BYOD: AN EMPLOYEE'S PERSPECTIVE

by

Cynthia N. Sass, Esquire

American Bar Association
Section of Labor and Employment Law
Employee Rights and Responsibilities Committee
Midwinter Meeting
March 21, 2014

Available Courtesy of:
Law Offices of Cynthia N. Sass, P.A.
601 West Dr. Martin Luther King Jr. Boulevard
Tampa, Florida 33603
(813) 251-5599
www.EmploymentLawTampa.com

BYOD: AN EMPLOYEE'S PERSPECTIVE[1]

Cynthia N. Sass, Esquire
Law Offices of Cynthia N. Sass, P.A.
601 West Dr. Martin Luther King Jr. Boulevard
Tampa, Florida 33603
www.EmploymentLawTampa.com

Bring Your Own Device, or BYOD, is the policy or practice of employees bringing personal mobile devices to the workplace and/or using them for work-related purposes, including the management of their employer's privileged and confidential communications.

I. **Why is BYOD Important to Employment Lawyers?** Because of the ubiquitous use of personal mobile devices, all employers will need to address practical and legal issues related to BYOD in upcoming years even if they choose not to embrace a BYOD policy or practice.

II. **Who Owns the Data on Employee-Owned Devices When the Device is Used in the Workplace and/or for Work Purposes?** Several factors weigh in when it comes to data ownership. Unless addressed otherwise via employer agreements and policies, employees own their personal data on their personal devices when they have paid for the device and the service. However, once the employee brings the device into the workplace, uses an employer's wireless Internet connection, and starts doing work with his or her personal device rather than using the employer's equipment, ownership issues become more complex, as they bring control, privacy rights, third-party access, off-the-clock work, and consent into the equation.

PRACTICAL TIP:

- **Contract Upfront** – An employee should address ownership before using his or her own device in the workplace or for work purposes.
- **Read it!** – Always read company policies when analyzing an employee's potential claims.

III. **Potential Employee Claims Against an Employer for Accessing and/or Modifying Employee's Device and/or Data**. When employees use their personal devices for work purposes, they may be subject to policies that purport to give their employers the right to regulate employee use of their own personal device, as well as the right to access, remotely or otherwise, and monitor or modify data. A proponent of these policies includes a requirement that employees sign a waiver of rights or consent to a notice that their employer

[1] The following material is intended to provide information of a general nature concerning the broad topic of employment law in Florida. The materials included in this paper are distributed by the Law Offices of Cynthia N. Sass, P.A., as a service to interested individuals. The outlines contained herein are provided for informal use only. This material should not be considered legal advice and should not be used as such. Thank you to Charlotte R. Fernée, Esquire, of the Law Offices of Cynthia N. Sass, P.A., for her assistance in preparing these materials.

intends to monitor or prohibit certain actions. In that event, employees may find themselves with little negotiating power in an at-will employment scenario, and will surrender many legal rights as defined by their employer's policies.

When representing an employee and determining whether a claim arises from an employer's access and/or deletion of data from an employee's device, one needs to fully read all of the employer's computer policies to evaluate whether the employee had sufficient notice of the extent the employer can monitor and/or regulate his or her use and access the data, whether the scope of the access is excessive and/or necessary, and whether consent was given and the extent of such consent. Because BYOD legal issues are somewhat of a new legal frontier, many potential causes of action need to be analyzed by analogy with existing precedent containing similar elements.

A. Invasion of Privacy. Does an employee have a "reasonable expectation of privacy" because they own the device or software?

- **Fourth Amendment**. Provides protection from *governmental* authority engaging in unreasonable search and seizures. Standard is whether the employee and/or applicant has a "reasonable expectation of privacy" in the thing or matter searched.

- **State Constitutional Right to Privacy**. State constitutions provide another source of privacy protection. For example, ten states: Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington, expressly recognize a right to privacy. In Florida, Art. 1, Sect. 23 states: "Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein." Further, Florida's constitution construes a right against unreasonable searches and seizure with the Fourth Amendment of the United States Constitution. As a result, monitoring employees in Florida requires balancing employee privacy rights with the employer's interests. Additionally Florida imposes restrictions on surveillance beyond those established by federal law. See Section 934.03, Fla. Stat.

- **Intrusion Upon Seclusion**. Restatement (Second) of Torts §652B provides "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." To prove this, the plaintiff must show a reasonable expectation of privacy. This cause of action is available to both public and private employees.

In determining whether a reasonable expectation of privacy exists, courts apply the two-prong test used in the Fourth Amendment constitutional context. First, an actual subjective expectation of privacy must exist. Second, the expectation of privacy must be one that is objectively reasonable.

1. **Reasonable Expectation of Privacy Defeats Employer's Policy** – *Stengart v. Loving Care Agency, Inc.*, 973 A.2d 390 (N.J. 2009). This case utilized the common

law tort of "intrusion on seclusion" as the source of the reasonable expectation of privacy standard. Here, the court held that an employee can expect privacy as well as confidentiality in e-mails with her attorney, which she sent and received through her personal, password-protected, web-based e-mail account using an employer-issued computer. The court found that the employee had a subjective expectation of privacy because she took steps to protect the privacy of the e-mails and shield them from her employer. She used a personal, password-protected e-mail account instead of her company e-mail address and did not save the account's password on her computer. The court also reasoned that language used in the employer's Internet-use policy created an objectively reasonable expectation of privacy because it permitted some personal use of the employer's Internet and equipment.

2. **Company Property vs. Personal Property**. Additionally, *Stengart* discusses what information on an employee's computer is personal and which is company property:

   a. Not Company Property Because Done on Working Time. The *Stengart* court stated, "We thus reject the philosophy ... that, because the employer buys the employee's energies and talents during a certain portion of each workday, anything that the employee does during those hours becomes company property." *Id*. at 401.

   b. Not Company Property Because Done on Company Property. The *Stengart* court stated, "A policy imposed by an employer, purporting to transform all private communications into company property—merely because the company owned the computer used to make private communications or used to access such private information during work hours—furthers no legitimate business interest." *Id*. at 401.

   c. Not Going to Define the Extent an Employer May Go To in Searching. The *Stengart* court stated, "Here, we make no attempt to define the extent to which an employer may reach into an employee's private life or confidential records through an employment rule or regulation. Ultimately, these matters may be a subject best left for the Legislature." *Id*. at 401.

3. **E-mail Privacy** – *In re Asia Global Crossing, Ltd.*, 322 B.R. 247 (Bankr. S.D.N.Y. 2005). A federal bankruptcy court considered whether a trustee could force the production of e-mails sent by company employees to their personal attorneys on the *company's* e-mail system. The court developed a four-part test to measure an employee's expectation of privacy in their e-mails:

   (1) does company policy ban personal or other use;
   (2) does the company monitor the use of the employee's e-mail;
   (3) do third parties have a right of access to the e-mails; and
   (4) did the company notify the employee, or was the employee aware, of the use and monitoring policies?

4. **Attorney-Client Privilege**. In *Asia Global*, because the evidence was "equivocal" about the existence of a corporate policy banning personal use of e-mail and allowing monitoring, the court could not conclude that the employee's use of the company e-mail system eliminated any applicable attorney-client privilege. In applying the *Asia Global* factors, the fact-specific nature of the inquiry affects the outcome. According to some courts, employees have a lesser expectation of privacy when they communicate with an attorney using a company e-mail account as compared to a personal, web-based account.

5. **Policy vs. Practice** – *Curto v. Medical World Communications, Inc.*, 99 Fed. Empl. Prac. Cas. 298 (E.D.N.Y. May 15, 2006). An employee working from a home office sent e-mails to her attorney on a company laptop via her personal AOL account. Those messages did not go through the company's servers but were nonetheless retrievable. Notwithstanding a company policy banning personal use, the trial court found that the e-mails were privileged. Although employer had an electronic communications policy allowing for monitoring, the court held that the employee still had a reasonable expectation of privacy because employer rarely did in fact monitor the system, which lulled employees into a "false sense of security."

6. **Private Passwords** – *U.S. v. Long*, 64 M.J. 57 (C.A.A.F. 2006). Despite the fact that user had to acknowledge banner which stated that the computer system may be monitored and that evidence of unauthorized use collected during monitoring could be used for administrative, criminal, or other adverse action each time she logged on to use the computer, court held that plaintiff had a reasonable expectation of privacy in e-mails sent from her office computer and stored on the government server due in part to the fact she had a password known only to her.

