Electronic Surveillance – Legal and other Risks

Fred Williams

James, McElroy & Diehl, P.A.

Adjunct Prof., UNC-C, Dept. of Software & IT

Former AUSA, Dep. Criminal Chief, Computer & IP prosecutor.

“The [laws] they are a-changin”

~~~~

to a Brave New World?
~~~~

Main Topics

Risks for High Tech Surveillance

- Access to location – GPS, cells, etc.
- Photos & videos
- Access to emails and data

- Criminal liabilities
- Civil and ethical risks

Questions generally welcome

Law and Technology

- Technology changes society and law is slow to adapt
- Our Bill of Rights was a part of the social revolution associated with the economic revolutions of the 1700s.
- The information revolution is faster; there will be major changes in society, ethical standards, and laws over the next decades.

➔ Can there be firm answers?

Risks, uncertainties, traps for the unwary, hyper-technicalities

In many areas,

- There's enormous uncertainty as to what the law IS
- Even when law is clear, application to new technologies and societal values may be extremely difficult
- Regardless, the law is likely to change
- And so will juror attitudes

U.S. Supreme Court

- Troika of cases re new technologies change privacy and the 4th Amendment
- Do these foretell changes in other laws
  - Statutes?
  - Torts?
- Attitudes toward privacy are in flux, both among Justices and the general public

Kyllo v. United States,

533 U.S. 27 (2001)(Scalia)

Technology may erode privacy

Did not want "to permit [advancing] police technology to erode the privacy guaranteed by the Fourth Amendment."

Need to "assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted [1791]."

U.S. v. Jones,
565 U.S. __ (2012)(Scalia)

DoJ: in digital cases, apply the rule from the nearest real world analogue to the virtual world

- Hacker is like a burglar

Lower courts had found the nearest real world analogue to GPS was a cop following a car on streets – where driver had no REP

Jones rejected this way of deciding cases – throws much of what DoJ has been doing into limbo

Riley v. California,
573 U.S. ___ (6/25/14)

The courts had likened a cell phone ["digital world"] to physical objects in a person's pocket ["real world"]

BUT the Court reversed (8-0 + Alito):

- while old rule works "in the context of physical objects, neither of its rationales has much force with respect to digital content on cell phones."
- a cell contains a broad array of private info never found even in a home
  - **unless the phone is there**.

Advice

Be very conservative in re proposed spying

Risky area – more blacks than whites

If a court disagrees, the consequences could be terrible

Locational privacy

U.S. v. Maynard,
615 F.3d 544 (D.C. Cir. 2010)
S.Ct. decided it as Jones

- Held: extended 24/7 tracking is a search requiring a warrant – reversed conviction
- "the whole of a person's movements over the course of a month is not actually exposed to the public because the likelihood a stranger would observe all those movements … is essentially nil"
- the "whole reveals far more than the individual movements it comprises. The difference is not one of degree but of kind"

U.S. v. Jones

All 9 Justices agreed there was a 4th Am. violation

- 5 Scalia majority relied on the trespass to the car and didn't decide the REP issue
- 4 Alito concur relied on REP "the lengthy monitoring that occurred in this case constituted a search" requiring a warrant
- Sotomayor joined majority but expressed agreement with Alito opinion

131 L. Ed. 2d 911

She said, e.g., "GPS monitoring—by making available at ... low cost such a substantial quantum of intimate information about any person … may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'"

ACLU v Clapper (D.C.Cir. 5/7/15)

In its detailed decision finding NSA's mass collection of metadata about everyone's phone calls is illegal, the court found that:

- "the extent to which modern technology alters our traditional expectations of privacy" is
- "one of the most difficult issues in Fourth Amendment jurisprudence".

Focused on Jones and Sotomayor opinion

A few states have acted against GPS

Calif. prohibits “use an electronic tracking device to determine the location or movement of a person” because “electronic tracking of a person's location without that person's knowledge violates that person's” REP

Cal Pen Code § 637.7; Stats 1998 ch 449

imposition of a fee for every time rental car exceeded 79 miles per hour for 2 minutes, as determined by GPS, was unfair trade practice and contrary to public policy

Am. Car Rental, Inc. v. Comm. Cons. Prot., 273 Conn. 296 (2005)

GPS and damages

GPS on spouse's truck for 6 months; jury verdicts of (1) $2,500 for the trespass plus (2) $160,000 for Intentional Infliction of Emotional Distress by obstructing his access to children:

- "Her outrageous conduct included ... monitoring his activities by planting a GPS on his truck" – affirmed the $160k
- apparently would have affirmed the $2,500, but held it barred by a settlement with the PI

Tinory v. DePierre, 2015 Mass. App. Div. 23 (2/4/15)

Photos and videos

Is a pix more intrusive than 1000 intercepted words?

