

Weekly Review

**Volume 6, Issue 1
January 6, 2010**

In this issue:

- . A New (and Important) Twist on
Data Privacy**
By David Hill, Mesabi Group

**Pund-IT, Inc.
Hayward, CA
U.S.A. 94541**

**Contact:
Office: 510-383-6767
Mobile: 510-909-0750
charles@pund-it.com
www.pund-it.com**

A New (and Important) Twist on Data Privacy

By David Hill, Mesabi Group

The Supreme Court of the United States (SCOTUS) recently agreed to accept a case on a data privacy issue related to whether or not an employee has a reasonable expectation of privacy for personal messages sent on devices owned by an employer. The legal question revolves around whether or not such personal messages are protected under the Fourth Amendment of the Constitution, which prohibits unreasonable searches and seizures.

Ostensibly, this is about a narrow situation where a public employee had his pager messages transcribed into text and read by his superior. But practically, it touches a much broader and more important issue, which could very well be the reason that the SCOTUS agreed to hear the case. That issue is how employee data privacy affects the management of information that organizations (including business, governmental and non-profit entities) need to keep and examine for legitimate purposes, such as compliance with government regulations or discovery related to a court case.

It's easy to understand how a strong stance on behalf of employee data privacy might create significant problems for businesses. As a result, the SCOTUS ruling may not be as important as its clarity so that businesses know what they can and cannot do as related to employee data privacy.

Among the issues that will be discussed are the following:

- How collecting personal communications may be an unavoidable byproduct of a normal business process.
- The difficulty of separating business from personal communications.
- How denying an organization the ability to read personal communications captured as part of a normal business process could conceivably expose it to both business and legal risk.
- What might happen if businesses decide to try and collect personal business communications not part of a normal business process.

Data Devices — Proliferation, Location and Ownership

The case is really not only about the use of an employee pager but also touches the shared personal/business use of electronic devices at various locations and under different ownership models. Let's consider device, location, and ownership complexity.

Today, the use of electronic devices for both personal and business/enterprise use is common. That can include untethered mobile devices that use wireless communications, such as pagers, cell phones, and personal digital assistants (PDAs), as well as those that may also use network connections, such as laptop, notebook and netbook computers. It can also include tethered devices, such as telephones and desktop PCs.

The location where electronic devices are used can vary considerably. Many employees work only at employer-owned sites, but an increasing number of workers are permanently or semi-permanently out of the office due to job requirements or travel. Other employees work at home either full- or part-time.

The “owner” (i.e., the purchaser) of a device may vary too, as either the employee or the employer may own the device (joint ownership is conceivable but less likely). Since the collaboration that electronic devices enable requires a network of some kind, communications costs may be borne either by the employee or the employer or in some combination. For example, a person who works at home may have a single Internet connection that he/she pays for fully even though the connection is sometimes used for business purposes. On the other hand, the employer may pay (either directly or via reimbursement to the employee via an expense account) for all of an Internet connection although some of it is used for personal purposes.

The commingling of personal and business use of various devices at different locations and with different ownership patterns may sound very complicated, but it has become commonplace. That said, from the perspective of employee data privacy proliferation, location and ownership are general principles that are likely to apply to virtually all the different possible combinations related to the SCOTUS case.

Capturing Data

This Mesabi Group analysis takes as its starting point some of the principles, ideas, and concepts discussed in my recent book “Data Protection: Governance, Risk Management, and Compliance,” builds upon that foundation and is extended to meet the particular requirements of this particular situation. Even though data protection and data privacy are more or less synonymous in many areas (including the European Union), more generally, data privacy is really a subset of overall data protection.

Before considering data privacy however, we must examine the capture of data. Whenever an electronic device generates data, the question is whether or not it can be captured in non-transient form. For example, landline telephone conversations are typically not captured on recording (i.e., storage) media. That means that it could not be reproduced and would be lost forever. No data privacy violation could occur.

However, some calls would be recorded with the caller’s knowledge and implicit consent. That is the case for phone calls which “may be recorded for quality assurance purposes” and for emergency 911 calls. Other data, such as e-mail, is automatically captured to non-transient media, such as a hard disk. This non-transient media might be called “permanent” as long as one recognizes that media has a finite lifetime and that the data itself may be deleted or spoliated for some reason.

Presumably, the data captured in work circumstances or by devices purchased or owned by organizations is generally assumed to be work-related data and any personal data is simply captured as a byproduct of a normal process. This data may be captured on storage within the physical walls of an enterprise or may be captured by a third party, such as a telecommunications vendor or a cloud service supplier.

