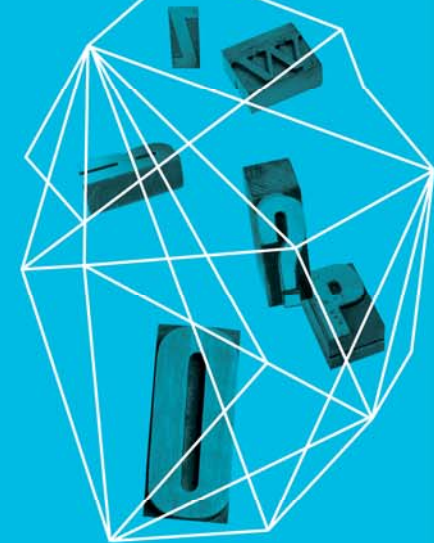


Tracking Employees Via Mobile Devices: Legal or Not?

Aaron Turner
President, IntegriCell

Randy Sabett
Counsel, ZwillGen PLLC

Security in
knowledge



Session ID: LAW-W23

Session Classification: Intermediate

— This presentation is not legal advice

- ▶ You want a lawyer? Go pay for one!
- ▶ We're going to walk through several hypothetical scenarios dealing with situations that don't really have good precedents but will compare/contrast to existing precedent.
- ▶ We'll make this as fun as we can



— Who are these people?

▶ Aaron Turner

- ▶ Involved in many aspects of security research relating to mobile infrastructure, mobile payments, mobile apps
MOBILE MOBILE MOBILE!
- ▶ Founder of IntegriCell



▶ Randy Sabett

- ▶ Technology and privacy law specialist who also worked for the NSA in the past
SUPER GEEKY PRIVACY ATTORNEY
- ▶ Counsel at ZwillGen PLLC



— History of intercepting comms

- ▶ 1967: Katz v. US
 - ▶ USSC rules that use of technology constitutes a 'search'
 - ▶ Citizens are entitled to a 'reasonable expectation of privacy' in their communications (be they in-person or using technology)
- ▶ 1968: Wiretap Act passed
 - ▶ Protected privacy of wire and oral communications, and
 - ▶ Defined a uniform basis for interception processes, procedures, etc.
- ▶ 1986: Electronic Communications Privacy Act (ECPA)
 - ▶ Updated and clarified privacy protections in light of 'dramatic changes in technologies'
 - ▶ What we now know as 18 USC §§ 2510 – 2521
 - ▶ Special shout out to my phreaker phriends!



— Employer considerations

- ▶ Own the backend + own the frontend =



- ▶ Email@companyname.com + email on company-owned device =



- ▶ Voicemail @ company phone + stored on company server =



— Good to go!

▶ **General precedents for these abilities:**

- ▶ Exception exists to ECPA permits employers to monitor employee email
- ▶ State law permits employers to read/monitor employees' corporate emails or internet use (but the right is not unlimited)

▶ **Case law precedents:**

- ▶ ***Sporer v. UAL Corp.***, (N.D.Cal. 2009): employee lacked REP in work email; employer had policy of monitoring computer use and warned employees that they had no expectation of privacy on email transmitted on the company system.
- ▶ ***United States v. Simons***, (4th Cir. 2000): employee's belief that computer files were private not reasonable; employer policy reserved right to "audit, inspect, and monitor"
- ▶ ***Smyth v. Pillsbury Co.***, (E.D. Pa. 1996): no REP in email communications over a company email system, even when the employee has been assured by management that corporate email will not be monitored.
- ▶ ***Sitton v. Print Direction***, (Ga. App. 2011): no privacy rights violation for accessing employee's personal computer to print personal email messages where (a) employee used computer at work for non-work purposes and (b) legitimate interest existed to investigate if employee running competing business

— Be careful...

- ▶ Rights of employers not unlimited:
 - ▶ Not ok where privileged (*Isom*), employer guesses p/w (*Fischer*), no announced policy (*Heckenkamp*)
 - ▶ Several states have enacted laws prohibiting employers from requesting employees or applicants to provide access to their personal Internet accounts, including social networking sites: CA, DE, IL, MD, MI, and NJ.










— Mobile technologies... ?