7. **Expectation of Privacy Even Where Employer Expressly States No Expectation Exists** – *Haynes v. Office of the Attorney General*, 298 F. Supp. 2d 1154, 1161-62 (D. Kan. 2003). Employee had reasonable expectation of privacy in private computer files, despite computer screen warning that there shall be no expectation of privacy in using employer's computer system, where employees were allowed to use computers for private communications, were advised that unauthorized access to user's e-mail was prohibited, employees were given passwords to prevent access by others and no evidence was offered to show that the employer ever monitored private files or employee e-mails.

PRACTICAL TIP:

- **Actual Monitoring** – Always ask whether the employee knows if his or her employer actually monitors their device, the network connection, or communications to and from the device. At least one court has held an electronic communications policy was ineffective where the employer did not *actually* monitor the communications.

- *United States v. Slanina*, 283 F.3d 670, 676-77 (5th Cir.), vacated on other grounds, 537 U.S. 802, 154 L. Ed. 2d 3, 123 S. Ct. 69 (2002). Employee had reasonable expectation of privacy in his computer and files where the computer was maintained in a closed, locked office, the employee had installed passwords to limit access, and the employer "did not disseminate any policy that prevented the storage of personal information on city computers and also did not inform its employees that computer usage and Internet access would be monitored."

- *Leventhal v. Knapek*, 266 F.3d 64 (2d Cir. 2001). Employee had reasonable expectation of privacy in contents of workplace computer where the employee had a private office and exclusive use of his desk, filing cabinets and computers, the employer did not have a general practice of routinely searching office computers, and had not "placed [the plaintiff] on notice that he should have no expectation of privacy in the contents of his office computer."

9. **Limited or No Privacy**.

   a. Partial Reimbursement from Employer – *Mintz v. Mark Bartelstein & Associates, Inc.*, 885 F. Supp. 2d 987 (C.D. Ca. 2012). Personal cell phone was used in plaintiff's work as a sports agent. Court found that employee had only a **LIMITED** expectation of privacy concerning his phone records because the phone was a BYOD device that was paid for by both the employee and the employer ($300 & monthly bill from employer, about $115 from employee's check). Interestingly, the employer had a phone policy that employee did not read, nor did he sign an acknowledgement form saying he did read it/would read it.

   b. Public Location and Employer Network – *U.S. v. Barrows*, 481 F.3d 1246 (10th Cir. 2007). City employee did **NOT** have reasonable expectation of privacy in personal computer that he brought to city hall for work-related use, hooked up to city's network for file sharing, kept continuously on, and failed to password protect or take any other steps to prevent third-party use despite computer's location in public area, and thus discovery of pornographic images on computer by another city worker was not a Fourth Amendment violation.

   c. Privacy in Discovery – *Kamalu v. Walmart Stores, Inc.*, 119 Fair Empl. Prac. Cas. (BNA) 1223 (E.D. Ca. 2013). Court held **LIMITED** privacy for relevant cell phone documents in discovery. Employer was entitled to basic subscriber information from employee's personal cell phone records where employee claimed illegal discrimination based on national origin, sex, and race because the claims involved cell phone use at work and wage and hour discrepancies. However, discovery inquiries about phone records were limited to date, time and duration of phone calls and text messages. The court held that for purposes of document production in discovery, privacy rights only attach to content of the information.

d. No Expectation of Privacy, Even Though Company Expressly Stated They WOULD NOT Monitor Employees' E-mail – *Smyth v. Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996). Employee had **NO** reasonable expectation of privacy despite assurances that e-mail sent over the company e-mail system would not be intercepted by management; when employee communicated a comment over e-mail system utilized by entire company, a reasonable expectation of privacy was lost, and even if employee had a reasonable expectation of privacy, a reasonable person would not have considered employer's interception of communications to be a substantial and highly offensive invasion of privacy because e-mail system was shared by entire company.

e. No Expectation Because of Employer Policy.

i. **Others Can Monitor** – *State v. Young*, 974 So. 2d 601 (Fla. 1st DCA 2008). Where an employer has a clear policy allowing others to monitor a workplace computer, an employee who uses the computer has **NO** reasonable expectation of privacy in it. In the absence of such a policy, the legitimacy of an expectation of privacy depends on the other circumstances of the workplace.

ii. **Four-Factor Test** – *Leor Exploration & Production LLC v. Aguiar*, 2009 WL 3097207 at *4 (S.D. Fla. 2009). The court addressed whether a company's CEO had a reasonable expectation of privacy in e-mail communications that were sent to his personal attorney through the company's e-mail system where the company had an employee handbook which included a general warning that, "[e]mployees should have no expectation of privacy in communications made over [the company's] systems." The court noted that mere existence of a no-privacy provision in an employee handbook is generally not determinative of an employee privacy claim. Instead, the court adopted the following four-factor test:

(1) Does the corporation maintain a policy banning personal or other objectionable use?
(2) Does the company monitor the use of the employee's computer or e-mail?
(3) Do third parties have a right of access to the computer or e-mails?
(4) Did the corporation notify the employee, or was the employee aware, of the use and monitoring policies?

Applying those factors, the court in *Leor* concluded that the CEO had **NO** expectation of privacy.

iii. **Monitor Personal Use** – *U.S. v. Hassoun*, 2007 WL 141151 (S.D. Fla. 2007). Employee had **NO** reasonable expectation of privacy in any material on work computer where, although company policy did not forbid personal use of computer, it made clear that all uses, work or personal, would be subject to monitoring.

iv. **Subject to Inspection** – *Muick v. Glenayre Elecs.*, 280 F.3d 741, 743 (7th Cir. 2002). **NO** reasonable expectation of privacy in workplace computer files where employer had announced that it could inspect the computer.

v. **Audit Internet Use** – *United States v. Simons*, 206 F.3d 392, 398 & n.8 (4th Cir. 2000). **NO** reasonable expectation of privacy in office computer and downloaded Internet files where employer had a policy of auditing employee's use of the Internet, and the employee did not assert that he was unaware of or had not consented to the policy.

vi. **Daily Opportunity to Consent** – *Sporer v. UAL Corp.*, 2009 WL 2761329 (N.D. Cal. 2009). Employee had **NO** expectation of privacy in computer usage where employer (1) had a policy of monitoring its employees' computer use; (2) warned employees that they had no expectation of privacy in e-mail transmitted on the company system; and (3) provided its employees with a daily opportunity to consent to such monitoring by having to click through a warning to access the company system.

vii. **Express Restriction on Use** – *Thygeson v. U.S. Bancorp*, 2004 U.S. Dist. LEXIS 18863 (D. Or. Sept. 15, 2004). **NO** reasonable expectation of privacy in e-mails saved on the network or in website addresses, given an express policy restricting personal use of office computers and notice that activity could be monitored.

viii. **Periodic Reminders** – *Garrity v. John Hancock Mutual Life Ins. Co.*, 2002 U.S. Dist. LEXIS 8343 (D. Mass. May 7, 2002). **NO** reasonable expectation of privacy where, despite the fact that the employee created a password to limit access, the company periodically reminded employees that the company e-mail policy prohibited certain uses, the e-mail system belonged to the company, although the company did not intentionally inspect e-mail usage, it might do so where there were business or legal reasons to do so, and the plaintiff assumed her e-mails might be forwarded to others.

ix. **Violation of Law** – *U.S. v. Simons*, 206 F.3d 392 (4th Cir. 2000). Public employer's remote, unwarranted searches of employee's office computer did **NOT** violate the employee's Fourth Amendment rights because, in light of the employer's Internet policy, the employee lacked a legitimate expectation of privacy in the files downloaded from the Internet. Additionally, the employer had a responsibility to inquire via policy enforcement once it learned that the content of downloaded files was illegal (child pornography).

10. ***Quon* and Progeny Further Expand and Define Employee Privacy Rights**.

a. Monitoring Issues With Government Employees. As a general matter, the Fourth Amendment makes warrantless searches by the government per se unreasonable. However there are certain exceptions to that rule, one of which is the special

needs of the workplace. This issue arises in the employer-employee context most often where the government is the individual's employer. In order for a government employer to perform a warrantless search of an employee's electronic media, the search must:

(1) be motivated by a legitimate work-related purpose; and
(2) not be excessively intrusive in light of the justification.

- *City of Ontario v. Quon*, 130 S. Ct. 2619 (2010). The Supreme Court applied Fourth Amendment protection and stated that as a general rule public employees generally have a reasonable expectation of privacy in electronic communications on employer devices. Additionally, the court reasoned that cell 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. This might strengthen the case for an expectation of privacy.

- Further, while *Quon* addresses questions raised concerning the Fourth Amendment rights of a government employee in the face of conduct by the employer, because of the underlying facts this ruling can influence similar claims of private employees.