That said, the capture process should be for valid business purposes. Those business purposes may include (but are not necessarily limited to):

- **Mandatory data capture** — for example, an organization may be legally ordered to retain data that it has collected. That is the case in Boston, where a judge requires city

employees to keep their emails, and a brouhaha arose when a city employee deleted a large number of emails.

- **Prudent data capture** — the Federal Rules of Civil Procedure (FRCP) clearly state that electronically stored information (ESI) captured in information systems is discoverable. As a result, enterprises must be very conscious about what data they need to capture and be able to identify what and where the data is if there is a reasonable chance that it will serve as part of a discovery process.
- **Legitimate business use data capture** — enterprises have any number of reasons for wanting to capture data that might serve a valid business purpose. In fact businesses might well claim that any and all data created during the course of business by an employee is owned by the employer; for example, intellectual property that may result in a patent.

Foundation: Understanding Different Types of Data

Before we can address the question of whether or not separating business data from personal data captured in the same data store is possible (or if possibly desirable), we need to examine the different types of data (Figure 1) and how they are typically used.

Figure 1: Differentiating Types of Data

Type	Common Form	Key Differentiators	Examples
Structured	Databases (such as SQL-based)	Sort	Transaction processing systems, such as for online purchases
Semistructured	“Text” documents such as e-mail and word processing	Search	Business and worker productivity tools (e-mail and word processing) and text on Web sites
Unstructured	Natively bit-mapped data, such as video, audio, photographs, and medical images	Sense	Video surveillance, voice recording, MRI scans

Source: Mesabi Group, January 2010

Structured data typically relates to or arises from transaction processing, such as those common in retail outlets, financial services and banking where the exchange of information is often transparent to the end user. For example, a person placing an order from a catalog or at a Web site probably unknowingly provides personal information (such as a credit card number) that is legitimately retained by the retailer as business data. Obviously, there are major data privacy issues involved, but regulations regarding the information vary widely. European Union countries have very strong rules on how such personal information can be used. In the U.S., a number of data breach laws can be invoked in cases where personal information (such as a credit card number) is not kept confidential. This is a very important data privacy issue, but is beyond the scope of this discussion.

The data privacy issue can also arise with semistructured data, which is often lumped in with unstructured data. However, doing so is incorrect and for this analysis the distinction between the two is very important. Why? Because the content of semi-structured information can be searched, a critical distinction in eDiscovery. In such cases, analytical tools can

help separate the relevant from the irrelevant without manual visual inspection that may at best simply be expensive and at worst may be impractical because of the volume. That process does not necessarily eliminate the need for “manual” visual inspection.

Unstructured data can *natively* (which means in its raw original form) only be sensed, i.e., you can watch a video or listen to a voice recording. Technology is evolving to put more structure around unstructured data. For example, a voice recording can be reduced to a text transcript with each portion of the transcript identified by the speaker. Surveillance video is system-generated data rather than individual-generated data. That is, the system generates video of an individual when that individual comes into the range of an active camera. The individual does not generate the video (except perhaps by motion detection) and may be entirely unaware that the video, say in a bank or mall, is actually being created.

This situation is in contrast with audio where a person, say, initiates a cell phone call and is aware of what they are saying (although they or may not be aware that it is being recorded). Video surveillance has a business use where personal data is involved, such as determining whether a crime or accident occurred or to measure the traffic flow patterns in a store. Now data privacy issues apply to unstructured data but, as with transactions, the personal information is intrinsically interwoven within the business application itself, which could not perform its function without that information. Audio recordings are different. One employee phone call may be completely personal, another may be purely business, and a third might mix personal and business information, but all three might be captured in the same data store. This is one place where the employee’s personal data privacy issue can arise.

Is Separating the Business Data Wheat from the Personal Data Chaff Possible?

To consider this question, let’s take the case where personal data is captured as a byproduct of a normal business process. For example, a company may have a policy that all e-mails sent or received must be captured in a central data store. Those e-mails must be retained in an unaltered form until they may (or must) be deleted according to the organization’s data retention policy.

Now some organizations may have rigid rules strictly prohibiting employees from putting computers or phones to personal use, such as for personal telephone calls or personal e-mails. There may be good reasons for this prohibition, such as the need for regulatory compliance or strict confidentiality requirements. Any personal use could be subject to stern sanctions or penalties, such as termination of employment.

Although some organizations may long to use that draconian an approach at all times to all devices, applying such rules universally is both unrealistic and impractical. Take a mobile employee traveling with a business laptop. Shouldn’t that person be allowed to send personal e-mails after his or her workday is through? After all, taking two laptops (one for business and one for personal use) is impractical.

