# On the Effects of Enterprise Security on Employee Privacy

By Amn Rahman and Ashish Gehani

**Employees sync apps across personal and work devices, resulting in commingled data entering enterprise backups. Further, employee-monitoring tools collect information about individuals' system use that is also archived. The authors identify resulting harms to both employees and employers and suggest solutions that help meet the needs of both stakeholders.**

## Commingling of data

Many companies choose to backup company data for a variety of reasons, ranging from legal and contractual to protecting data against loss. Some backup policies may include archiving data held in devices used by employees and records from monitoring logs. While this may seem harmless, the commingling of personal and work data on employers' devices is likely to result in personal data flowing into companies' backup storage. Commingling is further complicated by bring-your-own-device (BYOD) policies since these may require remote backups or monitoring of devices to guard against data loss.

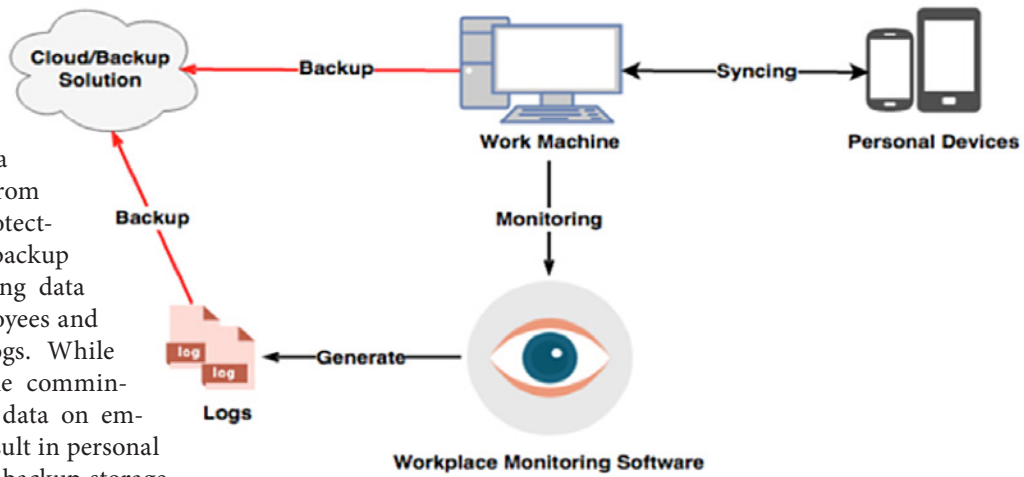



**Figure 1 – Apps on personal mobile devices may sync with employers' computers, on which enterprise monitoring and backup software run, creating channels for personal information to enter corporate archives.**

## Blurred lines

In 2016, it was estimated that digital consumers use between three and four devices on average [3]. It is therefore unsurprising to find individuals using multiple devices to carry out work-related tasks. Nearly half of all respondents in a survey by Gartner spent more than an hour a day using their personal devices for work [12]. There is mounting evidence that employees cannot do their jobs effectively without their mobile devices and that most employees use their phones for calendaring, phone calls, and email [7]. Many productivity apps allow users to seamlessly migrate tasks from one device to another by syncing data across them. The dangers associated with companies losing control of their data through such means are widely discussed. However, little attention is paid to the effect of personal employee data entering the corporate environment [2].

Synced calendars, documents, email, address books, and browsers are all likely to commingle personal- and work-related data, even if a person uses his employer's computer solely for work (as illustrated in figure 1). Employees who sync their web browsers across devices to allow migration of searches and bookmarks from one device to another allow

metadata and browsing history to be recorded in their company's backups as well.

Many employees may be permitted and feel comfortable using their work computers for personal use. This may further aggravate the degree of data commingling. In a survey by ePolicy Institute, 79 percent of the participants claimed that one to 10 percent of the email they sent or received was personal, that is, not work related [6]. In such cases, the commingling of data is easier to observe. In the absence of an appropriate use policy stopping the utilization of work computers for personal use, an individual's work computer may become a primary personal computer as well.