- In *Quon*, the issue involved the city police department performing a search of officers' text messages sent and received on employer-issued pagers. The officers alleged that the search constituted a warrantless government search in violation of the Fourth Amendment. The court held that because the reason for the search (to see if officers, who were charged for service overages, were being unfairly charged money for pager use which was required by their job) was motivated by a legitimate, work-related purpose and the method in which the search was conducted was not overly intrusive in light of that reason, there was no Fourth Amendment violation.

- Additionally, the court reasoned that employer policies concerning communications shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated. The city's unequivocal Internet usage policy specified it "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." The court also stated that clear communication from the city that text messages transmitted from employees' devices would be considered e-mails meant they were also covered under the policy. Such clear and unequivocal communication effectively terminated any expectation of privacy.

- However, the facts in *Quon* are so air-tight for extinguishing an employee's expectation of privacy, citing *Quon*'s general rule in favor of employee

privacy rights and then distinguishing *Quon* facts from the case at bar makes this a very useful case for employees.

c. *Quon* Progeny Cases Generalize Employee Privacy Rights with Non-Employment Facts. To the extent a private employee's fact-specific reasonable expectation of privacy relies on successful Fourth Amendment arguments legitimized in an employment context, non-employment cases citing *Quon* arguably extend the circumstances under which employees can validate this expectation.

d. Sole Purpose to Obtain Admission – *State v. Clampitt*, 364 S.W.3d 605 (Mo. Ct. App. 2012). Criminal case not involving employment matters where the court cited *Quon*, suggesting that the workplace expectation of privacy employees have that pertains to employer-provided devices should also extend to devices and e-mails that are not work-related. In *Clampitt*, a court properly found investigative subpoenas to be an unreasonable search under the Fourth Amendment because the State had no relevant purpose for requesting defendant's text messages beyond the time of the accident. The State sought the contents of the text messages for the sole purpose of obtaining an admission from defendant as to who was driving and provided no evidence that it had reason to believe defendant made admissions or divulged any details about his role in the accident via text messages.

e. Call Records Included – *United States v. Davis*, 787 F. Supp. 2d 1165, 1170 (D. Or. 2011). Citing *Quon*, the court held that an individual has a reasonable expectation of privacy in his or her personal cell phone, including call records and text messages. This was a criminal case where defendant moved to suppress evidence obtained as a result of the search of his cell phone. While the phone was lawfully seized as part of an inventory search before his crashed vehicle was towed away, the government failed to prove that a subsequent search of the phone was justified by an exception to the warrant requirement.

f. Personal Nature of Device – *United States v. Gomez*, 807 F. Supp. 2d 1134 (S.D. Fla. Aug. 31, 2011). An individual has a reasonable expectation of privacy in his personal cell phone because "the weight of authority agrees that accessing a cell phone's call log or text message folder is considered a 'search' for Fourth Amendment purposes." This was a criminal case where a cell phone was seized and used by law enforcement to collect additional evidence. The court cited *Quon* and determined that defendant's Fourth Amendment rights attached to his cell phone and its operational functions such as exchanging phone calls and text messages, as opposed to a land line, because of the personal nature of the device.

11. **Court Analogizes Cell Phone with Laptop** – *State v. Smith*, 920 N.E.2d 949, 956 (Ohio 2009). Criminal case where defendant was arrested for drug dealing and then his phone searched for incriminating conversations. Defendant argued that the search incident to a lawful arrest exception to the warrant requirement to search his cell phone did not exist. The district court reasoned that modern cell phones "have the capacity for storing immense amounts of private information" and thus likened the

devices to laptop computers, in which arrestees have significant privacy interests, rather than to address books or pagers found on their persons in which they have lesser privacy interests. Additionally, the search of the phone's contents was not necessary to ensure officer safety, and there was no evidence that the information police were searching for was subject to imminent destruction.

PRACTICAL TIP:

- **Intermingling** – Instruct the employee to avoid the intermingling of company and personal information on the device as much as reasonably possible.

B. Violations of Federal and State Computer Trespass Statutes.

- **Example of Data Wiping**. Many current BYOD policies require employees to permit employer access to a software app installed to the employee's personal device that includes a potential to remotely wipe data. Such action is normally taken in an effort to mitigate the risk of disclosing and/or misappropriating confidential or proprietary information and trade secrets. However, at times, this wipe may not only delete company data, but also the employee's personal data. Depending on whether the employee consented to the employer's policy, how the language in the policy is crafted and its subsequent enforcement in standard practices, the employee may or may not have a claim although his or her personal data has been compromised or completely deleted.

  Computer savvy employers now use methods where they access only employer data on employee devices. Thus when they access or wipe data on employee devices remotely, they delete employer-related data only and leave the employee's personal data intact. This information can be used when bringing a claim against an employer who has wiped out a plaintiff's personal data to show there is a less intrusive way to inspect, control or delete employer information.

  Data wipe case law precedent is expected to emerge and solidify within the next few years. Potential claims are currently analyzed by analogy, anticipating eventual application of existing state and federal computer trespass statutes. Similarly, many other BYOD-related legal issues are analyzed by analogy.

1. **The Computer Fraud and Abuse Act, 18 U.S.C. §1030 ("CFAA")**. The CFAA prohibits the unauthorized access of a computer (or exceeding authorized access of a computer) and obtaining information, and violations can be alleged against both employees and employers. The problem often arises when departing employees attempt to gain an advantage by taking information from the employer prior to their departure, and this is discussed in further detail later in this outline.

   However, in a BYOD context where an employer accesses an employee's personal device without the requisite authorization, the employee could allege a violation of

the CFAA. There is disagreement among the circuits as to when a party acts with the requisite authorization.

The CFAA provides both criminal penalties including fines and imprisonment for up to 10 years (18 U.S.C. §1030(c)) and a civil cause of action for certain violations of the CFAA where compensatory damages and other injunctive or equitable relief may be granted. 18 U.S.C. §1030(g).

Section 1030(a)(5) of the CFAA provides for liability on a person who:

(1) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
(2) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
(3) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

a. Damage to Data or Device is Not Enough – *Keen v. Bovie Med. Corp.,* 2013 U.S. Dist. LEXIS 64999 (M.D. Fla. May 7, 2013). Employee used a program to wipe the laptop clean, and employer's data recovery vendor report stated that no data was recoverable, resulting in permanent damage. Employee's access to employer-owned laptop was authorized and **NOT** violative of CFAA.

2. **The Electronic Communications Privacy Act of 1986, 18 U.S.C. §2510, *et seq.*, a/k/a the Federal Wiretap Act ("ECPA")**. Title I of the ECPA regulates the search and seizure of electronic communications while they are in transit. It provides civil and criminal penalties for the unlawful interception, disclosure or use of electronic communications, and it most often arises in the labor context where employers monitor and intercept communications between employees. However, under the ECPA, consent to the interception by one party to the communication is a defense to a violation. The ECPA provides for separate causes of action both by private individuals and by the government.

In a private cause of action under the ECPA, a plaintiff may recover preliminary and other equitable or declaratory relief as may be appropriate, declaratory damages, punitive damages where appropriate, reasonable attorney's fees and other litigation costs reasonably incurred. 18 U.S.C. §2520.

Notably, the ECPA provides that the plaintiff will receive at a minimum $10,000, regardless of a showing of any actual damages. In addition, if the communication involves certain radio or private satellite video communications, the violator may be subject to suit by the federal government. 18 U.S.C. §2511(5).

Finally, the ECPA provides for criminal penalties including a fine and imprisonment for up to five years. 18 U.S.C. §2511(4).

a. Interception Where Access Web-Based E-mails – *Shefts v. Petrakis*, 2012 U.S. Dist. LEXIS 130542 (C.D. Ill. Sept. 12, 2012). In an action between owners of a telecommunications company, co-owners accessing Yahoo!®-based e-mails as well as a screen-capture software that took images of plaintiff's computer activities constituted interceptions in violation of the ECPA.

b. Interception Where E-mails Diverted – *United States v. Szymuszkiewicz*, 622 F.3d 701 (7th Cir. 2010). Jury found violation of ECPA where employee went on his supervisor's computer while she was away and activated a "rule" on her e-mail account so that any e-mail that was sent to the employee's supervisor was also forwarded to him.

c. No Interception Because Post-Transmission Storage – *Ehling v. Monmouth-Ocean Hosp. Serv.*, 872 F. Supp. 2d 369 (D.N.J. May 30, 2012). Court dismissed claim under analogous state wiretap act against an employer who accessed an employee's private Facebook® page via another employee's account because the posting accessed was in "post-transmission storage."

d. Viewing a Website Not an Interception – *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 883-84 (9th Cir. 2002). The airline pilot sued the employer under the ECPA after a company executive, using log-in information for another employee, accessed the pilot's private website, which contained derogatory comments of upper management. The court held that viewing the website was not an interception as defined by the ECPA.

