

1-1-2015

Managing Personal Device Use in the Workplace: How to Avoid Data Security Issues and the Dig Yourself out of Your Failed BYOD Policy

Andrew Freedman
Suffolk University Law School

Follow this and additional works at: <https://dc.suffolk.edu/jtaa-suffolk>



Part of the [Litigation Commons](#)

Recommended Citation

20 Suffolk J. Trial & App. Advoc. 284 (2015)

This Article is brought to you for free and open access by Digital Collections @ Suffolk. It has been accepted for inclusion in Suffolk Journal of Trial and Appellate Advocacy by an authorized editor of Digital Collections @ Suffolk. For more information, please contact dct@suffolk.edu.

MANAGING PERSONAL DEVICE USE IN THE WORKPLACE: HOW TO AVOID DATA SECURITY ISSUES AND TO DIG YOURSELF OUT OF YOUR FAILED BYOD POLICY

I. INTRODUCTION

First coined in 2001, the term the “Consumerization of Information Technology” describes the reorientation of the IT industry towards the immense potential of consumer technologies in lowering costs and improving corporate IT infrastructure.¹ This reorientation resulted from booming development in IT innovation and growth in the consumer market, requiring a firm to match the norms established by consumer technologies which have become the expectation of customers and employees.² Smartphones and tablets, with mainstream adoption outpacing any comparable technology in human history, have enabled employees to conduct business on the fly without the provision of business-use IT equipment by the employer.³ The consequence of this rampant innovation is the availability of sophisticated IT at the employee’s market level, with such sophistication at a magnitude that enables the “dual-use” of an employee’s personal consumer device for the conducting of the employer’s business.⁴

A recent survey by Cisco and Redshirt Research indicates that 48% of companies globally would not authorize the use of personal devices for work.⁵ The same survey also found that 57% of companies reported their

¹ See David Moschella, *What the Consumerization of IT Means to your Business, Ten Messages for CXOs*, LEADING EDGE FORUM (Jun. 23, 2011), <http://lef.csc.com/blog/post/2011/06/what-the-consumerization-of-it-means-to-your-business-ten-messages-for-cxos> (reviewing trend of consumerization of IT).

² See *id.* (noting firms must be “customer-centric” due to expectations employees have as consumers of technology).

³ See Michael Degusta, *Are Smart Phones Spreading Faster than Any Technology in Human History?*, MIT TECH. REV. (May 9, 2012), <http://www.technologyreview.com/news/427787/are-smart-phones-spreading-faster-than-any-technology-in-human-history/> (comparing smartphone and tablet consumer market penetration rates to penetration rates of other technologies).

⁴ See GARRY G. MATHIASON ET AL., LITTLER REP., THE ‘BRING YOUR OWN DEVICE’ TO WORK MOVEMENT: ENGINEERING PRACTICAL EMPLOYMENT AND LABOR LAW COMPLIANCE SOLUTIONS 1 (May 2012), available at <http://www.littler.com/files/press/pdf/TheLittlerReport-TheBringYourOwnDeviceToWorkMovement.pdf> (discussing prevalence of personal device use for business purposes in workplace).

⁵ See Michelle Drolet, *BYOD Brings on a War of Worry*, BOSTINNO (Jan. 25, 2013),

employees were nevertheless using personal devices without their employer's consent.⁶ Unrestricted and unregulated use of personal devices in the workplace exposes employers to significant liability; employers may be responsible for the safeguarding of sensitive, proprietary, or confidential information created or received in the course of business.⁷ In an effort to insulate itself from liability, an employer might then monitor and regulate personal devices used to conduct business on the employer's behalf, either unilaterally or through the implementation of a Bring Your Own Device ("BYOD") policy.⁸ In either undertaking, the employer risks exposure to liability for the violation of liberally-applied privacy laws now entering the workplace.⁹

This note will discuss the litigation of unauthorized access or privacy claims by employees generally, the mechanics of permissibly regulating employee personal device use in the workplace, and finally, the bastardization of anti-hacking and privacy laws wrongfully applied in the employment context. First, there will be a discussion outlining the sources of privacy and confidentiality obligations with respect to certain information through (i) state and federal law requirements and (ii) contractual confidentiality mandates.¹⁰ Then an employer's binate liabilities associated with personal device use in the workplace will be further distilled: (i) liability arising from the failure to safeguard, preserve, or destroy sensitive data; and (ii) liability arising from an employer's monitoring of employees to safeguard the aforementioned sensitive data.¹¹ With respect to the former, there will be a discussion of various confidentiality provisions commonly found in commercial contracts, as well as federal and Massachusetts law governing personal or confidential information.¹² In regards to the latter, this note will outline the relevant federal and state law and common law principles applicable to the monitoring of employees.¹³

<http://bostinno.streetwise.co/channels/byod-brings-on-a-war-of-worry/> (discussing reasoning for and mechanics of BYOD programs, and risk factors associated therewith).

⁶ See *id.* (discussing prevalence of prohibited personal device use by employees).

⁷ See *infra* Part II.B (outlining potential statutory and contractual obligations to safeguard certain information).

⁸ MATHIASON ET AL., *supra* note 4, at 1 (defining and rationalizing trend toward BYOD policy implementation).

⁹ See *infra* Part III (discussing liability inherent in monitoring employees); Part IV (arguing certain privacy laws are inappropriate to apply in BYOD context).

¹⁰ See *infra* Part II.

¹¹ See *infra* Parts II-III (outlining potential liability of employers in regards to sensitive information handled in course of business).

¹² See *infra* Part II.B (discussing confidentiality obligations incidental to modern business).

¹³ See *infra* Part III.

There will then be an analysis of an employer's potential litigation strategies pertaining to unauthorized access and privacy claims by aggrieved employees by way of analogy of the judicial treatment of claims arising from employer-owned device use.¹⁴ Further, there will be suggestions offered for employers wishing to insulate themselves from liability through the use of properly drafted employee policies, with conclusions regarding employee personal device use in the workplace in light of the liability it creates and the potential to mitigate it.¹⁵ Finally, editorial conclusions will be made regarding the inappropriate application of federal anti-hacking and privacy laws in the employment context.¹⁶

II. DATA SECURITY ISSUES IN THE COURSE OF MODERN BUSINESS

A. Causes and Implications of Security Breaches Resulting from Personal Device Use for Conducting Employer's Business

The past two decades have been accompanied by unprecedented data security breaches, both in scope and in damages.¹⁷ Recently, major retailers Home Depot and Target have fallen victim to various types of data security incidents.¹⁸ In just one quarter, Home Depot incurred forty-three million dollars in costs related to the compromising of fifty-six million credit cards and fifty-three million email addresses when hackers gained access to IT infrastructure using a vendor's login credentials.¹⁹ The data breach which compromised the credit cards of roughly twelve million Target customers through the installation of malicious software on credit card machines cost the company one hundred forty-eight million dollars in a single quarter.²⁰ While third party hacking caused these breaches, it has

¹⁴ See *infra* Part IV (providing litigation strategies for employers wishing to distinguish applicability of federal statutes).

¹⁵ See *infra* Parts IV-V (concluding that personal device use should be prohibited, but formally regulated if permitted).

¹⁶ See *infra* Part V (arguing CFAA and SCA wrongfully applied in employment contexts).

¹⁷ See *World's Biggest Data Breaches*, INFORMATION IS BEAUTIFUL (Feb. 5, 2015), <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/> (aggregating information on significant data breaches).

¹⁸ See *id.* (describing gravity of damages).

¹⁹ See The Home Depot, Inc., Quarterly Report (Form 10-Q), at 7 (November 2, 2014). Costs incurred were a result of identity protection and credit monitoring services offered to compromised shoppers, increased call center staffing, and legal and other professional services related to managing the breach. *Id.*

²⁰ See Rachel Abrams, *Target Puts Data Breach Costs at \$148 Million, and Forecasts Profit Drop*, N.Y. TIMES (Aug. 5, 2014), <http://www.nytimes.com/2014/08/06/business/target-puts->

been estimated that the average loss resulting from a security breach arising from any source is roughly \$7 million, averaging \$201 per lost or stolen record across major industries.²¹ On average, a data breach arising from a lost or stolen device costs eighteen dollars more per record than a data breach not arising from the same.²²

A study by the Ponemon Institute (financed by IBM) for 2013 and 2014 estimated that 31% of organizations experienced a data breach due to an employee's negligence, and 37% by a malicious or criminal attack.²³ What is quite problematic is that 46% of data breach incidents involved lost or stolen devices, including smartphones and tablets.²⁴ For example, in 2009 the U.S. Department of Veteran Affairs settled a lawsuit brought by veterans groups for twenty million dollars, after a laptop was stolen in 2006 which potentially exposed more than twenty-six million records.²⁵ More recently, Advocate Medical Group in Chicago gained infamy for its involvement in the second largest HIPAA violation in history after four unencrypted laptops containing Social Security numbers and dates of birth were stolen from an administrative building in July 2014, necessitating the notification of more than four million patients.²⁶ The aforementioned examples are just those worth mentioning; less notable data breaches involving lost or stolen devices happen quite frequently.²⁷

data-breach-costs-at-148-million.html?_r=0 (reporting on ramifications of Target data breach).

²¹ PONEMON INSTITUTE, 2014 COST OF DATA BREACH STUDY: UNITED STATES 2 (May 2014) *available at* http://www-935.ibm.com/services/multimedia/SEL03027USEN_Poneman_2014_Cost_of_Data_Breach_Study.pdf (quantifying financial losses resulting from security breaches). Businesses experiencing security breaches in 2013 and 2014 incurred on average \$3.2 million in lost business costs resulting from customer turnover, increased efforts to reacquire customers, and loss of reputation and goodwill. *Id.* The report cited provides further cost detail by industry in the Appendix attached hereto. *Id.*

²² See PONEMON INSTITUTE, *supra* note 21, at 9 (illustrating several factors that increase costs when present in data breach)

²³ See *id.* at 8 (summarizing common causes of data breaches).