Corporate-owned
Tower










Corporate-owned
Devices

- ▶ Corporate calls from POTS 
- ▶ Corporate emails 
- ▶ Corporate application data 
- ▶ SMS messages directed to Corporate LOS 
- ▶ Personal Google Voice/Skype calls 
- ▶ Personal emails 
- ▶ Personal application data 

Corporate-owned
Tower



Personal Devices

- ▶ Corporate calls from POTS 
- ▶ Corporate emails 
- ▶ Corporate application data 
- ▶ SMS messages directed to Corporate LOS 
- ▶ Personal Google Voice/Skype calls 
- ▶ Personal emails 
- ▶ Personal application data 

— Extending the precedents...

- ▶ Generally, employer can monitor calls/vmail/SMS made on employer's equipment
- ▶ Case law:
 - ▶ ***Shefts v. Petrakis***, (C.D. Ill. 2010): Business Use Exception places monitoring of communications done in ordinary business outside the purview of the Wiretap Act.
 - ▶ ***Ali v. Dougals Cable Communications***, (D. Kan. 1996): Business Use exception permitted employer's practice of monitoring in person all business calls and intercepting personal calls *only to extent necessary* to determine whether call was personal, and not for unwarranted surveillance)(emphasis added).
 - ▶ ***O'Sullivan v. NYNEX Corp.***, (Mass. 1997): employer may monitor an employee's business-related calls as long as the employer offers a legitimate business reason
 - ▶ ***United States v. McLaren***, (M.D. Fla. 1997): employer (an electronic communication service provider) intercepting 211 calls involving its employee's cellular telephone in investigation of cloning fraud was not so unreasonable as to warrant blanket suppression of total fruits of the effort



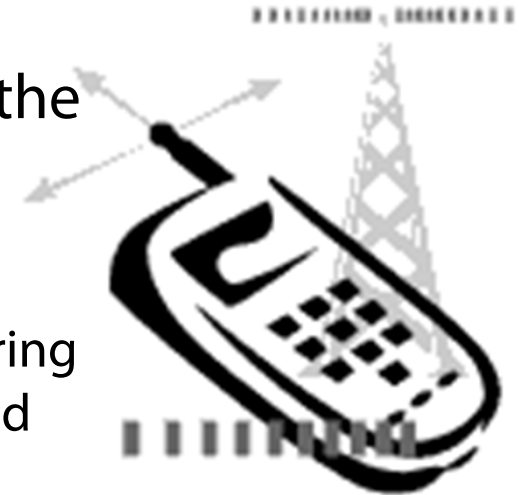
— It depends...

▶ Other considerations:

- ▶ Monitoring ok if employee consent (can be implied by conduct)
- ▶ State statutes can be more restrictive re consent; laws of 38 states do not permit call recording unless one party consents; 12 states (including California) generally prohibit the recording of phone calls unless all parties provide consent
- ▶ Reasonable expectations of privacy not static (e.g., Supreme Court decision in *Quon* case from 2010)
- ▶ Employee-owned: more likely to be deemed a privacy violation, unless business cause to investigate, e.g., breach of loyalty, harassment, etc.

— What was that?

- ▶ So... what about situations where the enterprise provides the cell towers or corporate-owned & operated micro-cell in the building
- ▶ Legal analysis:
 - ▶ No different from the earlier scenario of monitoring email, vmail, calls, or SMS on an employer-owned and issued device.
 - ▶ Employees should be placed on heightened notice that their activities will be monitored for network administration or other legitimate business purposes
 - ▶ No known case law on this issue



— Crazy stuff we've seen...

- ▶ So... what's the enterprises' duty of care to protect the infrastructure (e.g., rogue tower sitting in your parking lot in the back of a white van)
- ▶ No case law directly on point, but much exists related to:
 - ▶ Protection of personal information
 - ▶ Employing proper technology to avoid negligence



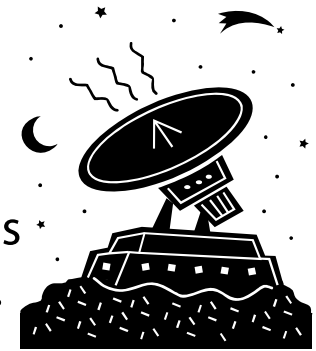
— More craziness

- ▶ Imagine a member of the cleaning crew is paid to insert a 4G USB network stick in the back of the CEO's admin's computer
- ▶ How can we legally find it?
 - ▶ Can an enterprise manipulate licensed spectrum?
- ▶ "It Depends"
 - ▶ Could the cleaning crew claim that the device is their personal device and that they had no expectation that the company would intercept it?
 - ▶ Will the carrier's object to us shutting down a line of service and thereby depriving them of revenue?