3. **The Stored Communications Act ("SCA"), 18 U.S.C. §2701, *et seq.* of the Electronic Communications Privacy Act of 1986**. Federal law prohibits intentional unauthorized access to employees' personal electronic communications. The ECPA amended wiretapping laws and regulates other forms of electronic communications. The SCA contained in Title II of the ECPA, provides that "whoever intentionally accesses without authorization a facility through which an electronic communication service is provided … and thereby obtains, alters or prevents authorized access to a wire or electronic communication while it is in electronic storage … shall be punished as provided…." 18 U.S.C. §2701(a)(1).

   The statute includes a civil action as well as criminal penalties. 18 U.S.C. §2701(b).

   The SCA does permit access to a stored communication, however, when consent is provided by the user. 18 U.S.C. §2701(c)(2).

   a. Employer Vicariously Liable for Supervisor's Unauthorized BlackBerry® Use – *Lazette v. Kulmatycki*, 2013 U.S. Dist. LEXIS 81174 (N.D. Ohio June 5, 2013). Plaintiff was told that she could use the company-issued BlackBerry® for personal e-mail. She had an account with Google™ e-mail, though she believed she had deleted that account from the BlackBerry® before returning it to her supervisor when she left employment in September 2010. She understood that the employer would "recycle" the device for use by another employee. Plaintiff later learned

that her supervisor, rather than deleting her Google™ e-mail account, had been accessing her Google™ e-mail for 18 months. In addition, her supervisor disclosed the contents of the e-mails he had accessed. These actions were outside the scope of his employment. The court found that a supervisor using a company-owned BlackBerry® personal mobile device to access a former employee's personal e-mail may violate the SCA because he did not have authority to do so. Moreover, the court held that the employer could be vicariously liable. The fact that the device was owned by the company did not satisfy the requirement for authorization.

b. Personal Web-Based E-mail Accounts – *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548 (S.D.N.Y. 2008). Employer's access of employee's personal e-mails, which were stored and accessed directly from accounts maintained by outside electronic communication service provider, was unauthorized, and thus violated SCA. The employee did not store any of the communications on the employer's computers, servers, or systems; did not send or receive such communications through the company's e-mail system or computer; had a reasonable expectation of privacy in his personal, password-protected e-mail accounts; and nothing in employer's policy suggested that viewing of e-mail from a third-party e-mail provider over employer's computers would subject all personal e-mails on the account to inspection.

c. Password-Protected Does Not Mean Private. The SCA does not apply to an electronic communication that is readily accessible to the general public. 18 U.S.C. §2511(2)(g)(i); *Snow v. DirecTV, Inc.*, 450 F.3d 1314, 1322 (11th Cir. 2006). Fact that website users had to create a username and password did not mean the information was not readily available to the general public because nearly anyone was eligible to create a username and password.

4. **State Wiretap Statutes**.

a. FOR EXAMPLE: Florida Wiretap Statute, §934.03 Fla. Stat. – Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited.

- The Florida wiretap statute prohibits an individual from intercepting any "wire, oral or electronic communication." Any person who has their wire, oral, or electronic communication intercepted in violation of the statute has a private cause of action where they may seek preliminary or equitable or declaratory relief as may be appropriate, actual damages but not less than liquidated damages computed at a rate of $100 a day for each day of the violation or $1,000, whichever is higher, punitive damages and a reasonable attorney's fee and other litigation costs reasonably incurred. Fla. Stat. §934.10.

- In contrast to the Federal Wiretap Act, Florida's wiretap statute provides that consent to the interception is a defense only if all parties consent.

Additionally, violation of the statute may result in a first degree misdemeanor charge resulting in up to one year in jail.

b. Device Monitoring Software Apps – *O'Brien v. O'Brien*, 899 So. 2d 1133 (Fla. 5th DCA 2005). Court found wife violated Florida Statute §934.03 when she installed software on husband's computer which intercepted e-mails, chat conversations and instant messages without his consent.

5. **State Computer Crime Statutes**. Check whether your state has an equivalent to the federal ECPA.

   a. FOR EXAMPLE: Florida Computer Crimes Act, Chapter. 815, Fla. Stat.

   - Florida state law uses the term "offense against computer users" to describe unauthorized access to a computer, computer system, or computer network. The term includes access made for the purpose of harm, damage, or destruction. In addition, Florida law prohibits the introduction of computer viruses. To prove the offense, the prosecutor must show that the defendant willfully and knowingly participated in the computer-related activities.

     In general, Florida law sets the prosecution of an offense against computer users as a third degree felony, punishable by a term of imprisonment for up to five years, a fine in an amount up to $5,000, or both. If the offense causes over $5,000 in damage, carries out a scheme to commit fraud or theft, interrupts governmental operations, or disrupts public services, state laws increase the offense to a second degree felony. Florida state laws set a term of imprisonment for up to 15 years, a fine in an amount up to $10,000, or both.

   - Under the Florida statute, the term 'offense against intellectual property' includes unauthorized acts to alter, modify, or destroy data or information contained within a computer, computer system, or computer network. In addition, the term prohibits computer-related acts in order to disclose or steal confidential information, trade secrets, and other intellectual property. As with an offense against computer users, the prosecutor must show that the defendant participated willfully and knowingly.

     An offense against intellectual property similarly requires prosecution as a third degree felony, with the accompanying punishments, unless the offense qualifies as a second degree felony because the defendant intended to commit fraud or theft.

   - If the offense endangers human life, it becomes a first degree felony, which may result in a term of imprisonment for up to 30 years, a fine in an amount up to $10,000, or both.

- *Willoughby v. State*, 84 So. 3d 121 (Fla. 3d DCA 2012). A jury in the Circuit Court for Miami-Dade County convicted the defendant of unlawfully accessing a computer database in violation of §§815.06(1) and (2)(a), Fla. Stat. (2006) (Count 1), and obtaining trade secret or confidential data in violation of §§815.04(3)(b) and (4)(a), Fla. Stat. (2006) (Count 2). Defendant's work supervisor suspected that defendant had transferred her employer's confidential data to her laptop. The police seized defendant's laptop and discovered that defendant had e-mailed her employer's client trust fund list to her laptop. The appellate court found that the State failed to show that defendant was unauthorized to access the employer's computer network for purposes of the conviction under §§815.06(1) and (2)(a). The evidence showed that defendant's supervisor authorized defendant to access the employer's computer network to perform her job, and defendant's personal laptop was connected to the employer's network by the employer's administrator. However, the State proved that defendant did not have authorization to download data from her employer's computer system to her personal laptop. Thus, the State proved all the elements of obtaining trade secret or confidential data. Section 815.04(3)(b) did not include a requirement that defendant have a malicious purpose, but required only that defendant's conduct be willful, knowing, and without authorization. Defendant repeatedly was informed that she could not obtain any of the data from the network system.

IV. **Employer Liability Discrimination Claims When Employees Utilize BYOD**. Covered employers generally have an obligation to ensure that employees are not discriminated and/or retaliated against and/or harassed based on protected characteristics in the workplace. Harassment outside of the workplace may also be illegal if there is a link with the workplace, for example, if a supervisor harasses an employee while driving the employee to a meeting.[2] Employee use of personal devices could perpetuate discriminatory, retaliatory or harassing behavior towards other co-workers (i.e. texting, etc.) for which the employer may be liable.

A. Company Bulletin Boards – *Blakely v. Continental Airlines, Inc. et al.*, 751 A.2d 538 (N.J. 2000). Continental operated a website where employees could log on to find flight times, schedules, etc. There was also a message board where co-workers posted derogatory and harassing messages about Blakely. The court stated, "Employers do not have a duty to monitor private communications of their employees; employers do have a duty to take effective measures to stop co-employee harassment when the employer knows or has reason to know that such harassment is part of a pattern of harassment that is taking place in the workplace." The message board was found sufficiently related to the workplace in order to hold the employer liable.

B. Off-the-Job Electronic Communications – *Summa v. Hofstra University*, 708 F.3d 115 (2d Cir. 2013). In plaintiff's gender discrimination and harassment case against the university where the football players, non-employees, made harassing posts on

[2] EEOC Enforcement Guidance: Vicarious Employer Liability for Unlawful Harassment by Supervisor (June 18, 1999) http://www.eeoc.gov/Policy/docs/harassment.html.

