mdpc medical device privacy consortium

September 25, 2014

WHITE PAPER

SECURING THE ENTERPRISE IN A PRIVACY-RESPONSIBLE MANNER

Good security practices are essential for maintaining an enterprise's value and maintaining the privacy of personal data in a world of high-speed digital information flow. However, data security measures can substantially invade personal privacy rights if not applied with care and forethought. Procedural and technical security measures must respect core privacy principles, especially when monitoring the activity and behavior of users and information storage and transmission. In this paper, we examine some common methods of monitoring the enterprise and the privacy principles that should govern such security measures. We go on to recommend a governance framework for ensuring responsible security by means of an enterprise Security and Privacy Board appointed to responsibly balance emerging threats with the privacy needs and obligations of the enterprise.

Introduction

Technology is constantly changing the workplace. To create and preserve value, enterprises use technologies that maintain, collect, process, and transmit confidential data relating to commercial products, workers, customers, and business partners. Because of the value of this information, information technology (IT) systems are increasingly being attacked by those who would illegally profit from stolen information. Such crime is a serious threat to a business's core activities and diverts staff and resources that would better be deployed toward growth and product improvement. Countering criminal activity requires ever more sophisticated methods of protection to ensure continued operation and preservation of enterprise data.

In tandem with these technological developments and threats, data security and privacy regulations are expanding and changing in an effort to keep pace. Over 65 countries now have data protection laws regulating the collection, use, transfer, and disclosure of personal information. Compliance with data security and privacy requirements is becoming especially complicated for global enterprises facing multiple and varied legal regimes. The repercussions of non-compliance extend beyond regulatory sanctions and can have a negative impact on brand, operations, competitive advantage, consumer trust, and worker morale and retention.

Accordingly, new data security technology is being developed to meet these increasing data protection requirements and cybercrime realities. With the right technology, enterprises can control the risk associated with maintaining confidential and private information. However, as many of these security measures require a detailed supervision of business operations, enterprises must be careful to avoid intruding on worker privacy. Importantly, there is a highly developed right of privacy in the European Union and increasingly so in the United States. Enterprises operating in these regions must determine how such privacy rights apply in the workplace. Here, we discuss the competing values of enterprise security and worker privacy and suggest best practices for industry.

I. THE BALANCE OF SECURITY MONITORING: RETAINING VALUE AND WORKER PRIVACY

Enterprises have incentive to know what is happening with their confidential and protected information at all times for purposes of retaining commercial value and complying with data security regulations. Accordingly, enterprises may implement any number of security measures that capture data relating to workers, business partners, and customers, and can be viewed as invasive. For example, surveillance of a worker's whereabouts and internet usage to monitor security protocols can be misused by an employer for performance monitoring and may result in a conflict where security mechanisms protect the confidentiality of enterprise data but invade the privacy of workers. As stated by the European Union's Article 29 Data Protection Working Party, "workers do not abandon their right to privacy and data protection every morning at the doors of the workplace."[1] Under privacy regimes in many regions, there are limits to processing personal data even for purposes of legitimate investigation of a breach or other enterprise security issue. However, though worker privacy rights must be held in high regard, it is universally accepted that these rights must be balanced to some degree against the employer's interests.

Below, we provide two examples of the intersection of security monitoring and privacy. In the course of operation, nearly all businesses suffer loss due directly to criminal activity perpetrated by workers, customers, partners or outsiders. Crime detection and prevention techniques can prevent direct loss and mitigate indirect loss where failure to implement reasonable safeguards to prevent criminal activity is itself a violation of the law. Each of the following two categorical anti-crime surveillance practices presents distinct challenges to personal privacy.

a. Surveillance to Prevent Loss.

Surveillance to prevent loss identifies and intervenes in crime before losses occur. Such surveillance may identify potential criminal activity, engage a response process, and record the activity for subsequent investigation and prosecution. For example:

- Monitoring for abnormal patterns of access to sensitive information
- Monitoring use of copy and file transfer functions in applications or computer systems
- Monitoring transactions and transaction patterns for evidence of crime
- Monitoring purchasing or expense recovery patterns for evidence of fraud

These surveillance techniques are necessarily non-discriminatory when used to generally identify and collect information about people and environmental metadata. By their nature, however, these techniques capture and retain vast amounts of information about non-criminal activity, including personal information such as name, likeness, biometric data, IP address, home address, gender, marital status, financial information and other personal attributes. Accordingly, it is important that these techniques collect only the personal information necessary for the loss prevention objective and destroy information not attributable to a potential criminal act.