## Employee-monitoring software

In addition to employee work habits, companies also contribute to the commingling of information by collecting and analyzing data on staff activity in the enterprise. Companies may choose to monitor employee use of work computers for a variety of business reasons: to catch violation of company policies in emails, to detect data theft, to measure employee productivity or time spent on non-work-related sites, or even to detect malicious activity on corporate networks. A huge market of employee-monitoring solutions caters to this demand and provides tools that track web activity, key strokes, email, detailed app and file usage, and software installations, among other activities [21]. At the same time, employee devices, email, and social media accounts have been used in termination decisions or litigation [16]. In the US, employers have the right to monitor their employees. Some organizations may also be required to store the data in accordance with the law.

Sarbanes-Oxley Act [17], Health Insurance Portability and Accountability Act (HIPAA) [10], Gramm-Leach-Bliley Act [8], and other laws require organizations to preserve and protect data in very specific ways [21]. The Electronic Communications and Privacy Act (ECPA) [5], a hallmark privacy protection statute protecting the privacy of communications, allows exceptions for employers to monitor their employees' use of computer equipment provided to them. Depending on state law, employers may or may not have to notify employees of any monitoring activities.

The type of employee-monitoring solution in place affects the extent of commingling and the dangers associated with it. Key logging, for instance, may be used to capture key strokes per minute and this may inadvertently result in sensitive information, such as passwords, in temporary files becoming part of backup logs. More intrusive monitoring is therefore likely to capture employee information that would otherwise not have been available to employers.

## Dangers of commingling

Commingled data held in backups can create concerns for both employees as well as employers.

### Employee concerns

The personal information held in backups may include financial details, health records, family information, passwords, and the names of external services used, among other pieces of data. The level of commingling is a predictor of the scale of damage that a breach may cause. Many aspects of a person's life that are monitored and recorded may cause long-term repercussions that may not be limited to pecuniary damages.

In the aftermath of a breach, the employer may know more about the incident than employees. If staff are unaware of their personal data being backed up or are unaware of the breach itself, they may not be able to trace the harm back to its source. In addition, employees who left the company while their data still resides in corporate backups may never be notified. In the event of a breach affecting customer data, companies dedicate significant resources for post-breach mitigation, towards public relations, and for customer support. It is estimated that 40 percent of the costs incurred by companies following a breach are due to lost customer business [13]. Contact costs, public relations, identity protection services, and customer acquisition cost make up about 21 percent of the total expenses [13]. However, if a breach targets employee data only, the media may not learn of it and it may not cause pecuniary damage for the employer. This creates an incentive to under report such incidents or potential effects.

One of the most common ways of alleviating customer or employee harm is to provide free credit monitoring and identity theft insurance for a number of months after the breach. Such compensation may be useful instruments for reducing financial damage in the short run but will not cover other harms that may occur later on through emotional distress,

blackmail, or other unpredictable damages. In addition, a long temporal lag between the event and the harm or injury is also likely to create difficulty in proving causation—other events may have led to the same data being exposed through other means.

Employees may also seek redress through the legal system, though a number of factors limit their chances of success. A case may be dismissed if the court believes that the employees had no right to privacy and should not have assumed that the company would provide adequate protection for their personal data on work computers. Nevertheless, if a case does make its way through the court system, it is still difficult for employees to win. Typically, data breach cases are filed as class action lawsuits. The critical factors that predict the probability of a favorable outcome in such cases are the cause of the data breach, whether an alleged harm can be attributed directly to the data breach, and the types of information lost [15]. The harms may take the form of financial loss, identity theft, emotional distress, anticipated future losses, or cost of credit monitoring. If the harm has not occurred already or isn't imminent, the precondition for harm will not be met. In addition, if a company has already provided employees with an initial remedy through credit monitoring or identity theft insurance, the chances of additional compensation through the court drop [15].

Privacy protection statutes in the US are a patchwork of different federal and state laws covering specific types of information. Therefore, cases may be argued on a number of different grounds. This increases the unpredictability of whether the plaintiffs will prevail. Employees are thus motivated to reach a settlement with their employer rather than seeking complete compensation. Defendants settle 30 percent more often when the plaintiffs claim financial loss from the breach or when presented with a certified class action lawsuit [15].

### Employer risks

Expectations of privacy have always been dependent on the laws and social norms. However, the pervasiveness of technology today leads to regular capture of granular information about employees' lives and activity. Consequently, employers need to be cautious about the type of data that they collect from employees.