Stuff to keep in mind

- ▶ Protection of personal information:
 - ▶ Federal law (HIPAA/HITECH, GLBA, FTC, etc.)
 - ▶ State law:
 - ▶ MA regs – CISP, encryption, policies, training, etc.
 - ▶ NV law – PCI adopted into state law
 - ▶ CA and AK – “reasonable security measures” incorporated into the law
 - ▶ Negligent retention concepts
- ▶ Employing of “new” technology:
 - ▶ *T.J. Hooper* case (1932): "in most cases reasonable prudence is in fact common prudence, but strictly it is never its measure. A whole calling may have unduly lagged in the adoption of new and available devices. Courts must in the end say what is required. There are precautions so imperative that even their universal disregard will not excuse their omission."



— Some takeaways

- ▶ 1. Some broad generalizations can be made when dealing with employer monitoring of traditional comm's
- ▶ 2. With newer technology, lines not necessarily as clear
- ▶ 3. Often need to look at various use cases using a "reasonableness" approach
- ▶ 4. Not always appropriate to base analysis on "no one else doing it" rationale
- ▶ 5. In light of recent events, some commentators saying more active involvement with more advanced equipment is becoming the new norm
- ▶ 6. Make sure those computer and network use agreements are in place and regularly acknowledged



It's QUESTION TIME!!

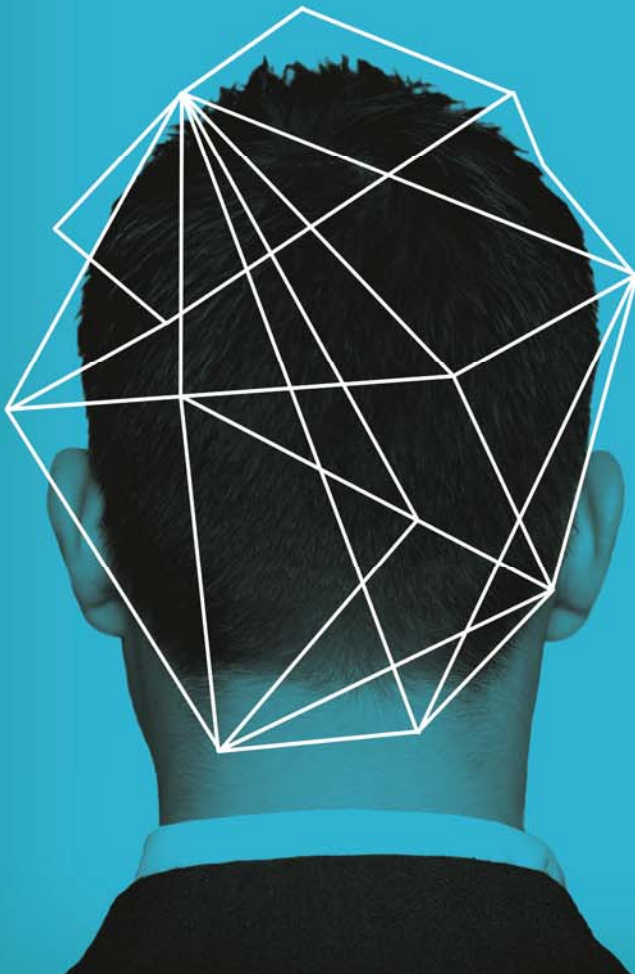
Thanks for your attention!

Aaron Turner

aaron.turner@integricell.com

Randy Sabett

randy@zwillgen.com



APPENDIX



— Federal Law

- ▶ Federal law applicable to electronic communications and phone conversations: Electronic Communications Privacy Act (ECPA)
 - ▶ Generally, prohibits monitoring but with exceptions
 - ▶ Specifically, Title II of ECPA, the Wiretap Act bars intentional interception, use, or disclosure of any wire/electronic communication, including phone, cell, vmail, email, etc. (18 U.S.C. § 2511(1)).
 - ▶ Any monitoring “in the ordinary course of its business,” (i.e. Business Use Exception). 18 U.S.C. § 2510(5). Thus, the Business Use Exception permits employers to intercept electronic communications for legitimate business purposes.