"video surveillance may involve a greater intrusion on privacy than audio surveillance" and we "see no constitutionally relevant distinction between audio and video surveillance ..."

- U.S. v. Lee, 359 F.3d 194 (3d Cir. 2004) (then Judge Alito)

Video "surveillance is identical in its indiscriminate character to wiretapping and bugging. It is even more invasive of privacy, just as a strip search is more invasive than a pat-down search … video surveillance can be vastly more intrusive" than audio surveillance.

- U.S. v. Nerber, 222 F.3d 597 (9th Cir. 2000)

NCGS § 14-202 – Peeping Tom

Prohibits e.g.:

- (a) "peep[ing] secretly into any room occupied by another person"
- (e) "secretly ... use[ing] any device to create ... image of another person underneath or through the clothing"
- (f) "secretly ... use[ing] or install[ing] in a room any device that can be used to create a photographic image" – "for the purpose of arousing … sexual desire"

Cf. 18 U.S.C. § 1801: only covers acts in the "special maritime and territorial jurisdiction of the" U.S.

Video camera in spouse's bedroom

punitive damages against spouse and PI – in part because they put "camera in the bedroom rather than in a less private area of the house"

- Miller v. Brooks, 123 **N.C.App.** 20 (1996)
- Clayton v. Richards, 47 S.W.3d 149 (Tex.App.2001)

$22k for innocuous video

- In re Tigges, 758 N.W.2d 824 (Iowa S.Ct. 2008)

Constitutes **domestic violence**, stalking, harassment

- HES v. JCS, 175 N.J. 309 (2003)

Emails and other electronic communications

City of Ontario v. Quon,
560 U.S. 746 (2010)

"Rapid changes in the dynamics of communication and information transmission are evident ... in what society accepts as proper behavior."

"many employers expect or at least tolerate personal use of such equipment by employees"

"it is uncertain how workplace norms, and the law's treatment of them, will evolve."

Key Federal Statutes

Real Time* Interception of Data

➔The Wiretap Act (Title III) – Content

Pen Register, Trap and Trace – not content

Access to Stored Data

Stored Communications Act (SCA)

➔18 U.S.C. § 1030(a)(2): unauthorized access to information on a computer

Electronic Communications Privacy Act (ECPA) amended Wiretap & added SCA in 1986

ECPA rules
based on series of dichotomies

Real time* vs. stored

Content of communications vs. non-content

Content

- unretrieved vs. retrieved e-mail
- unretrieved e-mail: stale vs. fresh
- retrieved: private v. public provider

Non-content: detailed vs. subscriber info

Basic Rule: real time content > protection

As an intrusion on your privacy, do you care whether:

Your letter is stolen from a mail truck while it is moving rather than stopped at a red light?

It is read before or after you receive it?

It is read before or after it has been in storage for 180 days ("stale")?

Should the law care whether your email is moving, read before or after you get it, or read six months after it was sent?

Pen-Trap §§ 3121-3127

Real time connection information – not content

Rarely relevant in private life

“war driving” or use of another's wireless internet MAY violate this statute

WIRETAP ACT

18 USC §§ 2510 – 2522

General Prohibition

The Wiretap Act prohibits the interception of wire, oral, or electronic communications and the use or disclosure of illegal interceptions

FIVE YEAR FELONY

unless a statutory exception applies

Wiretap Act is absolute

"except as otherwise **specifically** provided in this chapter" § 2511; Gelbard v. United States, 408 U.S. 41 (1972); Pritchard v. Pritchard, 732 F.2d 372 (4th Cir. 1984):

go to jail, do not pass go.

If a manager tells you to wiretap a problem employee, what is his defense?

What is your defense?

Statutes often hypertechnical

"When the Fifth Circuit observed that the Wiretap Act 'is famous (if not infamous) for its lack of clarity,' ..., it might have put the matter too mildly."

U.S. v. Smith, 155 F.3d 1051 (9th Cir. 1998)

"the complex, often convoluted intersection of the Wiretap Act and Stored Communications Act."