Facebook® page regarding a university employee, among other behavior, grant of summary judgment for the employer was proper because the employer took prompt action by removing the offender, addressing all complaints and providing sexual harassment training to stop and/or prevent the harassing conduct by non-employees.

C. Disparate Treatment Due to Personal Photograph – *Terry v. Borough*, 2013 U.S. Dist. LEXIS 174584 (E.D. Pa. Dec. 13, 2013). Denying motion to dismiss race discrimination claim where plaintiff alleged that the employer treated him different after learning about his interracial relationship from wedding ceremony photographs plaintiff posted on his Facebook® page.

D. Work-Related Photo Enough for Employer Liability – *Amira-Jabbar v. Travel Services, Inc.*, 726 F. Supp. 2d 77 (D. Puerto Rico 2010). Plaintiff sued for hostile work environment based on a racist Facebook® photo comment made by a co-worker. The court held that the comment was sufficiently work-related because the photo was taken of a work-related outing to give rise to employer liability irrespective of whether the comment was posted during work hours or off duty.

E. Example of Biometric Technologies. Employers are increasingly using biometric technologies that utilize scans of employees' fingerprints, palms, and voice prints to track time and attendance as well as to provide security and restrict access to certain areas in the workplace. Requiring biometric software applications for BYOD access to company data is not an unlikely future occurrence. Not only will biometrics in the workplace raise privacy concerns,[3] but the use may also give rise to discrimination claims.[4]

F. Biometrics Violate Religious Beliefs – *EEOC v. CONSOL Energy, Inc. and Consolidation Coal Company*, Case No. 1:13-cv-00215-IMK (N.D. W. Va.). On September 25, 2013, the EEOC filed suit against Consol Energy and Consolidation Coal Company for religious discrimination by requiring an employee to use biometric hand scanner to trace employee hours and attendance. The employee repeatedly objected to the use of biometric scanning as the use violated his religious beliefs (Evangelical Christian). The employer refused to provide the employee with a religious accommodation, which ultimately resulted in the employee being forced to retire.

G. Cyberbullying and Negligence. Employees, including managers, may use their BYOD devices to cyberbully or harass fellow co-workers. Thirty-five percent of working adults have reported being bullied at work.[5] If the employer learns of the behavior and does not make efforts to correct, it can be held liable regardless of whether the harassing or bullying was on a non-employer website.

[3] Currently, collecting biometric information, such as DNA sampling, is considered a minimal privacy intrusion. In the criminal context, no warrant is needed and is considered an extension of other booking procedures such as fingerprinting. *See Maryland v. King*, 133 S. Ct. 1958 (U.S. 2013).

[4] Illinois and New York currently have laws regulating the use and collection of biometric data. Claims against employers for identity theft as a result of leaked employee biometric data are expected to increase as employer use of this security technology becomes more widespread.

[5] Workplace Bullying Institute, *2010 & 2007 U.S. Workplace Bullying Surveys*, available at http://www.workplacebullying.org/multi/pdf/survey_flyer.pdf.

H. Harassment on Non-Employer Blog – *Espinoza v. County of Orange*, 2012 Cal. App. Unpub. LEXIS 1022, (Cal. Ct. App. Feb. 9, 2012). Jury held employer liable and awarded plaintiff over $820,700 in damages for cyberbullying and harassment. Employees posted to a non-employer blog reprehensible and hurtful comments about plaintiff's disfigured hand, of which the employer had knowledge but failed to take remedial action to correct.

I. Retaliation on Non-Employer Blog – *Stewart v. CUS Nashville, LLC*, 2013 U.S. Dist. LEXIS 16035 (M.D. Tenn. Feb. 6, 2013). Denying summary judgment to employer for plaintiffs' retaliation claims where supervisors and management made negative and defamatory statements on a blog after the employees engaged in protected activity.

V. **Respondeat Superior Liability for BYOD Use and Misuse**.

> "A master is subject to liability for the torts of his servants committed while acting in the scope of their employment." Restatement (Second) of Agency § 219 (1958).

A. Employer Liability for Employee Cell Phone Use While Driving. The general rule appears to be that if the accident or damage occurred while the employee was acting within the scope of employment, then the employee is not liable.

1. **Employer Cell Phone Policy Held Liable** – *Chatman-Wilson v. Cabral, Nueces Co. and Coca-Cola, Inc.*, Texas, Ct. At Law No. 2, Docket No. 10-61510-2 (2012). Employer ordered to pay $21.5M for employee's car accident resulting from talking on her personal cell phone while driving. Coca-Cola, Inc. had a hands-free cell phone policy for all employees using cell phones for work purposes and employee complied with policy at the time of the car accident. Employer found vicariously liable to accident victim where employee was unharmed.

2. **Employee Using Phone for Work-Related Purposes** – *Clo White Co. v. Lattimore*, 590 S.E.2d 381 (Ga. Ct. App. 2003). Accident victim brought personal injury lawsuit, arguing that employer was liable for employee's car accident. Employer filed motion for summary judgment. Summary judgment denied because evidence showed employee was on his personal cell phone calling work when he got into a car accident, thus triggering employer liability under the doctrine of respondeat superior. The company provided the employee with a pager, but had the employee's cell phone number and the employee would regularly use his personal cell phone for work-related purposes.

3. **Employee Liable Because Talking with Friend** – *Hoskins v. King*, 676 F. Supp. 2d 441, 446 (D. S.C. 2009). Employer was not liable for wrongful death caused by car accident, even though employee was driving company car and using a cell phone provided by the company. Because employee was talking with a friend on the company-issued phone during the time of the accident, the employee was not acting within the scope of employment for liability to attach under respondeat superior.

B. Security Considerations. BYOD use implicates significant security concerns such as safeguarding company information in the event of lost or stolen devices and/or security breaches and potential violations of HIPAA for protected health or medical data.

1. **HIPAA Example**. In December 2013, the Adult & Pediatric Dermatology, P.C. paid a penalty of $150,000 and settled a HIPAA violation lawsuit resulting from the loss of an employee's unencrypted thumb drive, which contained information for over 2,200 patients. The thumb drive was stolen from the employee's car. The healthcare provider, and not the employee, was found liable in that the Office for Civil Rights determined the healthcare provider did not properly assess potential risks to confidential protected health information.

C. Other Potential Claims Against Employers.

1. **Improper Trade Practices** – Federal Trade Commission Guidelines, 16 C.F.R., Part 255. Employers may face liability for employees commenting on their employer's services or products on blogs or social networking sites if the employment relationship is not disclosed.

2. **Concerted Activity**. The National Labor Relations Board ("NLRB") has started filing charges on behalf of employees for violations of Section 7 of the NLRA regarding restrictions on concerted activity, maintaining that a rule prohibiting all non-business use of a device or device services is facially overbroad and limits employees' ability to openly discuss work-related concerns.

3. **Chapter 119, Florida Statute Violations**. Government employees who use personal social media sites to conduct government business may convert the content of those sites to public records, meaning that the content is now required to comply with the Florida Public Records Act for purposes of access, storage and disclosure.[6]

VI. **Employee Liability**.

A. Employees Departing Employment. BYOD usage means that employees can easily and even unintentionally separate from their employer but retain company information and trade secrets on a personal device such as a thumb drive, external hard drive, personal laptop computer, personal smart phone or other personal electronic device. This exposes them to several legal violations including but not limited to misappropriation, conversion, spoliation, negligence, tortious interference.

1. **Can an Employer Require a Former Employee to Bring His or Her Personal Device to the Workplace for Inspection?** Possibly, yes. This ability is determined by the reason for the inspection and whether the employer has legal cause to inspect. If a security breach or misappropriation is suspected a former employee may need to seek injunctive relief.

[6] See AGO Opinion 2009-19 regarding the City of Coral Springs, Florida's desire to create its own Facebook® page.

- *AllianceBernstein L.P. v. Atha*, 100 A.D.3d 499 (N.Y. App. Div. 2012). Temporary restraining order attempting to prevent employer from getting defendant employee's personal iPhone information (which allegedly consisted of trade secret information and client information) was remanded with instructions for in camera review of iPhone such that all relevant disclosures could be made while protecting the privacy interests of the defendant. The iPhone in this case was compared to a laptop computer.

