only if those countries provide "adequate level of protection" for the personal data. Article 26 of the Directive provides that data can be transferred to non-E.U. countries if they provide adequate protection or if the following conditions are met:

> (1) The data subject has given his consent unambiguously to the proposed transfer, or
>
> (2) The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request, or
>
> (3) the transfer is necessary for the conclusion or for the performance of a contract concluded in the interest of the data subject between the controller and a third party, or
>
> (4) The transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims, or
>
> (5) The transfer is necessary in order to protect the vital interests of the data subject, or
>
> (6) The transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest.

Article 26 also provides that transfers of data to a third country that does not ensure an adequate level of protection can take place if the personal data will be protected by appropriate contractual clauses or by such arrangements as the U.S. /E.U. Safe Harbor Agreement[6] or binding corporate rules.[7] The U.S. / E.U. Safe Harbor Agreement is an important way for U.S. companies to avoid experiencing interruptions in their business dealings with the EU or facing prosecution by European authorities under European privacy laws. Certifying to the Safe Harbor will

---

[6] For additional information on the Safe Harbor program, visit the special Website which has been set up by the U.S. Department of Commerce at http://www.export.gov/safeharbor/.

[7] For additional information on the binding corporate rules, visit the European Union's Website at www.europa.eu.int.

assure that EU organizations know that your company provides "adequate" privacy protection, as defined by the Date Protection Directive.

Companies joining the Safe Harbor program must meet strict standards for protection of privacy. Another method of allowing the transfer of personal data is through "binding corporate rules." Binding corporate rules can be used by a multinational company or a group of companies as a mechanism to transfer personal data throughout the organization, even though some of the transfers may be made outside of the European Union.

Companies that opt for Safe Harbor or binding corporate rules must undertake a careful assessment of their personal data use – particularly where personal information is being gathered through workplace monitoring. Neither Safe Harbor nor the binding corporate rules replace the requirement to comply with the data protection laws of the individual Member States.

The restrictions on the transfer of personal data can come into play where a company operates within the E.U. but transfers the data collected during monitoring to the United States. If one of the compliance methods cannot be met, then it may be necessary to either restrict the transfer of data outside of the E.U. or mask or de-identify the data before it is transferred outside of the E.U. [8]

V. How Vontu Effectively Safeguards Employee Privacy

In developing its technology, Vontu clearly has given considerable thought to helping its customers effectively monitor the use of sensitive information while safeguarding employee privacy. Vontu's technology accomplishes this in a number of ways:

1) **Comply with Notice and Policies**: Vontu enables companies to comply with their privacy notices and policies. Vontu does this through policy-based monitoring.

2) **Legitimate Purposes and Proportionality**: Vontu ensures that data collected during monitoring is only used for legitimate purposes. Vontu enables companies to collect only data that violates policies, and then enables companies to ensure that

[8] Simply masking data may not be sufficient to enable the transfer outside of the E.U. The Data Protection Directive continues to protect data if it can be used to identify a particular individual.

only those individuals with a "need to know" have access to the collected data.

3) **Targeted Monitoring**: The fair information practice principles and the principles set forth in the European Union's Data Protection Directive require companies to collect data for legitimate purposes and then collect only such information that is proportional to the company's purpose for data monitoring. Vontu accomplishes this in several ways. First, Vontu safeguards employees' privacy by treating the sender's identity as "need-to-know." Second, Vontu collects only data that violates stated policy. And third, Vontu limits access to collected data to individuals who are approved to receive it.

4) **Data Integrity/Accuracy**: Collecting information that does not violate policy or information on the wrong individuals increases a company's privacy risks. Vontu has greatly reduced these risks by keeping false positives near zero.

5) **Security**: Vontu provides security for the data that is collected by providing secure communications of incident data. Additionally, Vontu provides for role-based access to incident information and a complete audit trail.

6) **Enforcement**: Vontu provides an audit trail for all information gathered during monitoring. Significantly, Vontu maintains the integrity of audits by logging changes to policies and all activities taken in response to an incident.

7) **Access**: Vontu's audit trail enables companies to easily provide individuals or Works Council representatives with access to specific information.

This section will examine some of Vontu's key functions that safeguard employee privacy while protecting against the loss of sensitive information.