²⁴ See *id.* at 9 (listing key factors affecting costs and of data breaches).

²⁵ See Terry Frieden, *VA Will Pay \$20 million to Settle Lawsuit Over Stolen Laptop's Data*, CNN (Jan. 27, 2009), <http://www.cnn.com/2009/POLITICS/01/27/va.data.theft/index.html?eref=onion> (discussing legal implications of stolen laptop of data analyst for U.S. Department of Veterans Affairs).

²⁶ See Patrick Ouellete, *Advocate Medical Group Endures Massive Data Breach*, HEALTH IT SECURITY (Aug. 27, 2013), <http://healthitsecurity.com/2013/08/27/advocate-medical-group-endures-massive-data-breach/> (reporting Advocate Medical Group data breach details).

²⁷ See Chronology of Data Breaches, PRIVACY RIGHTS CLEARINGHOUSE, www.privacyrights.org/data-breach (last updated Dec. 13, 2013) (select "Portable device (Port)" checkbox; select each "organization type(s)"; select each "year"; then select "GO!") (cataloging data breaches publicly reported). For example, on January 29, 2015, Riverside County Regional Medical Center in Moreno Valley, California provided twelve months of credit monitoring services following the theft of a laptop containing sensitive patient information used in its

Aside from the physical dispossession of a mobile device, other security risks include viruses, shared use with friends and family, and cloud computing.²⁸ Viruses and other malware account for 13% of security breaches, likely attributable to the 155% increase in volume for malware tailored for mobile devices from 2010 to 2011.²⁹ Shared use of a device with friends and family also poses a significant risk to corporate data security; the U.S. Treasury Department found that between 2003 and 2009, 27.5% of suspicious activity reports filed by depository institutions were instances where the victim of identity theft knew the thief, typically a friend, family member, or employee of the victim.³⁰ Finally, cloud computing poses a significant risk to employers in that sensitive information is uploaded and secured by third party vendors by the employee device, often without any oversight by the employer, potentially violating many of the federal regulations or contractual obligations that will be outlined in the proceeding paragraphs.³¹ Cloud services Evernote and Dropbox have been subject to data breach incidents in recent years, with the former requesting that fifty million (50,000,000) users change their passwords following an unsuccessful attempt to access the information of Evernote Business and Evernote Premium customers.³²

B. Obligations of Employers With Respect to Safeguarding Sensitive Information

1. Statutory Obligations to Secure Sensitive Information

Employers face both federal and state law mandates requiring adequate security of sensitive corporate data.³³ For example, data security

Ophthalmology and Dermatology clinics. *Id.* In December 23, 2014, Rob Kirby CPA in Santa Rosa, California suffered a data breach when his vehicle was broken into and a briefcase, laptop, and flash drive containing confidential information was stolen. *Id.* The query used to find this information returned 1073 breaches between 2005 and 2015. *Id.*

²⁸ See *id.* at 10-11 (outlining various security risks to storing corporate data on mobile devices).

²⁹ See JUNIPER NETWORKS, 2011 MOBILE THREATS REPORT 6 (Feb. 2012), available at http://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2011-mobile-threats-report.pdf?utm_source=promo&utm_medium=right_promo&utm_campaign=mobile_threat_report_0212 (discussing increasing risk and prevalence of malicious software).

³⁰ See MATHIASON ET AL., *supra* note 4, at 11 (finding that identity theft victims are often familiar with offender).

³¹ See MATHIASON ET AL., *supra* note 4, at 11-12. (warning employers of possible applicability of federal law to cloud storage); see also *infra* Part II.B (outlining federal and state law obligations to secure certain sensitive information).

³² See *World's Biggest Data Breaches*, *supra* note 17 (summarizing hacking incident).

³³ See, e.g., Security standards: General rules, 45 C.F.R. 164.306 (2013) (requiring "covered

mandates exist in two notable pieces of federal legislation: the Health Insurance Portability and Accountability Act (“HIPAA”) and the Gramm-Leach-Bliley Act.³⁴ HIPAA requires hospitals, healthcare providers, and insurers to implement administrative, physical, and technical safeguards for the security of “protected health information.”³⁵ The Gramm-Leach-Bliley Act similarly requires the protection of information created or received by a financial institution in connection with the customer relationship.³⁶

States have also imposed broad obligations on businesses that collect or store sensitive information.³⁷ Massachusetts imposes upon every person the obligation to implement appropriate safeguards to protect information about a resident.³⁸ Recognizing the increased risk posed by the use of mobile devices in the workplace, Massachusetts regulations specifically require security safeguards for personal information stored on laptops or other portable devices.³⁹ The Massachusetts Attorney General has enforced these regulations against businesses failing to abide by imposed information security obligations, obtaining monetary penalties in some instances.⁴⁰

entities” to “ensure the confidentiality, integrity, and availability of all electronic protected health information ... [p]rotect against any reasonably anticipated threats or hazards to security ... [p]rotect against any reasonably anticipated uses or disclosures of such information that are not permitted ... [e]nsure compliance with this subpart by its workforce”); Gramm-Leach-Bliley Act 15 U.S.C. § 6801 (2013) (requiring broadly defined “financial institutions” to “insure the security and confidentiality of customer records and information ... [to] protect against any anticipated threats or hazards to the security or integrity of such records ... [and to] protect against unauthorized access to or use of such records or information....”); 201 MASS. CODE REGS. 17.00 (2015) (implementing Massachusetts law requiring safeguarding of personal information of Massachusetts citizens).

³⁴ See sources cited, *supra* note 33 (establishing benchmarks for corporate held data).

³⁵ 45 C.F.R. 164.302-164.306 (2013) (defining security standards and mandating the implementation of safeguards and security procedures).

³⁶ 15 U.S.C. §§ 6801-09 (2014) (imposing security mandates for information created or received by financial institutions); see MATHIASON ET AL., *supra* note 4, at 12 (“[F]inancial institution [includes] not only banks but also car dealerships that extend credit and even some travel agencies....”).

³⁷ See *infra* notes 38-46 and accompanying text (outlining employer’s statutory obligations to secure sensitive information).

³⁸ 201 MASS. CODE REGS. § 17.03 (2015) (requiring administrative, technical, and physical safeguards” for personal devices).

³⁹ See 201 MASS. CODE REGS. 17.04(5) (2013) (requiring “encryption of all personal information stored on laptops or other portable devices”); *supra* Part II.A (discussing security breaches caused by malicious software).

⁴⁰ See Ellen Giblin, *Massachusetts Extends Reach of Data Protection Regulations, WORKPLACE PRIVACY COUNSEL* (May 18, 2011), available at <http://www.littler.com/2011/05/articles/state-law-claims/massachusetts-extends-reach-of-data-protection-regulations> (noting new causes of action available for security breach victims where private action previously nonexistent). The enforcement cited in the article, based upon a violation of Chapter 93A consumer protection law, resulted in a judgment against The Briar

Massachusetts, and forty-six other states, requires notification of security breaches involving personal information.⁴¹ A person or agency storing personal information is required to notify the victim of a security breach and the Attorney General if it knows or has reason to know of a security breach or that information was acquired or used by an unauthorized person.⁴²

When protected information is disseminated without an employer's knowledge, an employee may expose the employer to liability for failing to safeguard information in a manner required by law.⁴³ The previously cited Massachusetts Regulation section 17.03 requires entities holding personal information to develop and implement security programs and to oversee security providers.⁴⁴ If the protected information is uploaded to Dropbox, a consumer cloud-based storage provider who has suffered its own data breach, the employer has not taken steps to oversee, select, or retain its third party service provider, nor has it required the service provider by contract to safeguard the information as required by law.⁴⁵ Further,

Group, a restaurant chain, for:

(a) failing to change default usernames and passwords on its point-of-sale computer system, (b) allowing multiple employees to share common usernames and passwords, (c) failing to properly secure its remote access utilities and wireless network, (d) continuing to accept credit and debit cards from customers after the company knew that its systems were compromised but had not yet been secured, (e) storing payment card personal information in clear (*i.e.*, unencrypted) text on its servers ...

Id. Giblin suggests that the judgment's basis on the consumer protection law, Chapter 93A, is indicative of the potential for private causes of action by residents, provided that harm resulting from failure to comply with the data security regulations can be proven. *Id.*

⁴¹ See NAT'L CONF. OF STATE LEGISLATURES, *State Security Breach Notification Laws*, available at <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx> (last updated Aug. 20, 2012) (listing state statutes requiring notification of security breaches involving personal information).

⁴² MASS. GEN. LAWS ch. 93H, § 1-3 (2012) (explaining obligations of entity maintaining or storing resident's personal information to notify of breach). Notification is only required upon a "breach of security," where "unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security ..." is acquired without authorization. See MASS. GEN. LAWS ch. 93H §§ 1(a), 3(a)-3(b) (2012).

⁴³ See MASS. GEN. LAWS ch. 93H, §§ 1-3. Notwithstanding instances where the employer has utilized Mobile Device Management Software (MDM) to restrict transfer or use of protected information on the employee-owned personal device. See MATHIASON ET AL., *supra* note 4, at 11 (discussing issues regarding unbridled dissemination of protected information); see also *supra* Part II.A.

⁴⁴ 201 MASS. CODE REGS. 17.03(2)(f)(1)-(2) (2013) ("[R]easonable steps [taken] to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information ... [and] [r]equiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information . . .").