Well, can business and personal data be effectively isolated from one another? One possible way to do this is to “mark” personal data in some way. For example, the word “personal” could be put in e-mail metadata (which is data about the e-mail such as who sent an e-mail, to whom it was sent, and the time that it was sent, but not the actual con-

tent of the e-mail message itself). Software could then isolate data marked “personal” from other data. Does that do the job? The answer is not really.

Marking a communication, such as an e-mail, “personal” does not mean that the communication is in fact personal. Improper communications, such as inappropriate contracting and pricing discussions, unauthorized disclosure of a company’s intellectual property or secrets, or transmission of reprehensible pictures, could be masked by marking technologies. As a result, a company could come under scrutiny that could result in a lot of negative consequences, including embarrassment if not sanctions and penalties, for not properly monitoring the use of information that had come under their purview even though employees made inappropriate use of an electronic communications channel intended only for business.

By the way, an important side note is that encryption (even if could be used) is not an acceptable alternative. An employer would flag encrypted communications as possible hiding of information that would be relevant to the employer.

Can Personal Data Not Be Captured at All?

We have seen the difficulties of separating the business data wheat from the personal communications chaff if a business process captures both and puts both in a common data store. However, can a physical communications device distinguish between personal communications and business communications at time of creation and not send the data onto the business data store. That would mean that the personal data would not be captured at all in the business data store and could therefore not be examined, hence, no possibility of loss of employee data privacy would exist. The answer is theoretically yes. For example, a device could use what is called virtualization technology to separate two logical “personalities”; one for business use and one for personal use. Switching between the two virtual “personalities” should not be that difficult. Note that the technology may not exist yet for most electronic communication devices and, in fact, may never exist for devices using older technologies.

So does “logically” separating users from physical devices solve the problem of capturing personal data? The answer, again, is not necessarily so. Some businesses may not want to permit virtualization on a physical device that is used primarily for business reasons if there is a legitimate business reason for not doing so. For example, it may be difficult to ensure that company confidential information has not been transmitted improperly from a virtual machine to an unauthorized target. In such cases, the company may follow a “Caesar’s wife” rationale where all implications (and temptations) of impropriety are eliminated even if the business has confidence that employees would never do anything improper.

Let us note here, however, that some other businesses may take the opposite tack and not want to capture personal communications at all and will do what they can via rules, codes of conducts, etc. to avoid it. The use of virtualization would go a long way in assuring the separation of personal and business data. If challenged legally, an argument that the business might take is to accept the word of employees on what is and is not personal. If that trust is misused or abused, responsibility and guilt would rest solely on the employee who acted independently and irresponsibly. As a business, the company would appear to have acted responsibly by taking steps to both respect employee privacy and to ensure the con-

fidentiality of key data. The dilemma for businesses is which viewpoint (virtualization is acceptable vs. virtualization is unacceptable) will hold up legally when they risk being sued.

Hopefully, the upcoming SCOTUS decision will clarify (at least to some extent) the validity of the two arguments, i.e. where the company feels active intervention is required to avoid legal risk and where the company assumes a more *laissez faire* stance toward employee data privacy.

Should An Expectation of Employee Privacy Exist?

Does it matter that employees know that personal information will be captured and monitored by employers? If a person who is a member of a golf club speaks too loudly in the club restaurant and is overheard by others, that person has no one else to blame if that information is used to cause negative consequences. Just as the loud speaker could have spoken more softly as well as more carefully, so a user of electronic communications tools should recognize that others may see what he or she regarded as private. So logically, a user of an electronic communications channel may very well want to assume that any communications that are made could very be made public.

That does not mean that personal communications would necessarily be exposed. A business may or may not choose to search the data. For example, data on a desktop that is used at home for at least some business use may be protected by being backed up to remote storage and the employer may pay for the protection. In the process, personal information may also be protected. The employer may be protecting the data only so that it can be restored in the case of an emergency and never plans to look at it. However, by residing within the company's data repository that information could be included in an eDiscovery request.

A more usual case is that an authorized representative scans the information that has been collected so that the organization can meet any requirements for knowing what data is available and where it is located. This scan could be made with software, but the analytical capabilities of software are nowhere close to what visual inspection can reveal. Though this statement drifts into speculation, it would seem that both the capture (i.e., scan) of the data and the visual inspection of the data are reasonable.