Limits the Disclosure of Personal Information: "Need to Know"

Privacy laws and regulations apply to information that can be associated with a particular individual. If the information is anonymous or if the information is not otherwise tied to a particular individual, the risks of violating an employee's privacy rights are greatly reduced.

Vontu Monitor detects confidential information before it leaves the network over e-mail, instant message or the Web. Vontu Prevent stops

confidential information from leaving the network and prevents internal security breaches before they occur. If a transaction is identified as a violation of the company's policies, it is cached and stored on the Vontu Monitor. This automatically triggers a transaction to Vontu Enforce by providing basic information about the policy violation. The identity of the sender, however, does not have to be disclosed. The identity of the sender can be restricted to those the company has determined have a legitimate "need to know." Vontu can also send a message to the sender that a policy violation has occurred.[9]

Vontu can also be configured to comply with the transborder data transfer restrictions of the European Union. Vontu's Monitor and Enforce can be set up so that they reside in one location within the E.U. Accordingly, data collected during monitoring does not travel across national boundaries or outside of the E.U.

Legitimate Purpose and Proportionality: Policy-Based Monitoring and Focus on Specific Activities

The principles of legitimate purpose and proportionality provide that monitoring is justified only if it is necessary to protect the legitimate interests of the employer and the monitoring goes no further than is necessary to meet that need. A company usually discloses the legitimate purpose in documents such as a "Network Use" policy, an "Employee Privacy" or "Customer Data Privacy" policy.

Vontu automates policy enforcement options for notification, workflow, blocking, quarantine and encryption. Vontu allows users to define and deploy data security policies based on over fifty pre-built policy templates for protecting customer data, intellectual property and company confidential information.

The focus on specific activities and policy-based monitoring helps avoid additional compliance and privacy exposures. It enables a company to provide notice of exactly what is being monitored and what is being collected. Vontu's match highlighting gives the company a clear indication of why a communication generated an incident, saving time in the incident review process and ensuring that data collected is limited to that which violates policies.

[9] Notice to the originator of the e-mail can play an important role in establishing notice under both U.S. and E.U. data privacy laws. In Europe, this can be the event that alerts an employee that his or her communication has been recorded as an incident and, therefore, triggers any rights they may have to access the data collected about the violation.

Collects Only Data that Violates Policy

Vontu monitors data flowing across a network but **only** collects data if it violates company policy. This is a significant step in protecting employee's privacy rights. Whereas some monitoring technologies capture all data – even that which does not violate policy, Vontu does not. Some of Vontu's competitors enable companies to run queries against all of the captured data in an effort to find violators. This is a clear violation of the principle of proportionality and one that Vontu does not allow.

Data Accuracy and Integrity: Limits False Positives

Vontu's patent-pending technology accurately detects confidential data across all network protocols, content formats and business contexts. Accurately identifying information that violates policy is key in reducing false positives.

Vontu's Exact Data Matching delivers a high degree of accuracy on structured data. This is essential for protecting customer and employee data. Vontu's Indexed Document Matching creates "digital fingerprints" on unstructured content, enabling accuracy. And finally, Vontu's Described Content Matching uses keywords, lexicons, pattern matching (regular expression), file types, file sizes, sender, receiver and network protocol information to detect data loss incidents.

Security for Data Collected

Vontu has provided numerous features to safeguard the data that is gathered during monitoring. To begin with, the information on violations is revealed to first responders or analysts through a secure visual display. In order to protect this information during transmission, Vontu uses a secured communication channel or encrypts the information being sent. Vontu's stored (cached) documents and summary reports reside within a company's secure corporate LAN and the information is not transferred to outside parties.

Vontu also allows a customer to determine who should see specific information on incidents. The role-based access controls are important to minimize risks of the improper use of sensitive information. A customer can limit access to sensitive information or sender identity to departmental supervisors or others who should have access to such information.

Access and Enforcement: A Comprehensive Audit Trail

One significant aspect of privacy protection is ensuring that an audit trail is kept of the collection and use of information. Additionally, the audit trail should keep complete records on any changes to policies as well as steps taken as a result of the incident. Vontu keeps detailed logs and accurately timestamps and records the information necessary to resolve disputes. Further, Vontu preserves evidence that may be needed for later use in the event of intentional violations.