⁴⁵ See *id.* (requiring certain measures to ensure information security); see also MATHIASON

because Massachusetts requires encryption of data disseminated to portable devices such as laptops and smartphones, the employer will have failed to adequately encrypt data that its employee has now disseminated.⁴⁶

2. Contractual Obligations to Secure Sensitive Information

Common in commercial contracts are obligations to safeguard the confidential information disclosed in the course of the performance of an agreement, with such obligations arising in the contract itself or under a nondisclosure agreement ancillary thereto.⁴⁷ These provisions may require that information be kept in strict confidence, using language similar to the following:

Consultant agrees to retain and maintain in strict confidence, and to require its representatives, agents, employees, officers, directors, shareholders, partners, principals, successors, assignees, members, affiliates, consultants, or professional representatives and advisors to retain in confidence any and all Confidential Information of the Company. Consultant agrees that, without the prior express written consent of the Company, Consultant shall not, either directly or indirectly, individually or in concert with others: (i) Disclose any such Confidential Information to any other Person; (ii) use any such Confidential Information for the benefit of any Person other than the Company; or (iii) permit any Confidential Information to be Disclosed to or used by any Person other than the Company.⁴⁸

Less draconian, and frankly, likely to be less offensive in

ET AL., *supra* note 4, at 11 (discussing risk associated with unregulated transfer of protected information disseminated to employees' personal devices). Dropbox itself suffered a data breach when one of its own employee's Dropbox account containing customer information was compromised. See *Dropbox Confirms Security Breach*, INFORMATION AGE (Aug. 1, 2012), <http://www.information-age.com/technology/security/2114488/dropbox-confirms-security-breach> (reporting Dropbox data breach and its cause).

⁴⁶ See *supra* notes 43-45 and accompanying text (defining obligations of person holding personal information of a resident to notify upon breach).

⁴⁷ Jere M. Webb, *A Practitioner's Guide to Confidentiality Agreements*, at 1, <http://www.stoel.com/files/confidentialityagreementguide.pdf> (stating that use of confidentiality agreements has become pervasive).

⁴⁸ ALAN GUTTERMAN, BUSINESS TRANSACTIONS SOLUTIONS §107:72 (2015) (providing sample confidentiality provision based upon standard of reasonableness).

negotiation, would be the following mutually protective language to safeguard confidential information using a standard of reasonableness:

Both parties acknowledge that, by reason of their relationship, they may have access to certain information and materials concerning the other's business, plans, and products (including, but not limited to, information and materials contained in technical data provided to the other party) which is confidential and of substantial value to the other party, which value would be impaired if such information were disclosed to third parties. Neither party shall use in any way, for their own account or the account of any third party, nor disclose to any third party, any such confidential information which is disclosed in written form to it by the other party hereto, without written authorization from the other party. If information is disclosed verbally, in order for it to be deemed confidential information it must be followed by a written summary within [number of days] days of such disclosure. Each party will take every reasonable precaution to protect the confidentiality of such information consistent with the efforts exercised by it with respect to its own confidential information. Each party shall advise the other if it considers any particular information or materials to be confidential. This provision shall survive termination of this Agreement.⁴⁹

In the event of a data breach, or other prohibited disclosure during the normal course of business, an employer permitting the use of personal devices to conduct business on its behalf without sufficient regulation or security would certainly constitute a breach in the first contract cited, and would likely constitute a breach in the second contract cited.⁵⁰

⁴⁹ *Id.* §120:244 (providing sample confidentiality provision requiring strict maintenance of information confidentiality).

⁵⁰ *See id.* (citing provision requiring parties to take reasonable precaution to protect confidential information); *see also id.* §120:244 (citing provision requiring parties to maintain confidential information in strict confidence).

C. Employer Obligations to Destroy or Retain Information on Employee-Owned Devices Used for Conducting Employer's Business

1. Statutory Obligations to Destroy or Retain Information

Massachusetts, along with twenty-eight other states, requires businesses and agencies to destroy or erase personal information in a manner that it cannot be practicably read or reconstructed.⁵¹ Employers holding personal information of Massachusetts residents face fines up to \$50,000 per instance of improper disposal of personal information.⁵² As data is unknowingly disseminated to personal devices, an employer's compliance with the statute is increasingly frustrated due to the difficulty in accounting for all pieces of unregulated, disseminated data that may require proper destruction.⁵³

In contrast, employers have a duty to preserve information as evidence when litigation is "pending or reasonably foreseeable."⁵⁴ The Massachusetts Rules of Civil Procedure require the production of potential evidence which is in the "possession, custody or control" of the party upon whom the request is served.⁵⁵ The First Circuit has held that a party has control over evidence "if that party has a legal right to obtain those

⁵¹ See MASS. GEN. LAWS ch. 93I, § 2 (2012) (promulgating "minimum standards for proper disposal of records containing personal information"). Personal information is defined as "a resident's first name [or initial] and last name ... in combination with any 1 or more of the following ... (a) Social Security Number; (b) driver's license number ... ; (c) financial account number, or credit or debit card number ... ; or a (d) biometric indicator." § 1 (defining personal information subject to data disposal requirements); see NAT'L CONF. OF STATE LEGISLATURES, *Data Disposal Laws*, <http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx> (last updated Jan. 21, 2015) (listing states imposing minimum standards on businesses and government agencies for data disposal).

⁵² See MASS. GEN. LAWS ch. 93I, § 2 (establishing penalties for failure to comply with proper data disposal requirements).

⁵³ See generally, MATHIASON ET AL., *supra* note 4, at 12-30. (discussing data related issues of employee personal device use).

⁵⁴ See *Silvestri v. Gen. Motors Corp.*, 271 F.3d 583, 590 (4th Cir. 2001) (discussing spoliation of evidence); see also *Kronisch v. U.S.*, 150 F.3d 112, 126 (2d Cir. 1998) ("[T]he party having control over the evidence must have had an obligation to preserve it at the time it was destroyed. This obligation to preserve evidence arises ... also on occasion in other circumstances, as for example when a party should have known that the evidence may be relevant to future litigation."). The Massachusetts Rules of Civil Procedure are "interpret[ed] ... consistently with ... their Federal counterparts absent compelling reasons to the contrary or significant differences in content." *Strom v. Am. Honda Motor Co., Inc.* 667 N.E.2d 1137, 1140-41 (Mass. 1996) (citation omitted) (quoting *Solimene v. B. Grauel & Co., KG*, 507 N.E.2d 662, 668 (Mass. 1987) and *Rollins Env'tl. Servs., Inc. v. Super. Ct.*, 330 N.E.2d 814, 818 (Mass. 1975)) (noting discovery issues at bar "follow the course of federal decisions where they seem sensible").

⁵⁵ See MASS. R. CIV. P. 34(a)(1) (codifying party's ability to request production of documents or electronically stored information).

documents,” rather than considering legal ownership as the determining factor.⁵⁶ The First Circuit also requires notice to opposing parties of the existence of evidence controlled by third parties.⁵⁷ If the employer fails to take the appropriate measures to preserve information within its or a third party’s control, it may be subject to spoliation sanctions during litigation.⁵⁸

2. Contractual Obligations to Destroy or Return Sensitive Information

Common in confidentiality provisions is the obligation to return or certify the destruction of the disclosing party’s confidential information.⁵⁹ More than half of employees have stored, transferred, or modified their employers’ documents on employee personal devices.⁶⁰ Of course, it would be quite difficult to certify the destruction of information, or to corral information to return to the discloser if such information was freely distributed among the receiving party’s employees or officers and their personal devices.⁶¹

III. LIABILITY ARISING FROM EMPLOYER MONITORING AND ACCESS OF EMPLOYEE PERSONAL DEVICES USED TO CONDUCT EMPLOYER’S BUSINESS

A. Statutory Protections Against Certain Electronic Access or Intrusions

Given the immense liability associated with the dissemination of

⁵⁶ See MATHIASON ET AL., *supra* note 4, at 57 (defining control in context of evidence subject to discovery).

⁵⁷ See *Velez v. Marriot PR Mgmt., Inc.*, 590 F. Supp. 2d 235, 258 (D.P.R. 2008) (“Litigants have the responsibility of ensuring that relevant evidence is protected from loss or destruction [and this] ... duty extends to giving notice if the evidence is in the hands of third parties.”).

⁵⁸ See *Micron Tech., Inc. v. Rambus Inc.*, 645 F.3d 1311, 1320 (Fed. Cir. 2011) (“[N]oting that [a] spoliation sanction is proper where (1) a party has a duty to preserve evidence because it knew, or should have known, that litigation was *imminent*, and (2) the adverse party was prejudiced by the destruction of the evidence.”) (internal quotation marks omitted).

⁵⁹ See *Return or Destruction of Confidential Information*, CONTRACT STANDARDS, <http://www.contractstandards.com/clauses/return-or-destruction-of-confidential-information> (select “Discloser” hyperlink) (providing sample contract language and noting prevalence of destruction or return mandates).

⁶⁰ See Tom Kaneshige, *Confidential Data is Leaving on Workers’ Mobile Devices*, CIO (Aug. 29, 2013), <http://www.cio.com/article/2382912/byod/confidential-data-is-leaving-on-workers-mobile-devices.html> (arguing that few employees, especially millennials, are aware of their company’s BYOD policy).

⁶¹ See *id.* (noting BYOD policies may not safeguard employer because employees “play loose with corporate documents”).

various types of protected information, employers may wish to monitor the activity of personal devices when used for business purposes.⁶² Extensive monitoring of employer-owned equipment has been commonplace for several years now, with sixty-six percent of employers monitoring employee internet use, forty-three percent monitoring email, and sixteen percent recording phone calls.⁶³ Such monitoring however, may be subject to statutory protections against unauthorized access by the employer or an employee's expectation of privacy.⁶⁴ It is therefore worth noting that sixteen percent of employers do not apprise employees of phone conversation monitoring, and twenty-seven percent of employers do not notify that voicemails are monitored.⁶⁵ Further, the use of the personal device for conducting business may enhance the employer's exposure to liability for an employee's inappropriate use of the device.⁶⁶

Enacted in 1986, the Computer Fraud and Abuse Act ("CFAA") imposes criminal and civil liability for whoever "having knowingly accessed a computer without authorization or exceeding authorized access . . . obtain[ing] information . . . from a protected computer," or "intentionally accesses a protected computer without authorization, and as a result . . . causes damage and loss."⁶⁷ While "exceeding authorization" is defined in

⁶² See *infra* Part IV (providing preventative measures with respect to unauthorized access or employee privacy claims); see also Moschella, *supra* note 1 (discussing risks posed by BYOD programs and employer efforts to mitigate them).