[1] Art. 29 Working Party Working document on surveillance of electronic communications in the workplace (2002) (hereinafter Working Document on Surveillance), p. 4.

b. Surveillance to Investigate Crime.

Once a potential crime is detected, incremental investigative and surveillance techniques are frequently employed to gather additional evidence. Computer forensic investigations work to produce evidence proving the pattern of facts. This frequently begins with a larger volume of information that is progressively reviewed and narrowed by relevance. The process is typically non-linear in the sense that evidence gathered during an investigation frequently leads to a progressive increase in collected information before it pinpoints the information necessary to establish the pattern of facts. Common characteristics of forensic investigations implicating personal information include:

- Full collection of the entire contents of all computer system hard drives or email records. Establishing relevance typically begins with an inspection of all content before narrowing begins.
- Full content inspections can lead to the identification of criminal activity not initially the subject of the investigation.
- Investigations routinely span connections between multiple computers. It is common that the number of machines inspected grows quickly during the initial phase of the investigation.
- Certain malware are self-propagating and can move from one computer to another without user assistance or knowledge. Investigations of this type require inspection of user computers, even when the users themselves are not the subjects of the investigation.
- Legal defense of evidence is often best facilitated by preservation of the complete initial collection. That typically results in the preservation of information not directly relevant to the crime being investigated.

While more focused than loss prevention surveillance, forensic investigative techniques still capture and retain information unrelated to the criminal activity in question. This is especially true when investigations include the computers of users that are victims of computer crime. User personal information such as name, likeness, biometric data, IP address, home address, gender, marital status, financial information and a host of other sensitive personal attributes are likely to be present on the computer. Such information may have been the target of the computer crime and thus helpful in preventing subsequent identity theft. Computer forensic investigators are challenged to limit collections appropriately and to protect collected information from inappropriate disclosure. Where the evidence demonstrates reasonable belief that a crime has occurred, collected materials are generally turned over to law enforcement.

II. RANGE OF SECURITY MONITORING PRACTICES

Businesses have a number of security mechanisms at their disposal, each of which poses a different threat to worker privacy. Some of the more prominent security measures are:

Identification and Authentication Mechanisms. Identification and authentication mechanisms determine a worker's presence and location at the workplace. Such tools can include keystroke

dynamics or smartcards used to authenticate access to secure areas. These measures can raise privacy concerns as they allow the tracking of a worker's personal movements and contact with other workers. Another concern can arise if the identification and authentication uses biometrics.

Access Control. Businesses may also control data by maintaining access control lists which assign security levels to users and objects and require the storage and usage of information about a worker's access rights. Providing a worker with a certain level of security clearance will often require a personal background check. Thus, such access control data reveals personal information about a worker's status and personal background.

Geolocation Monitoring. In addition to access controls and other on-premises monitoring, it may be possible for employers to monitor worker activity through geolocation monitoring through cellular equipment or a GPS system installed in a company vehicle. Both U.S. and EU privacy authorities have recently begun to consider restrictions on accessing an individual's geolocation data.[2]

Auditing and Post-hoc Intrusion Detection. Through an audit or security forensic investigation, a company will produce information about the activities and behavior of systems and persons (often workers) who use company technology and facilities. If the audit or investigation of a user involves other individuals, the audit trail may also contain private information about these individuals. Detailed auditing or investigation can involve statistical profiles on the behavior of users which can be used to understand worker behavior and control future behavior.

Information Back-up and Retention. For purposes of maintaining records, companies often have backup files which may contain personal data stored on a system at backup time. Many privacy acts include a right to correct erroneous personal data contained in a record. However, these corrections are not likely executed on any backup files, and, therefore, backup files may retain erroneous personal data, in conflict with the data subject's privacy rights.