2. **Misappropriation of Trade Secrets**. Check your own state's law in this area as the definition of trade secret can vary from state to state. Florida has adopted the Uniform Trade Secrets Act. Employees could use their BYOD devices to disclose an employer's trade secret, proprietary information or other information that an employer may not want publicly available, or which may give rise to liability for the employer.

   a. Wiping Own Device is Misappropriation – *1-800-East W. Mortg. Co. v. Bournazian*, 2010 Mass. Super. LEXIS 158 (Mass. Super. Ct. July 18, 2010). Employee sanctioned and held liable to employer for using CCleaner to wipe clean his desktop hard drive of sensitive information and then destroying his Toshiba external hard drive. He committed these acts less than seven hours after the court hearing and entry of the order, and less than 18 hours before employer's experts were scheduled to appear at his home to copy his electronic storage devices pursuant to the stipulated order.

   b. Home Computer, Via Employer's Remote Access Server – *Liebert Corp. v. Mazur*, 357 Ill. App. 3d 265 (Ill. App. Ct. 1st Dist. 2005). Misappropriation established where former employee downloaded 60 megabytes of data from former employer's limited access server to his home computer.

   c. Misappropriation With Thumb Drive – *EMC Corp. v. Arturi*, 2010 U.S. Dist. LEXIS 132621 (D. Mass. Dec. 15, 2010). Former employee found liable for misappropriation when he took with him from former employer a personal thumb drive containing thousands of the former employer's confidential files.

   d. Misappropriation With External Hard Drive – *ABT, Inc. v. Juszczyk*, 2010 U.S. Dist. LEXIS 91613 (W.D.N.C. Aug. 9, 2010). Misappropriation established where former employee "copied confidential, proprietary, and trade secret information maintained on his [work] laptop and belonging to [his former employer] to his personal Seagate external hard drive."

3. **But Is It Actually a Trade Secret?** The employer still has the burden to show the information meets the trade secret test. Just because employer information has been misappropriated does not mean that it is also a valuable trade secret. The rise in use of websites like LinkedIn© and Facebook® makes it more difficult for employers to protect client contacts or customer lists because those outlets provide public access to

contacts which are connected on social media sites, such as LinkedIn© and Facebook®.

- *Applogix Dev. Group, Inc. v. Dallas Cent. Appraisal Dist.*, 2006 U.S. Dist. LEXIS 61564 (N.D. Tex. Aug. 29, 2006). "That a former employee copies his personal hard drive before he departs does not transform those files into valuable, proprietary data guarded to the requisite degree to meet the trade secret test. A showing must still be made that a specified trade secret exists."

- *E.I. du Pont de Nemours & Co. v. Kolon Indus.*, 803 F. Supp. 2d 469 (E.D. Va. 2011). In a trade secret misappropriation suit, plaintiff manufacturer was entitled to sanctions consisting of attorneys' fees and costs incurred in moving for sanctions as well as an adverse inference instruction regarding spoliation because the record established intentional and bad faith deletion of relevant files and e-mail by key employees of defendant manufacturer after suit was filed.

- *Sasqua Group, Inc. v. Courtney*, 2010 U.S. Dist. LEXIS 93442 (E.D. N.Y. Aug. 2010). Court found that where contacts and customer information could be ascertained through an Internet search, such as LinkedIn©, Facebook®, etc., there was no protection to the customer list as a trade secret, especially if the employer does not take any steps to protect its customer lists.

4. **Employee Negligent with Employer Data.**

   a. Third-Party Liability. A defendant who negligently permits a third party to intrude into the plaintiff's affairs may be held liable for that intrusion.

   b. Text Messages With Sensitive Data Disclosed To Third Party – *Babatu v. Dallas Veterans Affairs Med. Ctr.*, 2014 U.S. Dist. LEXIS 19596 (N.D. Tex. Feb. 18, 2014). Defendant's summary judgment motion denied where plaintiff sued defendant health care provider and individual employee for both statutory and common law privacy violations because defendant's employee disclosed text messages from plaintiff containing information about his participation in a drug treatment program to a third party. Such information and disclosure was not in the scope of employee's duties.

PRACTICAL TIP:

♦ **Confidential Information** – Instruct clients to refrain from disclosing confidential information about the company or their co-workers, or from using the company name or logo in connection with any personal online communications.

VII. **Employee Violation of the Computer Fraud and Abuse Act, 18 U.S.C. §1030 ("CFAA")**. Here, the concern is that an employee using his or her BYOD device to remotely access employer information may violate the CFAA by exceeding their authorization and causing loss to employer as a result.

A. *Cont'l Group, Inc. v. Kw Prop. Mgmt., LLC*, 622 F. Supp. 2d 1357, 1364 (S.D. Fla. 2009). Employee used personal laptop and personal USB device for work-related matters during her employment at Continental. Continental sought a preliminary injunction to force employee's new employer to be restrained from retaining or using any of Continental's confidential information. The preliminary injunction was granted as to the claims for breach of restrictive contract with the employee and tortious interference with restrictive covenants, and was denied as to the claim for violation of the CFAA and tortious interference with customer relations. The new employer and the employee's motion to dismiss was granted as to the CFAA claim.

1. **Device with Internet Connection Sufficient as "Protected Computer"[7] for Jurisdictional Purposes**. The court denied Continental's motion for a preliminary injunction with respect to the claim under the CFAA, 18 U.S.C.S. §1030, because the issue of whether Continental's computer was a "protected computer" under the CFAA was a non-starter. Not only could Continental defeat the new employer's motion to dismiss as there was more than enough evidence to raise its claims beyond a speculative level, but Continental had shown a substantial likelihood of success that its computers were in fact "protected computers" as defined under 18 U.S.C.S. §1030(e)(2)(B) because they had an Internet connection that brought it into compliance with the interstate commerce requirement.

2. **Loss Required**. Because all loss had to be as a result of "interruption of service" and the data had to be impaired and not merely copied, the evidence that the company paid over $5,000 to its computer forensic consultant to investigate the integrity of its computers following the employee's alleged unauthorized access was insufficient to meet the jurisdictional threshold under 18 U.S.C.S. §1030(g).

B. Employer May Have Violated but Loss Required – *Eagle v. Morgan*, 2012 U.S. Dist. LEXIS 143614 (E.D. Pa. Oct. 4, 2012). Employer's access to a former employee's LinkedIn© site that was associated with the employer may have violated the CFAA, but summary judgment granted for the defendant because the plaintiff could not prove a cognizable loss as a result of the access.

[7] (2) the term "protected computer" means a computer—
(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
(B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;
18 U.S. Code § 1030(e)(2) - Fraud and related activity in connection with computers

C. Employee Violation.

a. **Broad Construction Means that BYOD Employee Misuse of Employer Information is Sufficient for Lack of Authorized Access** – *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010). Here, the court adopted a broad construction of the CFAA, that "without authorization" and/or "exceeds authorized access" includes employee misusing employer information that he or she is otherwise permitted to access. Employee found guilty of exceeding authorized access because the information was not in the furtherance of his job duties.

D. No Employee Violation.

1. **Unfettered Access** – *Ryan, LLC v. Evans*, 2012 U.S. Dist. LEXIS 59692 (M.D. Fla., Apr. 30, 2012). Relying on *Rodriguez*, the court declined to follow magistrate's finding of no unauthorized access where employees had unfettered access to employer data, information and computers and the right to add to, delete from and upload or download information.

2. **Full Administrative Access** – *Trademotion, LLC v. Marketcliq, Inc.*, 857 F. Supp. 2d 1285 (M.D. Fla. Feb. 14, 2012). Because an employee had been granted full administrative access, a claim could not be brought under the CFAA regardless of how access was used.

3. **Personal Websites** – *Lee v. PMSI, Inc.*, 2011 U.S. Dist. LEXIS 52828 (M.D. Fla. May 6, 2011). **NO** violation of CFAA where employee accessed personal websites from employer computer while working; further, employer could not show that employee was without authorization to access work computer.

4. **Still Authorized After Termination** – *Clarity Servs. v. Barney*, 698 F. Supp. 2d 1309 (M.D. Fla. 2010). CFAA claim failed because employee had authorized access to computer although used authorization to access an e-mail from the employer's e-mail account after his termination and deleted customer information on employer's laptop.

5. **Mere Use to Employer Detriment** – *Power Equip. Maint., Inc. v. Airco Power Servs.*, 2013 U.S. Dist. LEXIS 91484 (S.D. Ga. June 28, 2013). Cannot state a claim under the CFAA where employee had authorized access, properly accessed information, and merely used it to employer's detriment.

VIII. **State Law Conversion Claims**. Typically conversion claims are brought by employers against former employees for taking or destroying property belonging to the employer. However, employee counsel should consider using this cause of action against an employer when the employer destroys or takes employee data on their BYOD. Conversion, unlike the CFAA, does not require proof of a jurisdictional amount of damage. Failure to allege and prove $5,000 in loss automatically results in dismissal of the CFAA claim. See, e.g., *Nexans Wires S.A. v. Sark-USA Inc.*, 166 Fed. Appx. 559,

562-63 (2d Cir. 2006). No such loss needs to be alleged or proven for conversion. Finally, conversion provides a backstop for federal courts that may be hostile to the use of the CFAA against employees who have stolen data from their employer's computers for use in competition against their employer at a new job.