⁶³ See *The Latest on Workplace Monitoring and Surveillance*, AMERICAN MANAGEMENT ASSOCIATION, (last updated Nov. 17, 2014), available at <http://www.amanet.org/training/articles/The-Latest-on-Workplace-Monitoring-and-Surveillance.aspx> (presenting survey findings on percentage of employers monitoring employees).

⁶⁴ See *infra* Part III.A (outlining liability of employer for unauthorized access, and providing arguments for their defense, respectively).

⁶⁵ See *The Latest on Workplace Monitoring and Surveillance*, *supra* note 63 (noting trends regarding employers informing personnel regarding certain monitoring).

⁶⁶ MATHIASON ET AL., *supra* note 4, at 35-39 (discussing effect of personal device use on employer liability for hostile work environment and discrimination). While an employer's liability exposure in this regard may or may not be enhanced by the use of personal devices, for the purposes of this Note, it is assumed that the use of personal devices at the very least accords the same risk to employers as employer-owned devices. See *id.* (same).

⁶⁷ 18 U.S.C. § 1030(a) (2013). Congress cited the proliferation of computers and digital data in American society that has led to the "creat[ion] of a new type of criminal—one who uses computers to steal, to defraud, and to abuse the property of others." S. REP. NO. 99-432, at 2480 (1986) (justifying need for criminalization of computer-based frauds and abuses); see §§ 1030(a)(2)(C), (a)(5)(C) ("[I]mposing criminal and civil liability for] access[ing] a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information . . . causing damage or loss"). Exceeding authorized access is defined as accessing "a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." § 1030(e)(6) (2013). Computers are defined in the statute as an "electronic... or other high speed data processing

the statute, “without authorization” is not.⁶⁸ Because the statute could reasonably be construed quite broadly, Congress was concerned with the potential applicability of the statute to innocuous computer access, and included safeguards such as a damages threshold or scienter requirement.⁶⁹ Further, all fifty states have laws paralleling the CFAA, typically in the

device ... and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” 18 U.S.C. § 1030(e)(1) (defining “computer”). Acknowledging that the language of the statute is exceedingly broad, courts have found that the definition “captures any device that makes use of a [sic] electronic data processor, examples of which are legion.” *United States v. Kramer*, 631 F.3d 900, 902 (8th Cir. 2011) (finding that cellular phones are within contemplation of the CFAA’s definition of “computer”). A computer is “protected” if it “is used in or affecting interstate or foreign commerce or communication” § 1030(e)(2)(B) (defining “protected computer”).

⁶⁸ See *Advanced Micro Devices, Inc. v. Feldstein*, 951 F. Supp. 2d 212, 217-18 (D. Mass. 2013) (noting First Circuit has not articulated position on breadth of interpretation of “without authorization.”); *Guest-Tek Interactive Entm’t, Inc. v. Pullen*, 665 F. Supp. 2d 42, 43 (D. Mass. 2009) (recognizing that “without authorization” is not defined in the CFAA). Some First Circuit courts, as well as other circuits, advocate a narrower interpretation of “without authorization” under the CFAA. See *Advanced Micro Devices, Inc.*, 951 F. Supp. 2d at 217; see also *LVR Holdings LLC v. Brekka*, 581 F.3d 1127, 1132-33 (9th Cir. 2009) (using “plain language of the statute” and dictionary definition of “authorization” to determine violation). Although *Advanced Micro Devices, Inc.* involved 18 U.S.C. § 1030(a)(4), requiring intent to defraud, the Court recognized the lack of articulation by the First Circuit regarding the breadth of interpretation for application of the CFAA, before ultimately deciding to use a narrow interpretation. See *Advanced Micro Devices, Inc.*, 951 F. Supp. 2d at 217. Other First Circuit courts have used a broader interpretation, a product of the lack of a definition provided by the statute. See *Guest-Tek Interactive Entm’t, Inc.*, 665 F. Supp. 2d at 45 (recognizing that “without authorization” is not defined in the CFAA); see also *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 582-84 (1st Cir. 2001) (finding former employees, despite previous authorization, violated CFAA for access without authorization). The *Guest-Tek* court ultimately recognized the First Circuit Court of Appeals’ other broad interpretations of the CFAA, finding that wherever an employee breaches a contractual obligation, their authorization to access information stored on an employer’s computer terminates and all subsequent access is unauthorized. See *Guest-Tek Interactive Entm’t, Inc.*, 665 F. Supp. 2d at 45 (“Employers ... are increasingly taking advantage of the CFAA’s civil remedies to sue former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer’s computer system.”); cf. *United States v. Morris*, 928 F.2d 504, 506-07 (2d Cir. 1991) (finding that “intentionally” within the meaning of statute, refers to access, rather than damage).

⁶⁹ See S. REP. NO. 99-432, at 2489 (1986) (rationalizing need for limited applicability of CFAA to any instance involving data modification by another). The Senate Report goes on to state that “[s]ome modifications or alterations, while constituting ‘damage’ in a sense, do not warrant felony-level punishment, particularly when almost no effort or expense is required to restore the affected data to its original condition.” *Id.* at 2488. Further, Congress intended § 1030(a)(5) to be applied broadly to “‘outsiders,’ i.e., those lacking authorization to access any Federal interest computer” as it removed intentionality requirements for outside hackers. See *id.* (explaining intended applicability of act); see also S. REP. NO. 104-357, at *10-11 (1996) (explaining intentionality requirement distinction between insiders and outsiders). The Committee noted that insiders would face liability only if damage was intentionally caused, not recklessly or otherwise. S. REP. NO. 104-357, at *11.

form of criminal statutes allowing for civil remedies.⁷⁰ The Massachusetts statute prohibits “knowingly access[ing] a computer system by any means, or after gaining access to a computer system by any means know[ing] that such access is not authorized and fails to terminate such access. . . .”⁷¹

As part of the Electronic Communications Privacy Act (ECPA), the Stored Communications Act (SCA) provides criminal penalties for anyone who intentionally accesses electronically stored information without or exceeding authorization.⁷² Similarly, the ECPA provides a private right of action against whoever “intentionally intercepts, [or] endeavors to intercept . . . any wire, oral, or electronic communication” without the consent of the plaintiff.⁷³ As a result, all attempts to monitor, intercept, or access without authorization, a service that provides users the ability to send or receive wire or electronic communications, are impermissible under the SCA and ECPA.⁷⁴ In the First Circuit, the beneficiary of the consent exception has the burden of proving consent was

⁷⁰ See NAT’L CONF. OF STATE LEGISLATURES, *Computer Crime Statutes*, <http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx> (last updated Jun. 27, 2014) (listing states with computer trespass and hacking statutes).

⁷¹ MASS. GEN. LAWS ch. 266, § 120F (2012) (invoking criminal liability for knowingly accessing computer without authorization, and failing to terminate such access). Violations of the statute are found for each unauthorized login to the computer, rather than violations for each document accessed. See *Commonwealth v. Piersall*, 853 N.E.2d 210, 248 (Mass. App. Ct. 2006) (setting aside separate convictions for each email accessed, and upholding convictions for each login).

⁷² 18 U.S.C. § 2701(a) (2012) (“[W]hoever intentionally accesses without authorization a facility through which an electronic communication service is provided; or intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided under subsection (b). . . .”).

⁷³ 18 U.S.C. §§ 2511(1)(a), 2520 (2012). The ECPA and SCA share definitions for relevant terms, such as “electronic communications” and “electronic communications service.” 18 U.S.C. §§ 2510-2511 (2013) (providing definitions for ECPA & SCA terms). The consent exception to § 2511(1)(a) is as follows: “where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act. . . .” § 2511(2)(d). “Federal courts have equated ‘consent’ under the Wiretap Act with ‘authorization’ under the Stored Communications Act.” *Pietrylo v. Hillstone Rest. Grp.*, No. 06-5754(FSH), 2008 WL 6085437, at *3 (D.N.J. July 25, 2008).

⁷⁴ See 18 U.S.C. § 2701(a) (2012) (prohibiting unauthorized access or access exceeding authority of electronic communications service); § 2510(15) (defining “electronic communications service”). “Electronic communications” are defined as a “transfer of signals . . . sounds, data, or intelligence of any nature transmitted . . . by a wire, radio, [or] electromagnetic . . . system that affects interstate or foreign commerce” 18 U.S.C. § 2510(12) (2012). Excluded from this definition are communications from a tracking device, relevant for a later discussion of employers wishing to monitor the location of employees through an employee’s personal device used for business purposes. Cf. 18 U.S.C. § 2510(12) (2012).

received, and this exception is to be construed broadly.⁷⁵ Claims asserting SCA violations typically result from the accessing of a web-based email, discussion forum, or data storage service by an unauthorized party.⁷⁶ Further, applicability of the statute typically hinges on definitional interpretations of “facility” and “electronic storage,” as the statute is vague and has been interpreted in varying breadths.⁷⁷

B. Public Employee Expectations of Privacy in Employee Personal Devices Used to Conduct Employer’s Business

Public employees enjoy constitutional privacy protections, and can invoke the Fourth Amendment against state and federal government employers.⁷⁸ In order to maintain a legal right to privacy, a person must

⁷⁵ See *In re Pharmatrak, Inc.*, 329 F.3d 9, 19 (1st Cir. 2003) (examining consent exception to ECPA and lack of articulated position of pleading burden regarding consent). The *Pharmatrak* court suggests the burden is on the party seeking to benefit from the consent exception, as the prosecution was the beneficiary and had the burden to prove consent. *In re Pharmatrak, Inc.*, 329 F.3d at 19. In a New Jersey federal district court, the consent exception to the SCA was not fulfilled despite an employer’s claims that it had received verbal consent from the employee prior to accessing an online discussion forum using the employee’s provided login credentials. *Pietrylo*, 2008 WL 6085437, at *3-4 (awarding punitive damages against employer for violating SCA despite employee’s verbal consent). But see *Griggs-Ryan v. Smith*, 904 F.2d 112, 116 (1st Cir. 1990) (“Congress intended the consent requirement to be construed broadly.”).