E-mail, Chat, Collaborative Sites, Social Networking, and Desktop Monitoring. E-mail, chat, collaborative sites, and social networking sites are now the standard modes of conducting business. Accordingly, a significant portion of a business's sensitive data will likely be exchanged through these means. As a result, each is a potential vector for data loss and becomes a focal point for employer monitoring. E-mail monitoring is a common practice and is generally done through software programs which track the content, timing, volume, and recipients of sent and received e-mail. These programs can even track personal, Web-based e-mail accounts.

Keystroke Monitoring and Screen Shots. In addition, desktop monitoring programs can capture commands and keystrokes which a worker sends to the desktop or capture images of a worker's desktop screen. Programs can translate keystroke signals and provide this information to the employer. This sort of detailed collection of personal information is particularly invasive as the employer may be able to capture account numbers and passwords.

---

[2] *See, e.g.*, Geolocation Privacy and Surveillance Act of 2013, S. 639, 113th Cong. (U.S.); Art. 29 Working Party Opinion 13/2011 on geolocation services on smart mobile devices (EU).

Internet Use Controls. Filters and firewalls allow an enterprise to both prevent outsiders from gaining access to internal systems and also prevent workers from accessing inappropriate, illegal or malicious external content and systems. Alternatively, internet use audit systems can track a worker's Web activity over time. Employers may thereby utilize this technology to determine worker productivity and check for inappropriate activities.

Data Loss Prevention. Data loss prevention systems are designed to detect and prevent data breaches by monitoring, detecting, and blocking sensitive data. This monitoring, detection and blocking can occur on computer endpoints, networking devices, and data storage systems. Data is monitored to detect inappropriate transmission or storage of private company information or intellectual property. The most common monitoring points are data at rest (storage systems and client computer storage), data in internal transit (network interfaces), data leaving client device hardware ports (USB, Firewire, eSATA, etc.), e-mail clients and major system interfaces (laptop e-mail programs, virus/content scanners, e-mail bridges), and internet work interfaces (enterprise internet gateways, collaborative partner gateways). Personal data may be encountered in this process and thus privacy compromised.

Security Information and Event Management (SIEM). SIEM systems are an IT security infrastructure tool that provides a holistic view of an organization's information technology security by collecting logs and other security-related documentation from multiple different locations for analysis from a single point of view. Most SIEM systems deploy collection agents to gather security-related events from end-user devices, servers, network equipment and security equipment. The collection and analysis of these data permit the detection of subtle patterns that might indicate malicious activity. Additionally, when a security breach is suspected, the SIEM can determine the exact sequence of events to give a proper understanding of the weaknesses. Of course, any aggregation of log data contains an abundance of personal information on the usage patterns of individuals and therefore has a negative impact on privacy.

Behavioral Monitoring. This monitoring involves the collection of individual user activity data that allows enterprises to monitor workers. Information on workers' activities and use of enterprise property allows the enterprise to conduct general business oversight and assure regulators that workers are operating within the bounds of law. This technology can be used, for example, to determine when a worker who has logged into an account at their office in London is later seen to log in from a café in Singapore, or where a worker accesses or downloads volumes of customer records in an unusual manner. Such monitoring necessitates scrutiny of everyday practices and behavior of workers and therefore infringes on their privacy.

III. PRINCIPLES OF PRIVACY REGULATION

a. Privacy Protection Principles in Europe

Principles underlying the European approach to worker privacy can be found in the European Convention for the Protection of Human Rights and Fundamental Freedoms. Article 8 states that everyone has a right to privacy of private life and correspondence. From this provision, the EU's Article 29 Data Protection Working Party (Working Party) expounded the following principles:

(1) Workers[3] have a legitimate expectation of privacy at the workplace which is not overridden by a worker's use of the employer's business facilities (though notification of monitoring practices by the employer may reduce the expectation of privacy);

(2) The general principle of secrecy of correspondence covers communications at the workplace (likely including e-mail and files attached thereto); and

(3) Respect for private life includes the right to establish and develop relationships with other human beings. The fact that such relationships take place at the workplace must be balanced against an employer's legitimate need for surveillance measures.[4]