By removing employees' expectations of privacy on company-owned devices, employers find it easy to strip staff of any comfort afforded by privacy in the workplace. The law for decades, through the ECPA and legal opinions, has allowed companies to monitor their employees and has weighed heavily on the side of employers, allowing them to define and expand the scope of employee monitoring. Most courts seemed to rule in favor of the employer in cases where the employee has invoked the Fourth Amendment [21].

Recently, the attitude of courts towards employee privacy seems to be changing. Some judges have recognized the rights of employees to have reasonable expectation of privacy for their email sent over or accessed on equipment provided by the company, even in light of employer policies disregarding such an expectation. In one particular case, the court recognized the employee's rights to his personal email, even though it was on a company computer and the company had a specific policy that denied expectation of privacy for any email passing through the company's systems [18]. Other courts have also followed suit. With the drifting trend in legal judgments favoring employee privacy, employers need to be more wary of what they are capturing and storing. If rulings deem it unacceptable for companies to access employee personal emails or offsite online behavior, it may be harder to untangle and separate commingled data from the pipeline than taking preventative action that leaves out personal information.

The wealth of information available about an employee creates ambiguity concerning permissible access and use of such data [18]. If the court rules a certain type of logging or access as illegal, an employer may believe that they are not recording the information, but commingling may result in its collection and storage. In the event of a breach and actual harm, an employer's position may be jeopardized with respect to liability. For example, some states have begun to ban employers from demanding passwords to employees' social media accounts [4], but if employers use browser history tracking as a monitoring mechanism, they may be able to access and store employee authentication credentials, creating a repository of data they have no right to access. Future state privacy legislation is expected to affect government entities and companies that provide electronic equipment to their employees [11].

Indiscriminate recording of device data in backup storage can also create problems for the company itself. Our existing knowledge of data breaches and their costs and impacts is primarily framed by cases where the intent was to cause financial harm. Therefore, the known post-breach mitigation strategy usually surrounds financial compensation for the damage. However, not all breaches are driven solely by financial incentives. The recent Office of Personnel Management data breach was motivated by political espionage and the breach targeting Sony Pictures Entertainment was seen as an attempt to cause widespread humiliation of the company and its employees [20]. Such attacks lead to unpredictable costs. Having a repository of employee data that may partly be personal in nature acts as a honey pot for adversaries intent on causing harm to a company or its employees [1].

## Deleterious regulatory effects

In the aftermath of the Snowden revelations, US federal contractors face heightened regulatory enforcement for incident discovery and reporting. The companies and all subcontractors in the supply chain are expected to follow stringent cyber-incident reporting requirements if they handle covered defense information (CDI). In the event of a breach, companies may be asked to provide any data or access that the Department of Defense (DoD) deems relevant. The government's right to this data is settled law in the US [9][14][19].

### Defense Federal Acquisition Regulations

The Defense Federal Acquisition Regulation Supplement (DFARS) set the contractual requirements for federal defense contractors. Recently revised clauses in DFARS 252.204-7012 require contractors handling CDI to implement security standards listed in the National Institute of Standards and Technology (NIST) Special Publication 800-171. This document contains 14 families of security guidelines, including requirements for auditing and accountability. It entails information system record retention for monitoring, analysis, and investigation of unlawful or unauthorized activity, as well as for tracking actions back to responsible individuals.

The DFARS 252.204-7012 clause requires that cyber incidents be reported within 72 hours of discovery. Further, all device and storage images, relevant monitoring logs, and network packet capture data must be stored for at least 90 days from the submission of the report as the DoD may request this data to facilitate investigation. In addition, the DoD may also require any additional information or equipment involved to facilitate analysis, with no limitations specified in the clause. This data may also be shared with other government agencies for a number of purposes if the DoD decides that they may be affected by the information. The security of the data if shared

with other agencies, is implicitly affected with no guarantee of confidentiality provided in the clause. Many companies, including large contractors such as Raytheon, have expressed their concern about providing access to their systems and data for investigations.

If the DoD asks a contractor for access to data, it may also lead to backups and monitoring logs with private data entering the hands of the government without any court order or legal process. The ease of sharing data with government agencies defeats the purpose of any privacy guarantees surrounding personal data. This leads to an ethical dilemma for companies. Companies are trying to reduce the amount of personal data that they keep about customers—for example, end-to-end encryption is being introduced in messaging systems such as WhatsApp. At the same time, the regulations ask companies to take responsibility for holding personal employee data beyond what is needed for work.