Vontu keeps complete data on all incidents for purposes of an audit trail. Significantly, Vontu enables customers search historical data based on sender, policy, recipient and other relevant factors. This can be adjusted to comply with the E.U.'s restrictions on how long personally identifiable data can be retained.

VI. Grading Vontu's Safeguarding of Employee Privacy

At the outset of this paper, it was noted that effective management of workplace privacy issues requires a multi-faceted approach. Companies must educate themselves on the requirements of both U.S. and E.U. laws governing workplace monitoring. Companies must also put in place effective policies and procedures to regulate monitoring and to reduce employees' expectation of privacy for workplace communications. One important element is the adoption of the Vontu solutions that will enable companies to comply with their policies, protect their sensitive information while safeguarding employee privacy. Vontu is such a technology and provides reasonable steps to protect and secure data that is gathered as a result of targeted monitoring. Vontu receives high marks for its effort to provide its customers with effective tools for safeguarding employee privacy while providing effective monitoring.

Table 2 below provides a score card to determine how Vontu meets the fundamental privacy principles underlying workplace monitoring. It contains a listing of the basic fair information practice principles of the United States and the relevant principles from the European Union as they relate to monitoring.

Table 2		
Monitoring Requirements Under E.U.		
Requirement	**How Vontu Meets Requirement**	**Yes/No**
Notice: Companies must notify individuals about the purposes for which they collect and use personally identifiable information. Notice may also require information on who is collecting the data, how it is being collected, where it will be processed and when.	Companies must notify individuals about the purposes for which they collect and use information. Although Vontu does not provide the actual notice, companies can use Vontu to ensure that monitoring takes place in compliance with the stated purposes in the notice and, therefore, that the information in the notice is accurate. Companies most often get into trouble for stating one thing in their privacy notice and then doing something different in practice. The ability to use technology to aid in complying with a company's privacy policies is an important step in reducing privacy risks.	Yes
Legitimate Purpose:[10] Data collection must be necessary to protect the legitimate business needs of the employer. A company should carefully spell out its business reasons for data monitoring. In the U.K., for example, an employer must also conduct an assessment before monitoring in order to ensure that the steps being taken are reasonable and that the data collected will aid in achieving the objectives set by the company.	Vontu provides pre-built templates to assist customers in complying with privacy laws and best practices. Vontu provides policy-based monitoring to ensure that monitoring and data gathering only target information that violates the company's policies. These are important steps in ensuring that a company is conducting monitoring for legitimate purposes and collecting only relevant information.	Yes
Targeted Monitoring: The method of monitoring must be targeted to collect data for specific purposes and companies should use the least intrusive monitoring possible.	Vontu accomplishes this in a number of ways. First, Vontu only collects information that is determined to violate policy. Second, Vontu allows first responders or analysts to review incidents without revealing the sender's identity or message content. The ability to target specific data and then strictly limit who sees such data are important privacy safeguards.	Yes

[10] "Legitimate purpose" is different than "reasonable and proportionate." The "legitimate purpose" requires a company to ensure that its purposes for data collection are allowed under relevant laws. The "reasonable and proportionate" principles ensure that a company limits the data collected to only that reasonably necessary to achieve the legal purpose for collecting data.