Currently, there is no pan-EU legislation specifically protecting the personal data of workers. However, Data Privacy Directive 95/46/EC (Directive) protects all individuals with regard to the processing of personal data.[5] Beyond this, many EU Member States have implemented legislation or drafted industry codes which apply the Directive's data protection principles—legitimacy, finality, transparency, proportionality, confidentiality, security, and control—to the specific context of worker privacy.[6] The Working Party has not provided insight into what data processing is permitted but has stated that "the level of tolerated privacy's intrusion will very much depend on the nature of the employment as well as on the specific circumstances surrounding and interacting [sic] with the employment relationship."[7] EU employers may also consider consulting with trade unions or works councils before changing monitoring practices if the employer is bound by a collective bargaining agreement or employment standard.[8]

b. Privacy Protection Principles in the United States

The U.S. legal system approaches worker privacy differently than the EU system. There is no generally applicable protection of worker privacy in U.S. law. Workers in the U.S. have a low expectation of privacy at the workplace.[9] In fact, monitoring of worker use of employer-provided communication

---

[3] While the Working Party does not define "workers," the principles appear intended to extend to a broad category of those who work within the enterprise.

[4] Working Document on Surveillance, p. 8.

[5] In addition, Directive 2002/58/EC on Privacy and Electronic Communications addresses the processing of personal data and the protection of privacy in electronic communications.

[6] *See* Art. 29 Working Party Opinion 8/2001 on the processing of personal data in the employment context, adopted on 13 September 2001 (hereinafter Opinion 8/2001) (enumerating national data protection legislation applying to the employment context).

[7] *Id.*

[8] In the EU, Directive 94/45/EC, as later revised by Directive 2009/38/EC, establishes European Works Councils for purposes of ensuring that workers are provided information and the right to consultation with employers at companies whose operations span the EU community. In addition, national law of EU member states may require consultation or co-decision-making with a domestic works council.

[9] *See, e.g.*, U.S. v. Simons, 206 F.3d 392 (4th Cir. 2000), cert. denied, 534 U.S. 930 (2001) (holding that a defendant did not have a reasonable expectation of privacy in his computer or office since he was violating his employer's policy and the law); Smyth v. The Pillsbury Co., 914 F. Supp. 97 (E.D. Pa., 1996) (finding that a worker had no reasonable expectation of privacy in e-mail communications voluntarily made to his supervisor over the company e-mail system).

systems is viewed as a responsible business practice. Failure to investigate internal activities may even expose the employer to liability.

The limited scope of the right to privacy can even mean that communications relating to personal rather than work matters may not be protected in a workplace setting.[10] This is particularly true where the employer has notified the worker of a policy of inspection or monitoring. The Fourth Amendment to the U.S. Constitution provides government workers some protection in the workplace; however, this protection is limited and highly contextual and requires the worker to show a "reasonable expectation" of privacy based on the circumstances of his workplace.[11] The Fourth Amendment only applies when the government acts and therefore does not extend to private-sector workers.

Title III of the Omnibus Crime Control and Safe Streets Act (the Wiretap Act) prohibits the intentional interception of any wire, oral, or electronic communication by public and private actors, including private-sector employers.[12] However, the Wiretap Act's protection of workers is limited as the law does not prevent interception by certain devices of communications made in the "ordinary course of business" or when one party to the communications consents to the interception.[13] Accordingly, worker communications conducted at the employer's location and on the employer's devices could be considered communications in the "ordinary course of business" and a worker may be interpreted to have implicitly consented to such interception.

Workers could argue that monitoring practices constitute a common law tort of invasion of privacy; however, this claim also depends on proof of an expectation of privacy, and it is generally accepted that workers have a decreased expectation of privacy in the workplace.[14] Finally, some states have adopted

---

[10] *See, e.g.*, U.S. v. Hamilton, 701 F.3d 404 (4th Cir. 2012) (finding that a defendant was not entitled to a communications privilege after failing to protect emails despite being informed of employer policy permitting inspection); U.S. v. Barrows, 481 F.3d 1246 (10th Cir. 2007) (finding a city treasurer did not have a reasonable expectation of privacy in files on his personal computer when he brought the computer to work and connected it to the city's computer); McLaren v. Microsoft Corp., 1999 W.L 339015 (Tex. App. Dallas 1999) (finding that a worker had no legitimate expectation of privacy in a folder stored on a company-owned machine and emails sent over the company network); *Smyth*, 914 F. Supp. 97 (holding that worker termination for sending inappropriate email over employer's system was not an invasion of privacy despite employer's prior assurance that worker email would remain confidential).