But how can personal data revealed in this way be appropriately used? Assume that no illegal or otherwise unsavory behavior is revealed in a communication. Still, the examiner of the personal data, which may be an employee's supervisor, unavoidably brings his or her belief system and value judgments to the table in examining these communications. The employer's examiner may form an opinion that the personal communication is morally reprehensible, reflects inappropriate political opinions, or is some other way unacceptable. That may result in direct or indirect consequences for the employee. For example, termination for an employee who admitted smoking in a company that does not tolerate smoking would be a direct consequence. Indirect consequences may be more difficult to prove but could have negative connotations, such as denial of a promotion or unpleasant work assignments.

Controlling Data Privacy Remains in the Control of the Employee

Although the exposure of what an employee would have liked to keep private is undesirable to the employee, the employee could have avoided the consequences in one of two

ways. The first is to exercise discretion and caution in communications that the employee knows may be examined by others, such as a supervisor. The second is to choose channels of communication that are not the responsibility of or captured by the employer.

Although as we have seen that some personal communications may be appropriately commingled with business communications that does not mean that the individual does not have access to alternative communication channels (such as personally buying a cell phone that uses a different carrier than the cell phone used for business). Even though the worker could utilize such a device for business purposes — such as calling in sick — that is not its typical use.

Issues with Intentionally Collecting Non-Business Personal Communications

Does a company have the right (or responsibility) to capture employee data that is generally personal, only incidentally used for business purposes, is not part of a normal business process or has other intended uses? Ostensibly, the business might have a legitimate business concern, such as preventing the leakage of confidential information or to capture data that would be necessary to respond to eDiscovery requests should they occur.

Now this my personal opinion, but I suspect that businesses would be on very shaky legal ground if they captured such information. Yes, a worker may do things that are inappropriate or illegal related to the company, but if they do so on their own time and through private communication channels that is and remains their responsibility. The process of eDiscovery for ESI for businesses relates only to normal business processes. If a company suspects that an employee is using company data (such as revealing trade secrets) outside those normal business processes, the company should turn to law enforcement authorities to help address the issue rather than attempting a broad, surreptitious sweep of information where only a small portion of communications could conceivably be of importance and a number of individuals could risk having their private communications exposed.

Does that mean that a business could not sometimes collect that data reasonably and legally? No. For example, the company could ask employees to allow them to collect that data. Union and public sector employees could probably tell them no, but “at will” employees might feel that their jobs are at stake and consent only because of that threat. Whether such coercion is legal, I don’t know. However, say that a third party had a confidentiality arrangement with the employee for private matters totally unrelated to the employer (such as health-related matters) and the employer revealed that information. Once again this is only my opinion, but the third-party employee might have a very good case to receive damages from the employer. The bottom line is that businesses probably should collect private communications only as an unavoidable byproduct of their normal business processes. When they stray from that, they may be taking on unnecessary and unexpected risks which far exceed any benefits they might gain from capturing that information.

Mesabi Musings

As a non-attorney and one more or less unfamiliar with constitutional law (including the precedents), I cannot pretend to understand in depth the complex reasoning that goes on in any SCOTUS decision. People tend to like or dislike particular decisions based upon their political perspectives without fully comprehending the legal issues surrounding the conflict between two principles where only one can prevail.

However, as an industry analyst familiar with the technologies of ESI and with a strong business background, I have tried to frame the issues from at least a business perspective. The key points are:

- Collecting personal communications in a central business storage repository can very well be an unavoidable byproduct of normal business processes where a particular electronic device is used for the creation of both personal and business communications.
- The difficulty of determining what is truly personal means that the business may inadvertently visually scan and read what were meant to be strictly personal communications.
- Denying an organization this ability could prove to be technically infeasible and could conceivably expose it to both business and legal risk.
- Even if the data can be separated (such as through the use of virtualization) and a business wants to take a *laissez faire* stance respectful of employee privacy, is the business still at risk for not having done enough?
- Can businesses thus decide to try and collect personal business communications that are not part of a normal business process? One risk is in not doing enough and the other risk is in trying to do too much.

While the Supreme Court may choose to rule very narrowly, only on some of what is contained in the first point, a broader ruling would help businesses explicitly understand what is and what is not permissible, which would have the laudable effect of reducing future litigation.

In any event, the upcoming case and eventual ruling may be under the radar for most businesses but needs to be watched quite closely. Depending on the Court's ruling, some businesses may want to take a more proactive stance to avoid significant negative consequences.

© 2010 Mesabi Group. All rights reserved.

About the Mesabi Group

The Mesabi Group (www.mesabigroup.com) helps organizations make their complex storage, storage management, and interrelated IT infrastructure decisions easier by making the choices simpler and clearer to understand.