## Potential solutions

Public knowledge of attacks targeting non-financial data and company backup processes is limited. So is the understanding of the possible harms that may result. This makes estimating costs of such breaches difficult. To an extent, reasonable ex-post breach mitigation strategies are in place for financial data breaches. Unfortunately, they have little relevance for mitigating the harms of medical data loss, email archives, and other personal information that is not explicitly related to financial records [20]. In addition, it is difficult to map the entire spectrum of motivations that may attract the attention of attackers of corporate backups, or list the ways in which the data may be misused.

One way of reducing such incidents from occurring is to increase the measures used to secure the data. However, breaches do happen and complete prevention is impossible. Untangling commingled data is harder than preventing it from mixing in the first place. Solutions in this space need to recognize an employer's need to backup data of company-provided machines while allowing employees the flexibility to migrate their tasks easily within the bounds of company policies. This space may require improvisation to leverage existing research and approaches. No single technical solution is likely to suffice. Efforts to address the issues will require a combination of policy, behavioral, and technical changes. We provide examples below.

### Policy

- Companies must strive to be transparent regarding their backup and monitoring policies. They must ensure that employees understand the scale and scope of these policies.
- The data retention period for backup policies must be kept to a minimum to reduce the longevity of information held in storage.
- Companies should refrain from using invasive monitoring practices if possible. With regards to key loggers, monitored information should be limited to aggregated quantitative information rather than lists of typed words.
- A company's BYOD policy must be easy to understand. Any form of monitoring or backup of personal devices should be stated explicitly.
- Companies should attempt to limit the sources of data within employee computers by specifying certain files or folders for backup, as opposed to the entire machine.
- In the event of a data breach affecting employee records or backups, employees must be informed in a timely manner.
- The effect of employee monitoring should be assessed and re-evaluated to check the necessity for fulfilling business goals.
- Where it is necessary to maintain personal data, this should done using privacy-preserving aggregation if possible.
- Instead of indiscriminate logging, recording should be limited to that needed for tracing violations of policies.
- Companies should push back on egregious demands for data. When employee information is transferred to the government, the company should keep employees informed.

### Behavioral

- An effective solution is to create separate app accounts for work and personal use, to restrict sharing to a controlled set of data. While this is inconvenient, it can substantially decrease the dangers that arise from commingled data.
- Employees must be vigilant and ask about company monitoring and backup policies to learn how they may be affected.

### Technical

- Data held in storage should be encrypted using a key generated at the employee's endpoint. Data in backups should be

## LOOKING AHEAD

### November: Impact of Malware

For almost as long as there have been computing platforms in use, there have been inherent threats associated with them. One of the most prevalent is malicious software. From the Cascade and Brian viruses to the XcodeGhost exploit and WannaCry ransomware, malware has been an inevitable part of the computing landscape. As technology matured and became more sophisticated, so did the malware variations and the damage caused to millions of computers around the world. This month's issue of the ISSA Journal will explore the impacts of malicious software in the wild and how it has evolved as well as the techniques used by cybersecurity professionals to mitigate the risks posed by it.

**SUBMIT ARTICLES TO EDITOR@ISSA.ORG.**

encrypted using the same key (in addition to other keys used) to protect the backups. If the government requires data, the employee can provide access using the private key.

- Using containers or sandboxes can isolate company apps from personal apps to avoid incidental capture of data during backups.
- Before data enters the backup pipeline, files that may contain personal information should be sanitized or filtered out. A range of approaches, such as leveraging file extensions, magic strings in the content, or internal expression matching, can be employed to streamline this.
- Companies should monitor and log web activity or online behavior in aggregate only. Specific details should only be exposed if a policy violation occurs, for example, if the employee accesses blacklisted websites. Anomaly detection can be used to filter out accidental accesses, reporting only truly suspicious behavior.

## Conclusion

Companies backing up data become caretakers of personal employee information. If this data is exfiltrated, this can cause long-term harm to the employees and even to the company. Employers and the legal system must therefore step back and reassess the concept of privacy in the workplace, given modern trends in technology and work patterns.