⁷⁶ See *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC*, 759 F. Supp. 2d 417 (S.D.N.Y. 2010) (considering SCA violation with respect to employer access of employee’s personal web-based email account). In *Pure Power Boot Camp, Inc.*, an employer logged in to several of the former employee’s web-based email services using the log-in credentials stored in the computer, and subsequently discovered the former employee’s intentions of starting a new business. See *Pure Power Boot Camp, Inc.*, 759 F. Supp. 2d at 420. The employer sued the former employee, seeking to enjoin the opening of a competing business, resulting in the former employee’s counterclaim based on violations of the SCA. *Id.* at 421-22. The court granted summary judgment in the employee’s favor, finding violations of the SCA for each of the employee’s web-based email services accessed by the employer. *Id.* at 432.

⁷⁷ See *Mahoney v. DeNuzzio*, No. 13-11501-FDS, 2014 WL 347624, at *4 (D. Mass. Jan. 29, 2014) (citing interpretation dichotomies of “in electronic storage” and “facility”). *Mahoney* first cites courts finding “that using a computer to obtain access to an email on a server without authorization falls within the ambit of the SCA.” *Id.*; see *Cheng v. Romo*, No. 11-10007-DJC, 2013 WL 6814691 (D. Mass. Dec. 20, 2013) (determining “electronic storage” definition applied to e-mails on Yahoo! server); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1057 (N.D. Cal. 2012) (“[T]he computer system of an email provider ... or an ISP are uncontroversial examples of facilities that provide electronic communications services to multiple users....”).

⁷⁸ See *Nat’l Treasury Emps. Union v. Von Raab*, 489 U.S. 656, 665 (1989) (holding Fourth Amendment is applicable to government employers); *O’Connor v. Ortega*, 480 U.S. 709, 717 (1987) (“[I]ndividuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer....”); see also *Skinner v. Ry. Labor Exec. Ass’n*, 489 U.S. 602, 612-14 (1989) (“[T]he [Fourth] Amendment guarantees privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government or those acting at their direction....”).

have a subjective expectation of privacy, and that expectation must be objectively reasonable.⁷⁹ In a plurality opinion, the court established two analytical frameworks for determining the reasonable privacy expectations of government employees.⁸⁰ The first framework determined expectations of privacy first by examining the “operational realities of the workplace”, necessitating a case-by-case review to determine the reasonableness of the employee’s expectation.⁸¹ If a legitimate privacy expectation exists, a government employer’s intrusion for “noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct” is judged by a standard of reasonableness under the circumstances.⁸²

Justice Scalia established a different approach in his concurrence, dispensing with the “operational realities” approach, and concluded “that the offices of government employees . . . are covered by the Fourth Amendment as a general matter.”⁸³ Scalia continued, noting “government searches to retrieve work-related materials or to investigate violations of workplace rules” do not violate the Fourth Amendment, provided that these searches would be normal and reasonable if performed by a private employer.⁸⁴

Employee expectations of privacy in employer-owned equipment are fully examined in *City of Ontario v. Quon*,⁸⁵ where Quon, a city police officer was found not to have a legitimate expectation of privacy in an employer-owned, alphanumeric pager capable of sending text messages.⁸⁶ Quon was told of a universal policy that the employer “reserves the right to monitor and log all network activity including e-mail and internet use, with

⁷⁹ See *Katz v. United States*, 389 U.S. 347, 360-61 (1967) (Harlan, J., concurring) (proffering what was subsequently adopted as test for determining existence of legitimate expectations of privacy). This precedent was, however, established in contemplation of criminal investigations, and due to the “special needs, beyond the normal need for law enforcement,” the warrant and probable-cause requirement of the Fourth Amendment is “impracticable” for government employers. See *O'Connor*, 480 U.S. at 724-25; see also *City of Ontario v. Quon*, 560 U.S. 746, 756-57 (2010) (recognizing precedent finding employers have needs distinguishable from typical Fourth Amendment application).

⁸⁰ See *O'Connor*, 480 U.S. at 725-32.

⁸¹ See *id.* at 717-18. Operational realities can diminish an employee’s expectation of privacy, which should be taken into consideration when assessing the reasonableness of a workplace search. See *Von Raab*, 489 U.S. at 671 (finding urine testing did not violate employee right to privacy).

⁸² *O'Connor*, 480 U.S. at 725-26.

⁸³ *Id.* at 731 (Scalia, J., concurring).

⁸⁴ *Id.* at 732.

⁸⁵ 560 U.S. 746 (2010).

⁸⁶ *City of Ontario v. Quon*, 560 U.S. 746, 750-51 (2010). Quon was a member of the City’s SWAT team, and was given the device to better accommodate the exigencies of responding to emergency situations. *Id.*

or without notice. *Users should have no expectation of privacy or confidentiality when using these resources.*⁸⁷ After Quon was notified of recurring overage charges from the excessive use of his pager, his messages were audited without notice, incidentally revealing that he was sending sexually explicit text messages while on-duty.⁸⁸ Quon was disciplined by his employer, to which he responded with a claim alleging violation of his Fourth Amendment rights and the SCA.⁸⁹ The Supreme Court overruled the Ninth Circuit, stating that Quon had no reasonable expectation of privacy in the employer-owned device, and even if he did, the Fourth Amendment was not violated by obtaining and reviewing the transcripts.⁹⁰ The Court reasoned that the search was predicated on reasonable grounds for the employer to believe a search was necessary for a “noninvestigatory work-related purpose,” and that the search was “‘reasonably related to [its] objectives . . . and not excessively intrusive in light of’ the circumstances giving rise to the search.”⁹¹

C. Private Employee Expectations of Privacy in their Employee-Owned Devices Used for Conducting Business

The aforementioned invocation of the Fourth Amendment may not be asserted to claim a right to privacy in the private employer context; the right to privacy in private employment is subject to state statutes and common law protections from invasions of privacy.⁹² In Massachusetts, an

⁸⁷ *Id.* at 751.

⁸⁸ *Id.* at 752-53. The message transcripts were requested and audited by the employer to determine if the current service contract, possibly not substantial enough, was charging for work-related or personal use. *Id.*

⁸⁹ *Id.* at 753-54.

⁹⁰ *Id.* at 760-61. The Court first looked to the operational realities, noting the importance of the consistency and presentation of employer policies, the perceived authority of those establishing the policies, as well as the justifications for the search. *Id.* at 760-61. Justice Scalia again joined the opinion except for Part III-A of the opinion which used the “operational realities” framework for determining the permissibility of the search. *Id.* at 767-69 (Scalia, J., concurring in part and concurring in judgment). Justice Scalia advocated his threshold inquiry that the Fourth Amendment “applies *in general* to such messages on employer-issued pagers,” rather than inquiring as to whether the Fourth Amendment applies to messages on *public* employees’ employer-issued pagers.” *Id.* at 767.

⁹¹ *City of Ontario*, 560 U.S. at 761 (finding search by Quon’s employer to be reasonable).

⁹² See *Folmsbee v. Tech Tool Grinding & Supply, Inc.*, 630 N.E.2d 586, 589 (Mass. 1994) (“[B]ecause [plaintiff’s employer] is a private employer, [plaintiff’s] rights under art. 14 of the Massachusetts Declaration of Rights and the Fourth Amendment to the United States Constitution are not implicated.”); *Bally v. Northeastern Univ.*, 532 N.E.2d 49, 51 n.3 (Mass. 1989) (“Bally asserts his rights under the statutes because he proceeds here against a private institution.”). In *Folmsbee*, a drug testing policy was found not to invade the employee’s privacy given the nature of the employer’s business, the evidence of employee drug use, and the procedural safeguards in

employee has “a right against unreasonable, substantial or serious interference with his privacy.”⁹³ This right to privacy, however, is subject to the “legitimate countervailing business interests” of the employer, allowing for disclosure of personal information reasonable in certain situations.⁹⁴ Relevant factors in determining the gravity of the employer’s interest include the nature of the employer’s business and the specific employee’s duties, as well as the interest in protecting corporate property and preventing corporate liability.⁹⁵

IV. ANALYSIS

Given the aforementioned liabilities arising from employee personal device-use in the workplace, employers must decide whether to outright prohibit the use of employee-owned devices to conduct business, allow such device use to continue unregulated, or to construct a personal device-use policy, typically referred to as a BYOD policy.⁹⁶ The proceeding sections will analyze to what extent, if at all, the use of employee-owned devices, rather than employer-owned devices, changes an employee’s expectation of privacy, and sovereignty over their devices, and the resultant effect this has on defense litigation regarding invasion of privacy and unauthorized access claims against an employer.⁹⁷ Further, recommendations will be made for employers wishing to insulate themselves from liability arising from the sanctioned or unsanctioned use of personal devices in the workplace.⁹⁸ Upon conclusion of this analysis, it

place to guarantee privacy in the intrusion. *Folmsbee*, 630 N.E.2d at 590.