[11] Lawrence E. Rothstein, *Privacy or Dignity? Electronic Monitoring in the Workplace*, 19 N.Y.L. SCH. J. INT'L & COMP. L. 379, 400 ("Thus, the government employer's control of the premises and the equipment, the implied consent of the worker who is generally informed that monitoring might take place and the balancing of the magnitude of the intrusion into the worker's control over personal intimacy or information against the business necessities and efficiency of the public employer all combine to greatly limit a government worker's reasonable expectation of privacy.").

[12] 18 U.S.C. §§ 2510-2712 (2002).

[13] *Id.* §§ 2510 (5)(a); 2511 (2)(d).

[14] *See, e.g.*, Hernandez v. Hillsides, Inc., 47 Cal. 4th 272, 288 (Cal. 2009); Marrs v. Marriott Corp., 830 F. Supp. 274, 283 (D. Md. 1992).

statutory regimes that might protect worker privacy interests in certain types of communications.[15] However, such state privacy regimes are generally inconsistent and address only narrow issues.[16]

IV. RECOMMENDED PRIVACY PRINCIPLES APPLIED.

While sound security practices may enhance the protection of personal privacy, if misused or improperly controlled, these data security practices can erode personal privacy. Here, we highlight general privacy protection principles and make specific recommendations that enterprises should consider in constructing a privacy and security regime. These principles and recommendations are derived from the Working Party's interpretation of the Directive[17] and industry best practices:

(1) Necessity. Any monitoring should be justified as necessary for a specified purpose before the monitoring proceeds.
   a. Prior to monitoring, identify specific business benefits that monitoring will bring.
   b. Include specific business justifications in any monitoring policy statement.

(2) Finality. The data must be collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes

(3) Transparency. The employer must be clear and open about monitoring activities to the extent that they are not part of a legal investigation or action by the authorities.
   a. No covert monitoring should take place except where allowed by national law, *e.g.*, with regards to certain criminal activity or upon reasonable suspicion that enterprise assets are compromised.
   b. Give workers notice of data collection practices in the form of a clear, readable expression of the purpose and nature of the processing of personal data. A clearly delineated notice should:
      i. State that the computer system and/or communications services are the employer's property;
      ii. Indicate that the employer reserves the right to monitor electronic communications;
      iii. Explain the business-related reasons for the monitoring;
      iv. Clearly describe permissible and impermissible uses of the employer's computer system and/or communications services and indicate the penalties for violations;
      v. Obtain worker acknowledgment of understanding, where appropriate, and positive acceptance, where permitted, (being mindful of any legal restrictions on coercive consent); and

---

[15] *See, e.g.*, CAL. PENAL CODE § 631; ARIZ. REV. STAT. ANN. § 13-3005; CONN. GEN. STAT. § 53a-188.

[16] For more detail, *see e.g.*, Corey A. Ciocchetti, *The Eavesdropping Employer: A Twenty-First Century-Framework for Worker Monitoring*, 48 AM BUS. L.J. 2, 285 (2011); Justin Conforti, *Somebody's Watching Me: Workplace Privacy Interests, Technology Surveillance, and the Ninth Circuit's Misapplication of the* Ortega *Test in* Quon v. Arch Wireless, 5 SETON HALL CIR. REV. 2, 461 (2009); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006).

[17] Opinion 8/2001, *supra* note 6.

vi. Incorporate results of consultation with workers groups.

c. In the EU, notify supervisory authorities as required before carrying out any wholly or partly automatic processing operation or set of such processing operations.
d. Provide workers with a right to access data which is collected about them.