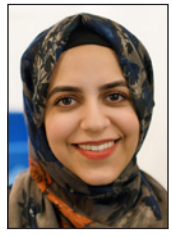
## Acknowledgments

This material is based upon work supported by the National Science Foundation under Grant ACI-1547467. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

### References

1. Abel, Robert, "Verity Health Systems Employee Data Compromised in Phishing Scam," SC Media, 2016 – https://www.scmagazine.com/employee-information-compromised-in-verity-health-systems-breach/article/528257/.
2. Bradley, Tony, "Survey: BYOD Security Remains Spotty, with Users Unaware or Unmotivated about Risks," PC World, 2014 – https://www.pcworld.com/article/2690359/survey-byod-security-remains-spotty-with-users-unaware-or-unmotivated-about-risks.html.
3. Buckle, Chase, "Digital Consumers Own 3.64 Connected Devices," Global Web Index, 2016 – https://blog.globalwebindex.com/chart-of-the-day/digital-consumers-own-3-64-connected-devices/.
4. Deschenaux, Joanne, State Laws Ban Access to Workers' Social Media Accounts," Society for Human Resource Management, 2015 – https://www.shrm.org/resourcesandtools/legal-and-compliance/state-and-local-updates/pages/states-social-media.aspx.
5. Electronic Communications Privacy Act – https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285.
6. Flynn, Nancy, "Electronic Business Communication Policies and Procedures Survey," The ePolicy Institute, 2009 – http://www.epolicyinstitute.com/2009-electronic-business-communication-policies-procedures-survey-results.
7. Government Computer News, "Employees Can't Do Their Jobs Effectively without Their Mobile Devices," GCN, 2012 – https://gcn.com/microsites/2012/download-mobile-and-wireless/01-employee-mobile-device-needs.aspx.
8. Gramm-Leach-Bliley Act – http://www.ftc.gov/privacy/privacyinitiatives/safeguards.html.
9. GSA Privacy and Contract Requirements, GSA – https://www.gsa.gov/reference/gsa-privacy-program/privacy-and-contract-requirements.
10. Health Insurance Portability and Accountability Act – https://www.hhs.gov/hipaa/for-professionals/security/.
11. Ibrahim, Rouman, "Preparing for New Electronic Communication Privacy Laws," Information Systems Security Association Journal, Vol. 14(6), 2016.
12. Pettey, Christy, "Gartner Survey Shows US Consumers Have Little Security Concern with BYOD," Gartner, 2014 – https://www.gartner.com/newsroom/id/2739617.
13. Ponemon, Larry, "Cost of a Data Breach Study," IBM, 2016 – https://www.ibm.com/security/data-breach.
14. Overview of The Privacy Act of 1974 – https://www.justice.gov/opcl/conditions-disclosure-third-parties.
15. Romanosky, Sasha, Hoffman D., and Acquisti, A., "Empirical Analysis Of Data Breach Litigation, Journal of Empirical Legal Studies, Vol. 11(1), 2014.
16. Smith, Kevin and Tischler, R., Electronic Monitoring in the Workplace," Employment Relations Today, Vol.Ê42(1), 2015.
17. Sarbanes-Oxley Act – http://www.sec.gov/news/studies/principlesbasedstand.htm.
18. Taylor Lisa, "The Times They Are A-Changin': Shifting Social Norms and Employee Privacy in the Technological Era," Minnesota Journal of Law, Science and Technology, Vol. 15(2), 2014.
19. "Use of Government Information, Property, and Time," US Department of the Interior – https://www.doi.gov/ethics/use-of-government-property.
20. Wolff, Josephine and Lehr, W., "Ex-Post Mitigation Strategies for Breaches of Non-Financial Data," 44th Research Conference on Communication, Information and Internet Policy, 2016.
21. Yerby, Johnathan, "Legal and Ethical Issues of Employee Monitoring," Online Journal of Applied Knowledge Management, Vol. 1(2), 2013.

## About the Authors



*Amn Rahman is an engineer on the Growth team at Docker. This contribution is the outcome of her prior work at SRI International. She may be reached at amn.rahman@gmail.com.*

*Ashish Gehani is a Principal Computer Scientist at SRI International. His research focuses on data provenance and security. He may be reached at gehani@csl.sri.com.*