⁹³ MASS. GEN. LAWS ch. 214, § 1B (2012) (“A person shall have a right against unreasonable, substantial or serious interference with his privacy. The superior court shall have jurisdiction in equity to enforce such right and in connection therewith to award damages.”).

⁹⁴ See *Bratt v. Int’l Bus. Machs. Corp.*, 467 N.E.2d 126, 135 (Mass. 1984) (holding that required answering of questionnaire used as basis for psychiatric evaluation violated privacy rights). But cf. *Hastings & Sons Publ’n Co. v. Treasurer of Lynn*, 375 N.E.2d 299, 303-04 (Mass. 1978) (“[E]ven if disclosure of municipal payroll records would bring the right of privacy into play, the paramount right of the public to know what its public servants are paid must prevail.”).

⁹⁵ See *Bratt*, 467 N.E.2d at 135 (“[T]he employer’s legitimate interest in determining the employees’ effectiveness in their jobs should be balanced against the seriousness of the intrusion on the employees’ privacy.”); see also *Webster v. Motorola, Inc.*, 637 N.E.2d 203, 206-08 (Mass. 1994) (finding employer’s interest sufficient to justify intrusion). *Webster* involved employees with two different positions, necessitating separate determinations of reasonableness based upon factual inquiries as to the peculiarities of the job duties of each employee and the interests of the employer served by the intrusion. *Webster*, 637 N.E.2d at 207-08.

⁹⁶ Cf. sources cited *supra* notes 3-8 and accompanying text (discussing BYOD trend and its impact).

⁹⁷ See *supra* Part IV (discussing variances in interpretation of privacy statutes).

⁹⁸ See *infra* notes 103-110, 126-131 and accompanying text (providing policy drafting recommendations for employers permitting or prohibiting personal device use).

will be argued that personal device use for the conducting of employer business is a risk capable of mitigation through regulation, however the implementation of BYOD programs should only occur under circumstances conducive to regulation, or where regulation is not necessary.⁹⁹ Although all of the issues raised in the preceding sections could be resolved through prohibition of personal device use by employees, it must be assumed that despite prohibitions, many employees still often conduct business on their personal devices.¹⁰⁰

Commonplace in employment policies are clauses that permit the employer to remotely clear employer data from devices in the event a device is lost, stolen, or the employee leaves the company.¹⁰¹ The deletion however, absent a bifurcated, containerized data storage system to distinguish employee-personal data and an employer's information, could result in the deletion of all information contained on the device.¹⁰² Employees surprised by the deletion of all personal photos, contacts, music, and books on their devices, it has been argued, may bring a claim asserting violation of the CFAA, arguing that the employer was not authorized to access their devices to that extent, or at all, ultimately causing damage or loss.¹⁰³

A court's interpretation of "without authorization," as it is not defined in the statute, is vital in determining an employer's liability in a claim brought by an aggrieved employee.¹⁰⁴ The First Circuit has not formally articulated its interpretation of "authorization" or "without authorization" under the CFAA, however case law does provide insight.¹⁰⁵ Judges of the Massachusetts U.S. District Courts have advocated for

⁹⁹ See *infra* Part V (arguing strict regulation of personal device use if data is subject to government regulation).

¹⁰⁰ See Drolet, *supra* note 5 (noting fifty-seven percent of employees use personal devices for employer business despite prohibitions against their use); Kaneshige, *supra* note 60 (finding more than half of employees storing or transferring employers' documents on personal device).

¹⁰¹ See MATHIASON ET AL., *supra* note 4, at 14 (citing remote wiping of devices as common feature of Mobile Device Management software security protocols).

¹⁰² See *id.* (explaining mechanics of remote data wipes via Mobile Device Management software).

¹⁰³ See *id.* (describing instance where CFAA may be applicable to BYOD programs). The authors note that their firm is "aware of two recent cases where employers have received demand letters from terminated employees whose dual-use devices had been remotely wiped by the employer's IT personnel without the terminated employee's prior authorization." *Id.*

¹⁰⁴ See *supra* note 68 and accompanying text (noting significance of accesser's lack of authority in finding liability). However, "exceeds authorized access" is defined as "mean[ing] to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter..." 18 U.S.C. § 1030(e)(6) (2012).

¹⁰⁵ See *supra* note 68 and accompanying text (noting discrepancy between First Circuit courts in interpreting meaning of "without authorization" in CFAA analyses).

varying breadths of interpretation of the applicability of the CFAA with regard to the meaning of “without authorization.”¹⁰⁶

The advocates of a broad interpretation, such as the *Guest-Tek* court, believe an expanded breadth of the interpretation of “without authorization”, was justified by the consistent amendments to the CFAA by Congress and subsequent expansion through “the enactment of a private cause of action and a more liberal judicial interpretation of the statutory provisions.”¹⁰⁷ Further, proponents argue that the CFAA’s inclusion of an “‘intent to defraud’ requirement . . . effectively differentiated between harmless workplace procrastination and more serious” offenses.¹⁰⁸ The innocuous deletion of an employee’s dual-use device or other monitoring necessitating access, predicated on the employer’s aforementioned obligation to safeguard personal data or confidential or proprietary information, would likely invoke the CFAA under a broad analysis guided by an opinion in alignment with *Guest-Tek*.¹⁰⁹

The broad interpretation of the CFAA’s applicability in the employee privacy context would be erroneous.¹¹⁰ Legislative history indicates that the CFAA contemplated deterrence of computer crime by hackers and the abuse of authority by insiders.¹¹¹ The CFAA was prompted by the 1983 hacking of Memorial Sloan-Kettering Cancer Center’s computer system, where adolescent hackers gained access to radiology records and the ability to alter radiation levels received by patients.¹¹² The same CFAA should not be applicable in the employee privacy context, a far cry from the nefarious acts prompting passage of the legislation, such as the hacking of the Department of Defense, NASA, and

¹⁰⁶ See *supra* note 68 and accompanying text (outlining varying interpretations of CFAA’s applicability in First Circuit).

¹⁰⁷ *Guest-Tek Interactive Entm’t, Inc. v. Pullen*, 665 F. Supp. 2d 42, 45 (D. Mass. 2009) (advocating for broader interpretation of CFAA applicability).

¹⁰⁸ *Advanced Micro Devices, Inc. v. Feldstein*, 951 F. Supp. 2d 212, 218 (D. Mass. 2013) (expressing fear of distorting purpose of CFAA through broad interpretation of “without authorization”).

¹⁰⁹ See *supra* notes 68-69 and accompanying text (discussing broad interpretation jurisprudence).

¹¹⁰ See *infra* notes 111-113 and accompanying text (arguing CFAA inappropriately applied in certain contexts).

¹¹¹ See *supra* note 67-69 and accompanying text (discussing generally CFAA); see also S. REP. NO. 99-432, at 2480-81 (1986) (noting agreement with ABA’s support of statute deterring computer crime).

¹¹² See S. REP. NO. 99-432, at 2480-81 (discussing legislative history of CFAA). The Judiciary Committee, along with the ABA, “strongly agreed” with the proposition that the CFAA would deter future computer crime, however the obligation to implement effective safeguards ultimately lied with private businesses. *Id.*

financial institutions.¹¹³

The narrower, and frankly, more persuasive interpretation advocated in the *Advanced Micro Devices* analysis is predicated on the aversion to extending applicability of the CFAA to innocuous violations of a contractual obligation regarding computer use, as any deviation from the obligations of one party to another may invoke the “without authorization” provisions of the CFAA where computers are involved.¹¹⁴ The *Advanced Micro Devices* court argued that “expanding the definition of authorization to encompass extrinsic contractual agreements has far-reaching and undesirable consequences, such as potentially transforming idle internet browsing at work into a federal crime.”¹¹⁵

In sections of the CFAA where no language requiring nefarious intent is present, such as section 1030(a)(5)(C), the distinction between innocuous computer use and criminal activity is less easily made under a broad interpretation of “without authorization.”¹¹⁶ The legislative history cited clearly evinces Congress’s desire to criminalize nefarious computer-related crimes and abuses, rather than innocuous access to secure corporate data, and therefore presents the most logical argument for distinguishing the CFAA’s applicability in the BYOD context.¹¹⁷ The lack of intentionality in (a)(5)(A)’s catchall is clarified by the Judiciary Committee’s distinction that “insiders, who are authorized to access a computer, face criminal liability only if they intend to cause damage to the computer, not for recklessly or negligently causing damage. By contrast, outside hackers . . . could be punished for any intentional, reckless, or other damage they cause by their trespass.”¹¹⁸

While Littler has reported that it is aware of two demand letters sent by aggrieved BYOD employees asserting CFAA violations, it is unlikely that these claims would survive distinction of the broad

¹¹³ See *supra* note 67-69 (explaining history of CFAA).

¹¹⁴ See *supra* note 68 and accompanying text (interpreting “without authorization”).

¹¹⁵ *Advanced Micro Devices, Inc. v. Feldstein*, 951 F. Supp. 2d 212, 217-18 (D. Mass. 2013) (expressing fear of distorting purpose of CFAA through broad interpretation of “without authorization”); see 18 U.S.C. § 1030(a)(5)(C) (2012) (“[W]hoever intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage or loss.”).

¹¹⁶ *Advanced Micro Devices, Inc.*, 951 F. Supp. 2d at 218 (“It is obviously absurd to impose criminal liability for checking personal email at the workplace, or some similarly innocuous violation of an employee computer use agreement. Nor is it acceptable to rely solely upon prosecutorial discretion to refrain from prosecuting trivial offenses.”).

¹¹⁷ See *supra* note 67 and accompanying text (defining language and legislative intent of CFAA).