A. Measuring Damages – *R&B Holding Co. v. Christopher Adver. Group, Inc.*, 994 So. 2d 329 (Fla. Dist. Ct. App. 3d Dist. 2008). The appellate court reversed and remanded the case for a new trial on the conversion claim concerning items not returned to the agency at the end of the business relationship. The agency alleged that after the parties' business relationship ended, the client kept advertising materials and other property belonging to the agency. The client argued on appeal that replacement cost was not a proper methodology for valuation of the unreturned items. As to the merits, the agency presented no testimony tending to show any losses for the unreturned items, or their value to the agency. Nor was there any testimony that decade-old advertising materials, for which the agency had been previously compensated by the client, were necessary for the agency's ongoing business operations. There was no evidence as to the economic consequences, if any, that were directly tied to the agency's possession of the unreturned items before conversion. The trebling of the civil theft damages for converted items that were replaced was affirmed, but the trebling of the interest award was reversed.

B. Actual Value Not Required – *Warshall v. Price*, 629 So. 2d 903 (Fla. Dist. Ct. App. 4th Dist. 1993). The court ruled that appellant/doctor had sufficiently proven all elements of conversion even though the patient list had no inherent value as he was denied exclusive possession. Appellant/doctor employed appellee/doctor. Appellee obtained a computer-generated list of appellant's patients at the time he departed employment. Appellee opened his own office and contacted all of appellant's patients, without disclosing the fact he was no longer associated with appellant. Appellee then sued appellant for past bonuses and appellant counter-sued for civil conversion of the patient list and breach of a non-compete clause. The court directed a verdict for appellee on the conversion claim, and appellant sought review. In reversing, the appellate court held there was sufficient evidence to support the conversion claim because all of the elements had been met. A conversion suit was proper even if the property converted had no actual value.

IX. **Discovery Issues Resulting From BYOD Devices**. An employer may have the ability to subpoena both the employee's personal device and the data, if necessary, to comply with duties of production.

A. Employer's Duty to Preserve Data. The trial court has broad discretion to permit a jury to draw adverse inferences from a party's destruction or failure to preserve evidence. Indeed, remedies for destruction of evidence or a failure to preserve vary greatly from state to state. While a finding of bad faith suffices to permit such an inference, it is not always necessary. To allow an adverse inference from the absence, loss or destruction of evidence, it would have to appear that the evidence would have been relevant to an issue at trial and otherwise would naturally have been introduced into evidence. Even the mere failure to produce evidence that naturally would have justified a fact at issue permits an inference that the party fears to produce the evidence; this fear is some evidence that the

circumstance or document or witness, if brought, would have exposed facts unfavorable to the party.

- *Jain v. Memphis Shelby County Airport Auth.*, 2010 U.S. Dist. LEXIS 16815 (W.D. Tenn. Feb. 24, 2010). Court ruled that the scope of the duty to preserve includes a duty to notify the opposing party of evidence in the hands of third parties.

- *Velez v. Marriott PR Mgmt.*, 590 F. Supp. 2d 235 (D.P.R. 2008). Court held that the scope of the duty to preserve includes a duty to notify the opposing party of evidence in the hands of third parties.

- *In re WRT Energy Secs. Litig.*, 246 F.R.D. 185 (S.D.N.Y. 2007). If a party cannot fulfill the duty to preserve because he does not own or control the evidence, he still has an obligation to give the opposing party notice of access to the evidence or of the possible destruction of the evidence if the party anticipates litigation involving that evidence.

- *Cache La Poudre Feeds, LLC v. Land O'Lakes Farmland Feed, LLC*, 244 F.R.D. 614 (D. Colo. 2007). "The court is not inclined to penalize a party for failing to approach former employees in an effort to respond to 'catch-all' or nearly indecipherable requests for production."

1. **Litigation Holds on Employee Personal Devices and Data**. When litigation against an employer is anticipated or commences, employees using personal devices may have information or evidence on their personal devices relevant to the litigation that will require the employer to issue a litigation hold and/or to preserve the information on the employee's personal device.

B. Employee's Duty to Preserve Data. Counsel for both the employer and employee have an obligation to ensure that data is preserved. Counsel typically accomplishes this through a litigation hold notice. As to when the obligation to preserve is triggered, check your applicable state and federal laws. With regard to penalties for not preserving data, the trial court has broad discretion from dismissing a case to permitting a jury to draw adverse inferences from a party's destruction or failure to preserve evidence.

1. **Employee's Duty to Preserve Misappropriated Data** – *Nucor Corp. v. Bell*, 251 F.R.D. 191 (D.S.C. 2008). Defendant/employee admitted that he downloaded information on plaintiff's production processes to his thumb drive. The court held that the employee engaged in sanctionable spoliation by willfully and deliberately throwing the thumb drive away so that plaintiff could not obtain it. The court found that the employee had a duty to preserve the thumb drive because he anticipated litigation prior to the time he destroyed the thumb drive. The court held that defendant/employee also spoliated evidence by continuing to use his laptop computer after litigation began.

2. **Cease Use of Device to Preserve Data**. The presence of plaintiff's confidential information on the laptop would make it more probable that defendant misappropriated plaintiff's trade secrets. It was inevitable that a substantial amount of data in unallocated space was lost because defendant continued to use the computer while under a duty to preserve evidence.

3. **Installing Additional Programs Sufficient for Alteration**. Defendant also significantly altered data during the relevant period by installing and uninstalling programs.

C. Failure to Preserve Results in Adverse Inference Spoliation Instruction.

- ***Gatto v. United Airlines***, 2013 WL 1285285 (D. N.J.). Plaintiff received adverse inference for deleting his own Facebook® account. Although Facebook® account was not the subject of litigation, entries potentially contradicted plaintiff's claims and were time stamped as occurring during the time period plaintiff's claims accrued.

- ***Southeastern Mech. Servs. v. Brody***, 657 F. Supp. 2d 1293, 1302 (M.D. Fla. 2009). Court held employer was entitled to an appropriate adverse inference jury instruction regarding employees' intentional wiping of data on their personal BlackBerrys®, for which they were reimbursed by employer, that would have been advantageous to employer and disadvantageous to employees.

D. Permitting Inspection of Device May Extinguish Duty to Preserve.

1. **Giving the Opposing Party an Adequate and Meaningful Opportunity to Inspect** – *Cedar Petrochemicals, Inc. v. Dongbu Hannong Chem. Co.*, 769 F. Supp. 2d 269 (S.D.N.Y. 2011). Court ruled that the duty to preserve may be extinguished by provision to the opposing party of an "adequate and meaningful opportunity to inspect" the evidence.

PRACTICAL TIP:

- **Obligation to Preserve** – Make sure you inform your clients of their obligations to preserve and not to delete anything.

- **Expert Needed?** – Potentially retain an expert to properly preserve data.

2. **Burden of Production**.

   a. Employer's Duty to Produce Data on Third-Party Devices. This duty to produce has largely to do with factors of ownership, custody or control of the data.

   b. Ability to Acquire – *Chevron Corp. v. Salazar*, 275 F.R.D. 437 (S.D.N.Y. 2011). Court held no evidence that former employee was "unwilling or unable" to

provide her employer with the relevant contents of her Google™ e-mail account or that the employer lacked the practical ability to acquire it from employee despite its being located on her private e-mail account rather than on employee's server.

c. Electronic Communications Policies Can be Used to Demonstrate Employer Duty – *Helmert v. Butterball, LLC*, 2010 U.S. Dist. LEXIS 60777 (E.D. Ark. May 27, 2010). Court ordered Butterball to "search hard drives, laptops, and the personal email accounts" of two members of its upper management when Butterball failed to "explain why these accounts are not reasonably accessible or unlikely to lead to the disclosure of relevant information."

d. Possession Not Required – *McCoy v. Whirlpool Corp.*, 214 F.R.D. 637 (D. Kan. 2003). Defendant/manufacturer represented to the court that it had conducted a thorough search for documents responsive to the discovery request in its possession and that all such documents had been produced. However, court ordered defendant/manufacturer to identify – of the 21 employees identified by plaintiffs in the discovery requests at issue – which employees had left defendant/manufacturer's employ and to contact such former employees to ascertain whether they took responsive documents with them when they left. If additional documents discovered, defendant/manufacturer was required to produce such documents to plaintiffs. If, however, no additional documents were discovered, defendant/manufacturer required to file a pleading with the court certifying compliance.

e. Employer's Duty to Notify Opposing Party of Data in Possession of Third Party. If a party knows or has reason to know that data could exist on employee personal devices, that party has a duty to notify opposing party of such.

f. Rule 34 Requirements – *Flagg v. City of Detroit*, 252 F.R.D. 346, 347 (E.D. Mich. 2008). Court held that city/defendant had sufficient control over city employees' text messages, albeit on city cell phones, to satisfy production requirements under Rule 34. In lieu of ruling on third-party service provider's motion to quash subpoena for defendant's text messages, court instructed plaintiff to serve Rule 34 request on defendant.