(4) Legitimacy. Data processing operations must have a legitimate purpose.
   a. Conduct an impact assessment to determine whether the impact on worker privacy is justified by the likely benefits.
   b. In making an impact assessment, seek input from works councils or the workers themselves.
   c. Keep all monitoring work-related and establish a sound and positive business rationale for monitoring.
   d. Fully research and understand what laws limit or regulate worker monitoring.

(5) Proportionality. Data must be adequate, relevant, and not excessive for a specified purpose.
   a. Eliminate blanket monitoring.
   b. Focus monitoring on traffic rather than the content of communications.
   c. Implement business-justified security measures that are least-intrusive to workers.
   d. Allow mail or internet use monitoring only in exceptional circumstances.
   e. Where technically feasible, prevent, rather than monitor, inappropriate use of company systems.

(6) Accuracy and Retention of Data. Keep records containing a worker's personal information accurate and up-to-date.
   a. Take reasonable steps to ensure that inaccurate or incomplete data are erased or rectified, having regard to the purposes for which they were collected or further processed.

(7) Security. Implement appropriate technical and organizational measures at the workplace to guarantee that the personal data of workers is secure.

(8) Governance. Design a leadership structure for managing security and privacy programs.
   a. Identify someone within the enterprise to authorize worker monitoring and ensure workers are aware of the employer's privacy responsibilities.
   b. Keep staff with responsibilities over the processing of personal data of other workers informed of data protection requirements and make sure they receive proper training.
   c. Minimize the number of individuals within the enterprise with access to personal information that is obtained during any security monitoring or investigation.

(9) Freedom of Consent. Consent can only be valid if the data subject is able to exercise a real choice and there is no risk of coercion if he or she does not consent. If the context of the consent undermines the individuals' freedom of choice, consent would not be free. An example is where the data subject is under the influence of the data controller, such as an employment relationship. The Working Party has highlighted that an employer's legitimization of necessary and unavoidable processing of workers' personal data through consent is

misleading.[18] The Working Party suggests that reliance on consent should be confined to cases where the worker has a genuinely free choice and is subsequently able to withdraw the consent without detriment.[19]

(10) Proper Transferring of Data. Ensure that transfers of personal data across borders can only take place where the receiving country ensures an adequate level of protection for the data, or other legally appropriate assurances are in place.

(11) Subsidiarity.[20] Although sometimes grouped with proportionality, subsidiarity is the principle that any necessary processing of personal data and any consequential actions should be performed at the lowest practical level. For example, chronic out-of-policy behavior can be the basis of a management discussion but only exposed to the lowest-level manager who can coach the worker on proper policy.

(12) Proper Data Retention and Disposition. Methods for storing and disposing of data should ensure the security of the data in accordance with the law.

V. ISSUES ON THE HORIZON

a. Implications of the EU Data Protection Regulation.

The ultimate implementation of the developing EU Data Protection Regulation (Regulation) may bring changes to employer-worker privacy standards in Europe by taking the aspirations of the Directive and making them binding on EU nations. Under the proposed Regulation, employers retain the right to process personal data based on the enterprise's "legitimate interests," or possibly also where the disclosure of data would meet the reasonable expectations of the data subject based on their relationship with the data controller. However, an enterprise's legitimate interests can be overridden by a worker's interests or fundamental rights and freedoms.[21] In addition, the proposed Regulation with amendments by the European Parliament contains a number of provisions that directly address the processing of employee data. First, the current draft of the Regulation contains a recital indicating that

---

[18] Art. 29 Working Party Opinion 15/2011 on the definition of consent.

[19] *Id.*

[20] This is an extraction from the larger principle of subsidiarity found in Article 5 of the Treaty on European Union, which ensures that decisions are taken as closely as possible to the citizen and that constant checks are made to verify that action at the Union level is justified in light of the actions available at the national, regional or local level.