¹¹⁸ See S. REP. NO. 104-357, at *10-11 (1996); see also *supra* notes 67-70 and accompanying text (discussing legislative history of CFAA).

interpretation of the CFAA in the employment context to allow federal offenses to arise from actions lacking the insidious nature that the CFAA was crafted to punish.¹¹⁹ Presumably, the objective of the employer's access to an employee's device is to prevent the misappropriation of trade secrets and the protection of information requiring enhanced protection by its statutory obligee.¹²⁰ The failure of the broad interpretation of the CFAA's applicability fails to distinguish between innocuous accesses of devices to ensure information security and nefarious accesses resulting in the misappropriation of trade secrets by a departing employee, is indicative of its needed distinction from application to BYOD policies.¹²¹ Employers must advocate for the application of this narrower applicability of the CFAA, as it limits the exposure of the employer and increases the employee's burden in pleading the necessary elements of the CFAA, absent any obvious wrongdoing by the employer.¹²²

Despite the arguments as to whether or not the CFAA should be made applicable to BYOD programs, employers are able, and must take measures to limit exposure under a possible application of the broad interpretation of "without authorization" under the CFAA, before litigation comes to fruition in the unsettled First Circuit.¹²³ By having at least some employee authorization obtained through a signed employment policy, an employer can greatly limit its liability, as one court has held section 1030(a)(5), applicable to remote deletion of device memory, noted that the "exceeding authorization" language's absence bars applicability where at least some level of authorization is obtained.¹²⁴ However, this will not apply to employer monitoring of information, as section 1030(a)(2)(C) does contain such language, and sufficient authorizations will be

¹¹⁹ See MATHIASON ET AL., *supra* note 4, at 14; see also *Advanced Micro Devices, Inc.*, 951 F. Supp. 2d at 218 (expressing fear of distorting purpose of CFAA through broad interpretation of "without authorization"). "There is no express indication ... that Congress intended for employers to sue ... to recover economic damages resulting from time spent looking at personal emails instead of working. However, any information stored on any computer can satisfy the textual requirements of § 1030(a)(2)(C)." *Advanced Micro Devices, Inc.*, 951 F. Supp. 2d at 218.

¹²⁰ Cf. MATHIASON ET AL., *supra* note 4, at 47 (recommending wiping lost/stolen devices among other security measures through employer's remote management of devices).

¹²¹ See *Advanced Micro Devices, Inc.*, 951 F. Supp. 2d at 217-18 (discussing interpretations of CFAA).

¹²² See *supra* notes 108-121 and accompanying text (arguing that applicability of CFAA is distinguishable in First Circuit).

¹²³ See cases cited *supra* notes 107-108 and accompanying text (discussing broad interpretation of CFAA's applicability); see also *infra* Part V (recommending certain policy language to preclude CFAA claims).

¹²⁴ See *United States v. Morris*, 928 F.2d 504, 510-11 (2d Cir. 1991) ("[N]either subsection (a)(3) nor (a)(5) punishes conduct that exceeds authorization. Both punish a person who 'accesses' 'without authorization' certain computers.").

required.¹²⁵

Employers must draft into their BYOD device acceptable use policies so that the employer will remotely wipe the employee's BYOD device in the event of a lost or stolen device, or when the employee leaves the company, and that such device clearing may result in the loss or damage to an employee's personal data or information.¹²⁶ Further, employers must obtain written authorization that thoroughly enumerates what data monitoring measures devices are subject to, as the failure to enumerate all monitoring measures may result in a finding of exceeded authorization.¹²⁷ Finally, BYOD program policies should require written authorization of such access by the employer, and the employee's acknowledgement of the possibility of the loss of personal data or damage to the device resulting from such access, with election into the program contingent on such written acknowledgement and authorization.¹²⁸ Properly drafted policies gut any possible claims asserting CFAA violations, as no ambiguity will exist as to sufficiency of authorization, or the employer's intention.¹²⁹

Liability under the SCA may be invoked where the employer accesses an employee's personal email, online forum, or cloud-based storage tethered to the BYOD device.¹³⁰ Because the employee, not the employer, is the subscriber to these web-based services, the SCA would criminalize unauthorized access by the employer to the information stored within them, regardless of which party owns the data.¹³¹

In litigation surrounding instances where the employer has accessed the aforementioned web-based electronic communications services such as Yahoo!, Gmail, and the like, there is little opportunity to

¹²⁵ See 18 U.S.C. § 1030(a)(2)(C) (2012) ("Whoever ... intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer ... shall be punished in accordance with subsection (c) of this section.").

¹²⁶ MATHIASON ET AL., *supra* note 4, at 45 (enumerating necessary clauses in employee device use policies).

¹²⁷ See *id.* at 46 (enumerating necessary clauses in employee device use policies).

¹²⁸ See *id.* at 13-15, 46-49 (discussing BYOD liabilities and their mitigation under proper policy drafting).

¹²⁹ *Id.*

¹³⁰ See *id.* at 14-15 (discussing applicability of SCA to BYOD programs). Email, discussion boards, and cloud-based data storage will be referred to interchangeably as web-based communication services. See *id.*

¹³¹ See MATHIASON ET AL., *supra* note 4, at 14-15 (providing practical examples of where SCA liability exposure may arise); see also *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1058 (N.D. Cal. 2012) (finding iPhone fails to constitute "facility through which an electronic communication service is provided"); *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 512 (S.D.N.Y. 2001) (finding information stored on plaintiffs' hard drives failed to fit statutory definition of "interim storage").

refute the applicability of the SCA, as these are traditionally regarded as appropriate applications for the SCA by the courts.¹³² However, in scenarios where the ambit of the SCA might not be so clear, courts have been inconsistent in their treatment of unauthorized access of electronic communications.¹³³ The applicability of the SCA, in the BYOD context, will likely hinge on the statutory interpretations of the definitions for “facility” and “in electronic storage.”¹³⁴

The legislative history of the SCA examined by the *DoubleClick Inc.* court and its iteration in *iPhone Application Litigation* presents the most supportive argument for this proposition, finding that the legislative history of the SCA is indicative of Congress’ intention only to protect electronic communications while in temporary storage with the service provider waiting for delivery, and not those stored on individual users’ computers at their endpoint.¹³⁵ Because the messages are typically stored on the flash memory or hard drive of the device, and not on the provider’s servers, employers should not face liability under the SCA for their access of the electronic communications that are stored on the device itself.¹³⁶

Although the above argument has been accepted by the courts, foreboding language in a recent opinion by a U.S. District Court in Massachusetts could be problematic for employers engaged in monitoring employee owned devices.¹³⁷ The defendant argued that the use of a non-web based client, such as Microsoft Outlook that downloads

¹³² See *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1057 (N.D. Cal. 2012) (“[T]he computer systems of an email provider, a bulletin board system, or an ISP are uncontroversial examples of facilities that provide electronic communications services to multiple users....”).

¹³³ See *supra* note 75-77 and accompanying text (discussing varying treatment of SCA language by the courts).

¹³⁴ See *supra* notes 72-77 and accompanying text (defining terms applicable to SCA).

¹³⁵ See *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d at 512 (discussing limited definition of Title II); *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1059 (“this location data resides on Plaintiffs’ iPhone hard drive for up to a one-year period, which is not merely a ‘temporary, intermediate storage ... incidental to the electronic transmission’ of an electronic communication.”).

¹³⁶ See *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 115 (3d Cir. 2003); *United States v. Weaver*, 636 F. Supp. 2d 769, 772 (C.D. Ill. 2009) (discussing data storage); *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548, 555 (S.D.N.Y. 2008) (“The majority of courts which have addressed the issue have determined that e-mail stored on an electronic communication service provider’s systems after it has been delivered, as opposed to e-mail stored on a personal computer, is a stored communication subject to the SCA.”) (holding search of emails stored in Nationwide’s information technology systems exempt); see also *Mahoney v. DeNuzzio*, No. 13-11501-FDS, 2014 WL 347624, at *10 (D. Mass. Jan. 29, 2014) (finding that computers at issue did not constitute “facility” within meaning of SCA).

¹³⁷ See *Cheng v. Romo*, No. 11-10007-DJC, 2013 WL 6814691, at *4-5 (D. Mass. Dec. 20, 2013) (rejecting defendant’s argument that use of software which received emails negates liability under SCA).

communications to the personal computer from the service provider, exempted her from liability on the grounds that the messages are no longer stored “by an electronic communications service for purposes of backup protection,” but stored by the non-web based client.¹³⁸ The court rejected this argument, despite its support in another jurisdiction, stating that liability should not hinge on the plaintiff’s choice of software used to access an email account.¹³⁹ The court’s reasoning, that the “clear intent of the SCA was to protect a form of communication in which citizenry clearly has a strong reasonable expectation of privacy,” represents a significant departure from the literal approach of prior decisions in very technically distinguishing what types of communications were covered by the SCA.¹⁴⁰

Regardless of whether or not the *Cheng* court was correct in deciding as it did, the decision nonetheless illustrates the need for protective policy drafting by employers in an effort to mitigate the risks of uncertain litigation.¹⁴¹ In drafting such policies, employers must consider the mechanics of the statute’s language, as well as the risks they are seeking to mitigate, rather than simply enumerating prohibited conduct and assuming the employee infers what type of monitoring such prohibitions would require.¹⁴² Participation in the BYOD program should be contingent on conspicuous clauses in employee personal device use policies, coupled with a written acknowledgement of such terms.¹⁴³

In the private employment context, employee expectations of privacy are subject to the “legitimate countervailing business interests” of the employer, with such interests determined by factors such as the nature of the employer’s business, the employee’s duties, as well as the interest in preventing liability and damage to corporate property.¹⁴⁴ In the public employment context, privacy expectations are limited by the operational realities of the workplace, and if reasonable, such operational realities

¹³⁸ *Id.* at *4 (noting distinction between PC-based Outlook software and electronic Hotmail service as backup to Outlook).