Table 2		
Monitoring Requirements Under E.U.		
Requirement	**How Vontu Meets Requirement**	**Yes/No**
Reasonable and Proportionate: The information gathered during monitoring must be reasonable and proportionate to the purpose for collecting.	One of the reasons that the U.K. requires an assessment prior to undertaking monitoring, is to ensure that a company understands what data should be gathered during monitoring and that monitoring is conducted in the least intrusive manner possible. Vontu aids businesses in achieving these goals by targeting only data that violates specific policies. Unlike some of its competitors, Vontu does not gather all employee communications into one large database for subsequent analysis.	Yes
Data Security: The information gathered must be protected from unauthorized use, access, alteration or destruction.	Vontu allows role-based access to incident information. Vontu provides a complete audit trail of incident workflow. Finally, Vontu provides secure communication of the incident data.	Yes
Comply with Policy: The monitoring must comply with the notice given to employees.	Vontu's policy-based monitoring allows companies to ensure that only non-compliant data is collected. This allows a company to set its policies and then feel comfortable that the monitoring is being limited to that related to the company's policies.	Yes
Specific Use of Data: The information gathered during monitoring must be used only for the stated purposes.	Vontu's audit trail records all workflows related to an incident – including who accessed personal information. Vontu's role-based access security enables individuals to see only what there is a "need to know."	Yes
Data Accuracy: The information gathered during monitoring is accurate.	Vontu's patent-pending detection technology delivers a high degree of accuracy across all types of data.	Yes
Access: Individuals must be given reasonable access to all personal information held about them.	Vontu's audit trail maintains a complete record if an incident workflow and all information related to the message that violated policy. Companies can easily provide employees or works council representatives with access to information on the violation.	Yes
Data Integrity: Steps must be taken to ensure that data is accurate and relevant for the purpose(s) for which it was collected.	Personal information must be relevant for the purposes for which it is to be used. Vontu's accuracy and policy-based monitoring help ensure the data gathered is relevant for stated purposes.	Yes

Table 2		
Monitoring Requirements Under E.U.		
Requirement	**How Vontu Meets Requirement**	**Yes/No**
Enforcement: Measures must be put in place to ensure that data is used appropriately and that the policies regarding the use of the data are enforced. Effective enforcement includes an audit trail of how data is used to ensure that individuals who violate privacy policies are dealt with appropriately.	While Vontu will not provide the actual dispute resolution mechanism, it does provide the audit trail and records necessary for an effective dispute resolution program. Since all information related to an incident is captured and logged, along with changes to the relevant policies, employees or works council representatives can have confidence that the information is accurate and that it has not been "manufactured." If information has been inappropriately used, the Vontu audit trail will enable companies to appropriately deal with the individuals who have violated the relevant policies.	Yes

Table 2 provides only a starting point for you to consider before monitoring employees within the European Union. Because the laws and regulations vary from country to country, it is important that you understand the laws related to each country where you are doing business. It is also very important to understand the cultural and historical perspectives of each country regarding monitoring and privacy. For many Europeans, privacy is viewed as a fundamental right that must be protected. In addition, it is important that you understand the technology that you will use to conduct monitoring, as its effectiveness and reliability can have an impact on the privacy risks you may be facing. Monitoring technology that provides safeguards to protect privacy rights of employees is an important step in managing privacy risks.

VII. Conclusion

Monitoring has become an important part of the steps that companies must consider in order to protect their sensitive information. As discussed throughout this paper, monitoring can be used to protect the company's intellectual property as well as to protect against the leaking of customer or employee data. In order to effectively manage the risks related to the loss of sensitive data – without creating new risks by improper monitoring, companies must implement a multi-faceted program. Such a program must address the complex privacy and data protection laws of the United States and the European Union. An important part of any such program is the implementation of technology that provides management with an effective tool in dealing with workplace monitoring and privacy issues. Vontu technology is such a technology that should be considered by companies with international operations.

VIII. About the Author

Gary Clayton is the founder and CEO of Privacy Compliance Group, Inc., a leading privacy and data protection consulting and technology company. Privacy Compliance Groups helps organizations establish effective privacy compliance programs and to develop practices and policies to comply with privacy laws around the globe.

Gary Clayton has worked with leading companies around the world and with numerous agencies of the U.S. Government, including the Department of Homeland Security, the Department of Transportation, the General Accounting Office and the Federal Trade Commission. He has extensive experience in all aspects of privacy and has been actively involved in working with clients in over 55 countries. Mr. Clayton has worked in the European Union and assisted the U.S. Department of Commerce in negotiations with the European Union on the Safe Harbor agreement and the Department of Homeland Security in negotiations regarding access to passenger data.

Mr. Clayton is an attorney who is admitted to practice in Washington, D.C., Texas and Louisiana. He has lived and studied in Europe where he received an advanced law degree (LLM) in European and International Law from the University of Exeter, England. He has also attended the law school at the university in Grenoble, France. He is a frequent author and speaker on global privacy and data protection issues. He can be contacted at gclayton@privacycg.com.