[21] European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Draft Data Protection Regulation), Art. 6. While the balance of these interests under the pending regulation is yet to be determined, the balance will likely reflect current standards whereby the legitimate business interests of the company cannot entirely override an individual's privacy rights. The Working Group has stated that "Workers, as long as they form part of an organization, have to accept a certain degree of intrusion in their privacy and they must share certain personal information with the employer. The employer has a legitimate interest in processing personal data of his workers for lawful and legitimate purposes that are necessary for the normal development of the employment relationship and the business operation." Opinion 8/2001, *supra* note 6.

the principles on processing data should apply in the employment context, though Member States may consider enacting statutes allowing for regulation of employee data processing through agreements between enterprise management and employee representatives.[22] Second, controllers and processors may be required to designate a Data Protection Officer where the core processing activities consist of processing the data of employees.[23] This Data Protection Officer would thereafter be required to inform employee representatives of all processing of employee data.[24] Third, the draft Regulation expands the Directive's territorial scope by imposing privacy requirements on enterprises operating outside the EU when those enterprises process personal data in connection with providing services to or monitoring individuals in the EU.[25] This latter change will bring foreign enterprises that process the data of EU citizens within the scope of EU data privacy law.

In addition to any new requirements under the pending EU data protection law, individual Member State worker privacy legislation will likely increase as well. The proposed Regulation specifically forecasts Member State implementation of specific rules regulating the processing of workers' personal data in the employment context.[26]

b. Foreign surveillance activity.

Another important consideration for the future is the capacity of private companies to protect individuals from government snooping. In the wake of the controversial surveillance practices of the U.S. National Security Agency, the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) has recently emphasized the need to protect the data of EU citizens from foreign surveillance.[27] The LIBE Committee reprimanded those companies that were involved in mass surveillance of EU citizens. The LIBE Committee noted that, while each of these companies was self-certified to the U.S.-EU Safe Harbor, many of these companies had not properly encrypted information and communications that were exchanged globally. This failure enabled intelligence services to intercept information. Because of this compromise of EU citizen data, companies may anticipate both stricter EU requirements for encrypting data flows and shifting standards for global data exchanges.

At the core of this issue is the recognition of the fact that enterprises in a particular jurisdiction must respect that jurisdiction's obligations with regards to data processing, even if more onerous than, or contrary to, the law of other countries where they operate. As a preliminary matter, companies may be inclined to consider, to the extent possible, establishing transparency of involvement in intelligence data collection and sharing programs.[28]

---

[22] Draft Data Protection Regulation, Art. 124.
[23] *Id.*, Art. 35.
[24] *Id.*, Art. 37.
[25] *Id.*, Art. 3.2.
[26] *Id.*, Art. 82.
[27] Committee on Civil Liberties, Justice and Home Affairs, Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)).
[28] *See* Article 29 Working Party Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes.

c. Legal developments in the U.S.

In the near term, state and federal U.S. law will likely begin to make incremental shifts toward recognizing worker privacy rights. This will show up in two trends: (1) privacy in hiring determinations and (2) the increasing intermingling of work and personal life. First, laws and regulations will likely continue to narrow the scope of information that an employer can consider in making a hiring decision. Already, states are rapidly banning an employer's rights to request an applicant's criminal history early in the application process or access to an applicant's online or social media accounts.[29] Second, technology will continue to blur the lines between work and personal life, requiring enterprises to wrestle with the use of social media as a business tool and the increasing utility of "bring-your-own-device" programs (BYOD). Currently, the heavy potential liability sustained by employers in the U.S. with regard to their workers' acts will likely prevent legislation that limits their monitoring ability. However, as privacy is a growing concern, it is likely that legislation in the U.S. will, over time, carve out worker privacy protections on a state-by-state basis.

d. Changing threats.

The most significant internal change facing employer technology security is the blend of work and personal life. Workers are becoming increasingly comfortable with using enterprise technology when operating away from company premises, or using their own equipment for both personal use and to conduct business on behalf of the enterprise. These devices, often outside the control of the enterprise IT or security staff, have the potential to expose the enterprise to malicious software (e.g., viruses, worms), theft, inadvertent/unauthorized disclosure or loss of personal data and intellectual property.