¹³⁹ *See id.* at *5 (rejecting reasoning of *Weaver*); *cf. Shefts v. Petrakis*, No. 10-cv-1104, 2012 WL 4049484, at *7 n. 21 (C.D. Ill. Sept. 13, 2012) (“[A] person’s email should not be excluded from ECPA protection merely because of the mechanism by which the email system operates”).

¹⁴⁰ *See Cheng*, 2013 WL 6814691 at *5 (rejecting accesser’s definitional distinction argument on grounds that it defied Congressional intent).

¹⁴¹ *Cf. id.* at *4-5 (providing counterarguments to inapplicability of SCA in certain BYOD contexts).

¹⁴² *See generally supra* Part IV (discussing liability employers face contingent on judicial interpretation of SCA’s language).

¹⁴³ *See MATHIASON ET AL.*, *supra* note 4, at 14-15 (discussing services subject to SCA provisions).

¹⁴⁴ *See supra* notes 92-95 and accompanying text (defining employee expectations of privacy and private employer’s justifications for their limitation).

justify employer intrusions for “noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct.”¹⁴⁵ While previous sections discussing generally an employee’s right to privacy were separated based on the differing analytical frameworks of the public and private employment relationships, this analysis will address them together, noting incongruence where it arises, as they ultimately achieve similar privacy protection goals.¹⁴⁶ Due to the dearth of on-point case law regarding privacy expectations of employees using personally owned devices, privacy expectations in various instances will be analyzed by way of analogy of employer-owned devices, with any predicted variance based on the difference in ownership noted.¹⁴⁷

To understand the strength of the citizenry’s expectation of privacy in its communications, one need look no further than the legislative history of the Stored Communications Act.¹⁴⁸ In the absence of such a statute however, employer monitoring of communications will generally be permissible if done in a reasonable manner to achieve the employer’s legitimate countervailing business interests.¹⁴⁹ However, it should be noted that an employer’s level of liability under a privacy claim is less certain where it fails to notify the employee that the device is under surveillance, as employees could more likely be found to have expectations of privacy when the device is personally owned.¹⁵⁰

City of Ontario likely provides the most insight on employee privacy expectations in the BYOD context.¹⁵¹ While the Supreme Court

¹⁴⁵ See *O’Connor v. Ortega*, 480 U.S. 709, 710 (1987).

¹⁴⁶ Compare *supra* notes 81-82 and accompanying text (permitting searches for noninvestigatory, work-related purposes and investigations of work-related misconduct if reasonable), with *supra* notes 83-84 and accompanying text (noting right to privacy is subject to employer’s legitimate business interest, to a reasonable extent).

¹⁴⁷ See *supra* Part IV (discussing potential judicial treatment of BYOD related privacy claims arising from various monitoring measures).

¹⁴⁸ See *Cheng v. Romo*, No. 11-10007-DJC, 2013 WL 6814691, at *4-5 (D. Mass. 2013) (“[T]he clear intent of the SCA was to protect a form of communication in which the citizenry clearly has a strong reasonable expectation of privacy.”).

¹⁴⁹ See *supra* notes 92-95 and accompanying text (discussing employee expectations of privacy in private employment).

¹⁵⁰ See *City of Ontario v. Quon*, 560 U.S. 746, 760 (2010) (noting that there may be an expectation of privacy if employee purchases its own device).

¹⁵¹ See *id.* at 759 (assuming, *arguendo*, that employee had expectation of privacy in employer-supplied equipment). The court demonstrates the sensitivity of privacy expectations to their context, cautioning against perceiving their decision to promulgate some guidance on the permissibility of monitoring by employers:

Prudence counsels caution before the facts in this case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations of employees using employer-provided communication devices. Rapid changes in the dynamics of

cautioned against according too much reverence to their decision, their language used in dicta provides guidance as to how personal devices may change an employee's expectation of privacy, stating "[c]ell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy."¹⁵² The Court provided a counter to this argument, stating that the ubiquity and resultant affordability of these devices allows employees to pursue a personal device if they wished to keep matters private.¹⁵³ An employee's personal device may serve as a receptacle of highly personal information and even a means of self-expression; however, the employee, by electing to participate in a BYOD program, does to a certain extent avail itself to lesser privacy by waiving the opportunity to use employer-issued equipment and participate in a BYOD program.¹⁵⁴

Where an employee is required to supply its own device however, this argument may not be as persuasive, and careful policy drafting and careful communication and treatment of the device's use will be critical.¹⁵⁵ Because Quon's employer allowed its officers to treat their employer supplied equipment as their own, and abstained from auditing provided that overages were paid, the Ninth Circuit found that Quon had a reasonable expectation of privacy with respect to his communications.¹⁵⁶ As a result, employers must clearly and conspicuously communicate in their policies that all electronic communications, including email, text messages, voice

communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior. At present, it is uncertain how workplace norms, and the law's treatment of them, will evolve.

Id.

¹⁵² *Id.* at 760 (describing reasoning and arguments regarding expectation of privacy).

¹⁵³ *See id.*

¹⁵⁴ *See id.* (proffering that employee's wishing to keep matters private should use personal devices for personal matters).

¹⁵⁵ *See City of Ontario v. Quon*, 560 U.S. at 760-61 (discussing role of cell phones in society and workplace).

¹⁵⁶ *See Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 899, 904-06 (9th Cir. 2009) (finding reasonable expectation of privacy as matter of law, despite policy conspicuously seeking its negation). While the Supreme Court avoided this issue when it ruled, it assumed *arguendo* that Quon had a reasonable expectation of privacy, despite an employee policy that they should have no expectation of privacy in company-owned equipment. *See City of Ontario v. Quon*, 560 U.S. at 760-61 (discussing the role of cell phones in society and workplace). The "Computer Usage, Internet and E-Mail Policy" at issue provided that the city "reserves the right to monitor and log all network activity including e-mail and Internet use, with or without notice. Users should have no expectation of privacy or confidentiality when using these resources." *Id.* at 751. While text messages weren't explicitly stated in the policy, the employer made clear to employees that it would treat text messages the same as it treated emails, which were subject to auditing. *Id.*

calls, or voice mail; information, whether stored on the device, remotely via cloud storage, or on social media will be subject to monitoring, and that the employee should have no expectation of privacy in any of the aforementioned matters.¹⁵⁷ However, equally important is communicating to the employee that it will engage only in monitoring to exact a specific, legitimate business interest, and that monitoring will achieve that regulatory goal.¹⁵⁸ This can be achieved through the modification of existing policies, such as confidentiality policies, social media policies, and acceptable use policies, as well as drafting a separate and distinct personal device use policy.¹⁵⁹ Finally, employers and their legal representatives must remember that the courts will not simply take the employer's privacy policies on their face and apply them to the aggrieved employee's privacy claim to determine the existence of a privacy expectation.¹⁶⁰ The *City of Ontario v. Quon* decision made very clear that employer policies will be "shaped by the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated."¹⁶¹ As a result, it is paramount that employers not only responsibly draft privacy-related policies, but that the policies are communicated and regarded consistently with their drafting.¹⁶²

V. CONCLUSION

While commentators have argued that federal anti-hacking and privacy laws pose a significant issue in the monitoring of employees, courts would err in applying such laws in the workplace IT context. Except for actual nefarious conduct by an employer, application of the CFAA in this context would bastardize the CFAA's intention in obviating the bootstrapping of enforcement efforts against hackers. In addition to the relevant respects aforementioned, the SCA is prehistoric relative to the current state of workplace technology, casting applicability of the SCA over technologies not contemplated or fitting under the Act. As a result, courts must be weary to apply these laws to rapidly evolving, modern iterations of now-archaic IT infrastructure.

¹⁵⁷ See MATHIASON ET AL., *supra* note 4, at 45-48 (providing policy drafting recommendations to employers).

¹⁵⁸ See *id.* (same).

¹⁵⁹ See *id.* (same).

¹⁶⁰ See *City of Ontario v. Quon*, 560 U.S. at 758 (finding that inquiry into operational realities is needed regardless of communicated employer policy).

¹⁶¹ *Id.* at 760 (stating that employer policies are not simply analyzed as written).

¹⁶² See *id.* (stating that employee policies are shaped to extent that they are clearly communicated).

The vast inconsistencies in judicial treatment of employee privacy and the uncertainty of how courts will treat the inevitable BYOD predicated lawsuits creates significant issues for employers. Fortunately, employers have sufficient mechanisms at their disposal to greatly reduce the likelihood of litigation through precise and transparent policy drafting. Obtaining employee authorizations that permit an employer to access, modify, or monitor any and all information on the device likely negates applicability of both the SCA and CFAA in almost any context. Further, conspicuously stating that they should have no expectation of privacy in the device greatly stunts the viability of privacy claims by employees, as any subjective expectation of privacy would be objectively unreasonable given the notice provided by the employer.

While employees would likely resent a seemingly Orwellian surveillance program instituted by the employer, employers can address these concerns via the traditional provision of a company owned device at no cost of the employee. However, simply providing this employee with a company-owned device does not exact the compliance goals of employers that are subject to strict sensitive data protection obligations. To truly ensure protection of sensitive corporate information, employers must prohibit and discipline the use of unregulated employee personal devices in the workplace, as the use of these devices defeats the security provided by the monitoring of business use devices, whether BYOD or company provided. Failure to prohibit the use of unregulated personal devices is likely to effectively gut any of the employer's regulatory compliance schemes, as the flow of sensitive corporate data will be uninhibited. Of course, these policies and regulatory schemes are not imperative for all industries, companies, or employees; the recommended regulation of employee devices is to exact legitimate business interests in preventing company liability only where it exists.

Andrew Freedman

APPENDIX