- *Flagg* at 252 F.R.D. at 353-54. Court ordered initial review of text message in camera to identify relevant information and then afforded defendant an opportunity to raise objections, "as a means of protecting against disclosure to Plaintiff of irrelevant, privileged or otherwise non-discoverable materials."

g. Practical Ability – *Exco Operating Co., LP v. Arnold*, 2011 U.S. Dist. LEXIS 138974 (W.D. La. Dec. 2, 2011). "Rule 34's definition of 'possession, custody, or control,' includes more than actual possession or control of the materials; it also contemplates a party's legal right or practical ability to obtain the materials from a nonparty to the action."

h. Subpoena Goes to Employer Control or Ownership Rather than Employee's Access or Possession – *Schaaf v. Smithkline Beecham Corp.,* 233 F.R.D. 451 (E.D.N.C. 2005). Court quashed subpoena issued to employee directly because documents sought were owned by company.

i. Corporate Level Employee Deem to Control Employer Documents – *McIntosh v. Kochan*, 2007 U.S. Dist. LEXIS 102848 (E.D.N.C. Nov. 7, 2007). Distinguishes *Schaaf v. Smithkline* because employee was higher-up/corporate level and thus was considered to be able to exercise control over documents.

j. Policy Obviates Employer Duty – *Hatfill v. New York Times Co.,* 242 F.R.D. 353 (E.D. Va. 2006). Court held that defendant/newspaper formally ceded to its reporters/employees any right to possess or control dissemination of notes and unpublished materials saved on an employees' personal flash drive pursuant to a collective bargaining agreement with the reporters' union.

   - Important case because appears the court would have required defendant newspaper to preserve, review, collect and produce documents on employee's personal flash drive absent policy embedded in collective bargaining agreement.

k. Control is Key – *Convertino v. United States DOJ*, 2013 U.S. Dist. LEXIS 5716 (E.D. Mich. Jan. 15, 2013). Court quoted *Hatfill*, stating that employer had legal right and control over employees' notes for production purposes although company policy indicated employer regularly destroyed employees' notes.

l. Control is Ability to Obtain from Non-Party – *Morris v. Lowe's Home Ctrs., Inc.*, 2012 U.S. Dist. LEXIS 44422 (M.D.N.C. Mar. 29, 2012). "A document is in a party's control when the party has 'the right, authority or practical ability to obtain the documents from a non-party to the action.'"

m. Reasonably Available – *Gray v. Faulkner*, 148 F.R.D. 220 (N.D. Ind. 1992). A party responding to a Rule 34 production request "cannot furnish only that information within his immediate knowledge or possession; he is under an affirmative duty to seek that information reasonably available to him from him employees, agents, or others subject to his control."

n. Corporate Employees Within Employer's Control – *Herbst v. Able*, 63 F.R.D. 135 (S.D.N.Y. 1972). Court held that corporate employees were within the corporate defendant's control and that defendant must obtain copies of SEC transcripts from the employees.

o. Good Faith Effort to Demonstrate Control – *Searock v. Stripling*, 736 F.2d 650 (11th Cir. Fla. 1984). "Control is defined not only as possession but as the legal right to obtain the documents requested upon demand….We do not, however, completely rest our holding on this factor of 'control.' We find instead that the

primary dispositive issue is whether [the defendant] made a good faith effort to obtain the documents over which he may have indicated he had 'control' in whatever sense, and whether after making such a good faith effort he was unable to obtain and thus produce them."

p. Employer Control Over Former Employee's Documents – *Export-Import Bank of the United States v. Asia Pulp & Paper Co.*, 233 F.R.D. 338 (S.D.N.Y. 2005). Court found no indication that corporation did not have practical means to obtain relevant work-related portions of former employee's journal given that former employee appeared for his deposition.

PRACTICAL TIP:

- **No Time Limit** – Plaintiffs should understand that electronic communications can be stored for years, infinitely in fact, and retrieved in litigation long after they have forgotten their existence.

X. **Potential Wage Claims for BYOD Users**. It is well-established under the Fair Labor Standards Act ("FLSA") that employers must compensate non-exempt employees for out of office time worked that benefits the employer and the business, including overtime pay. *Steiner v. Mitchell*, 350 U.S. 247, 256 (1956).

A. Still De Minimis? **–** Widespread use of BYOD means that employees are working off the clock more than ever. Work activities previously considered de minimis and therefore incompensable are now commonly recognized as compensable because of the increasing frequency of occurrence:

- *Levias v. Pac. Mar. Ass'n*, 760 F. Supp. 2d 1036, 1046 (W.D. Wash. 2011). "The de minimis doctrine provides that, even if certain activities are otherwise compensable under the FLSA, these activities are non-compensable if they involve an 'insubstantial and insignificant' amount of time because the FLSA does not compensate "a few seconds or minutes of work beyond the scheduled working hours.'" Still, courts recognize that the aggregate amount of those same "seconds or minutes" of work can be compensable if the work activity is one that the employee engages in regularly.

- *Farris v. County of Riverside*, 667 F. Supp. 2d 1151, 1166 (C.D. Cal. 2009). De minimis factors to consider are: "(1) the practical administrative difficulty of recording the additional time; (2) the aggregate amount of compensable time; and (3) the regularity of the additional work" (citing *Lindow v. United States*, 738 F.2d 1057, 1063 (9th Cir. 1984).

- *Allen v. City of Chicago*, 20 Wage & Hour Cas. 2d (BNA) 1124 (N.D. Ill. 2013). Class certified for employees who were "required to use" employer-issued PDAs to perform work outside of normal working hours without receiving compensation –

including overtime compensation. Work was "routinely and regularly accomplished through the use of these PDAs."

B. Portal-to-Portal Act. Additionally, courts have held that activities performed at the beginning and end of workday, such as starting laptops, checking and responding to e-mails and voice mail, making work-related phone calls and reviewing the day's assignments all "constituted principal activities under the Portal-to-Portal Act for which they were entitled to overtime compensation under the FLSA."

- *Dooley v. Liberty Mut. Ins. Co.*, 307 F. Supp. 2d 234 (D. Mass. 2004). The *Dooley* court has also held that employees are also entitled to compensation for travel time if they can show that principal work activities began at home, prior to the commute. *Id.*

- *Frew v. Tolt Techs. Serv. Group, LLC*, 2010 U.S. Dist. LEXIS 11991 (M.D. Fla. Feb. 10, 2010). Employer required to pay for: (1) work performed during unpaid lunch breaks; (2) service calls taken on employee's personal cell phone outside of the time he was clocked in; and (3) overtime worked but not reported on his time sheets.

C. On Call and Engaged to Wait. With BYOD, the employer has constant access to employees via text messages, phone calls, e-mail notifications and other online applications. The FLSA states that an employer must pay its employees for all of the time the employer employs them, even if the work is unrequested. This includes the time that the employee is in the office and "all other time during which the employee is suffered or permitted to work for the employer." 29 C.F.R. §553.221.

- *Rutti v. Lojack Corp., Inc.*, 596 F.3d 1046, 1061 (9th Cir. 2010). Several courts have held that so long as the employer remains in control of the employees' time, that time is compensable.

- *O'Neill v. Mermaid Touring Inc.*, 21 Wage & Hour Cas. 2d (BNA) 367 (S.D.N.Y. 2013). The employer is liable for overtime compensation when the employee is "engaged to wait" and cannot use the time for his own benefit.

- *Mohammadi v. Nwabuisi*, 2014 U.S. Dist. LEXIS 64 (W.D. Tex. Jan. 2, 2014). Employer found liable for not compensating employee for overtime work performed with personal cell phone and from personal e-mail address. Because employer failed to keep accurate and complete records, employee's oral recollection of time worked met employee's burden for recordkeeping.

PRACTICAL TIP:

♦ **Non-Exempt Work** - When evaluating a plaintiff's claims, always inquire as to how they are paid and what kind of work they do. If plaintiff is considered non-exempt and using BYOD, he or she could have an FLSA claim.