Employers have begun to accede to workers' use of personal devices in the workplace, rather than employer-provided devices. These BYOD programs pose new challenges in the balance between safeguarding enterprise data while protecting worker privacy. Many employers are beginning to address this problem through BYOD policies and user agreements. However, for multinational employers, BYOD for workers in jurisdictions with broad data protection laws can create complex challenges. Using personal devices also commonly leads to the comingling of worker personal/private data with enterprise data (as in photo collections, multi-account email etc.). Commingling poses significant challenges in company data destruction, monitoring, and forensic investigation.

Likewise, the increase of cloud-based services and use of third-party suppliers may also impact security policy within the enterprise as more data processing is outsourced to third parties. The use of third-party data processors opens the door for vicarious liability for the third-party's inadequate data protection. In addition, third-party data processors provide organized, malicious actors the opportunity to employ a secondary means to attack enterprise networks and obtain personal data, financial data, and intellectual property. Today such secondary targets have included external law firms (nearly 80 major U.S. law firms were hacked in 2011) or other service suppliers (e.g., the HVAC company used to

[29] A slew of jurisdictions have recently enacted "ban-the-box" legislation, which generally prohibits employers from requesting criminal history information in an employment application. Similar bills are pending in 26 states. In addition, twelve states have enacted "social media password protection" laws. *See* Philip L. Gordon, Workplace Privacy 2014: What's New and What Employers May Expect, *available at* https://www.privacyassociation.org.

attack Target). It is not an unreasonable leap to expect such threats to arise also through mobile BYOD pathways.

VI. CREATING A FRAMEWORK FOR DETERMINING APPROPRIATE MONITORING

The rapid change in technology and the ever-increasing creativity of cyber criminals means that the solution to this security-privacy puzzle does not lie in a static set of rules and specifications representing an exact balance of enterprise security and individual privacy. Instead, the best solution is a transparent, constituent-based decision making process that permits the interests of the individual, the enterprise and society to be combined to determine whether or not to employ a certain security surveillance method. This decision process will recognize that addressing computer-based theft of data requires some advanced, automated surveillance methods. Indeed, surveillance itself is a necessary means to protect the privacy interests of the workforce. The purpose of the proposed framework is to allow necessary, legitimate, transparent, proportional surveillance while preventing misuse.

To ensure appropriate balance, security surveillance programs should be designed and deployed under the watchful eye of a Security and Privacy Board: a named, multi-disciplinary team composed of experts in security, IT, human resources, ethics, privacy, works council, legal and any statutory Privacy Officer who is representative of a data protection authority. The actual constituency depends on the particular organization but the Security & Privacy Board members should be well versed in the principles of privacy as well as understanding the threats to the organization. The Security and Privacy Board will consult with works councils, review privacy principles and best practices, and be the approving authority for the security surveillance program. This team could be responsible for developing criteria for security vigilance, thresholds for when changes must be subjected to scrutiny and approval, criteria for launching investigations, and the general monitoring of security effectiveness as balanced against privacy interests. They are the owner of the employee privacy notice and are active participants in related IT, security and privacy policies.

VII. CONCLUSION

This paper attempts to reconcile the potentially conflicting priorities of individual privacy and enterprise security. We have outlined the basics of privacy protection and broadly described the essential methods used to detect criminal and out-of-policy behavior in commercial IT systems. Potential legal developments in both the U.S. and the EU will continue to shift the expectations and requirements of enterprises in establishing legal compliance in the jurisdictions in which they operate. In addition, the increasing sophistication of cybercrime will continue to pose ongoing challenges to enterprises in securing commercial viability, requiring new and novel means of surveillance and protection.

Despite the constant changes in legal requirements and technological capabilities, companies should continue to be guided by the privacy protection principles delineated above. These principles are generally applicable and provide broad guidance that can be applied to specific circumstances. On the whole, enterprises should consider those security mechanisms that will protect the enterprise while providing for a minimal intrusion on worker privacy.

Because of the complexity and changing nature of the technology, the legal frameworks, and the threat landscape, we propose the creation of an enterprise Security and Privacy Board to exercise discretion

and authority over the deployment and use of security surveillance. Because of the complexity and changing nature of both the technology and the threat landscape, the balance of interests at stake requires open and ongoing discussion and deliberation. By openly debating the privacy and security balance and monitoring the effectiveness of the security program, the interests of the individual and the enterprise can be properly served.