U.S. v. Councilman, 418 F.3d 67 (1st Cir. 2005)(en banc)

"a confusing and uncertain area of the law."

Konop v. Hawaiian Airlines, 302 F.3d 868 (9th Cir. 2002)

Use or Disclosure

The use or disclosure of the contents of illegally intercepted wire, oral, or electronic communications is also a 5 year felony.

- If you give it to someone, that's a criminal “disclosure.” § 2511(1)(c)
- If you have a PI follow someone or ask questions based on it, that's a criminal “use.” § 2511(1)(c) & (d)

U.S. v. Councilman,
418 F.3d 67 (1st Cir. 2005)(en banc)

- Company offered email services to customers, but copied incoming messages
- Owner indicted, dismissed, affirmed, then indictment re-instated en banc
- Even though the interception was within the computer and in very short storage while being processed, it was wiretap violation
  - "transient electronic storage that is intrinsic to the communication process"
- Acquitted at trial – defense argued no intent to copy before rather than after delivery

Real time intercept

Generally the courts have agreed that "intercept" requires contemporaneity -- bits in motion between a sender and a receiver, not bits in storage where SCA may apply

Technological changes make margins difficult

"keylogger" not a violation if capturing keystrokes to Word not to an e-mail??

BUT SEE Easterbrook dicta!

U. S. v. Szymuszkiewicz,

622 F.3d 701 (7th Cir. 9/9/10)

"we do not imply agreement with any statement that the interception must be 'contemporaneous.' Decisions articulating such a requirement are **thinking football** rather than the terms of the statute. There is no timing requirement in the Wiretap Act, and judges ought not add to statutory definitions."

Easterbrook, Chief Judge

- [this language was dicta, and was withdrawn 11/29/10]

Konop noted basic difficulty with the real time limitation

"'Intercept' is defined as 'the … **acquisition** of the contents of any wire, electronic, or oral communication ... '"

"Standing alone, this definition would seem to suggest that **an individual 'intercepts' an electronic communication merely by 'acquiring' its contents**, regardless of when or under what circumstances the acquisition occurs."

STORED COMMUNICATIONS ACT

18 USC §§ 2701 – 2712

§ 2701(a)

Access an ISP without or in excess of authorization "and thereby obtains, alters, or prevents authorized access to [an email] while it is in electronic storage"

§ 2702(a)(1)

Public ISP prohibited from disclosing emails

1 year misdemeanor or up to 10 year felony

Transaction records

Generally, no REP in 3d party records. Miller, 425 U.S. 435 (1976)(subpoena for bank customer's checks)

Warshak, 631 F.3d 266 (6th Cir. 2010), distinguished Miller and held there is an REP in your emails at your ISP because it has no interest in content

State v. Reid, 194 N.J. 386 (2008) (REP in subscriber info re an IP from ISPs)

- "names of stores ..., the political organizations ..., fantasies, her health concerns, ... intimate details about one's personal affairs ..."

Andersen LLP v. UOP, 991 F. Supp. 1041 (N.D. Ill. 1998)

- § 2702 prohibits disclosure of emails by a public provider of ECS
- Consultants worked at UOP's facilities and were allowed to use its e-mail system
- UOP divulged embarrassing e-mails to Wall Street Journal which published them
- Court ruled no SCA violation because UOP was not a **public** provider – UOP only a private provider

Devine v. Kapasi, 729 F.Supp.2d 1024 (N.D.Ill. 2010)

Anderson applies only to § 2702

- A company email system is a "facility through which an electronic communication service is provided"
- If company stores emails on its own system, it is a violation of § 2701 to access them intentionally and without authorization
- Does not matter whether it is in the business of providing that service or if it just does so for employees

Unauthorized access to computer

§ 1030(a)(2)

- Access without or in excess of authorization and obtain information
- From a protected computer = one used in commerce or communications
- Originally required interstate access
- Are there walk-by violations?
  - 5 year felony if for gain
  - 1 year misdemeanor if not

Does access include just looking?

YES!

- “'obtaining information' in this context includes mere observation of the data”
- “Actual asportation, in the sense of physically removing the data from its original location or transcribing the data, need not be proved in order to establish a violation”

S. Rep. No. 99-432 at 2484 (1986)

What is a computer?

"an electronic ... high speed data processing device performing logical, arithmetic, or storage functions ... [but not] an automated typewriter ... a portable hand held calculator ... ." § 1030(e)(1)

Cell phone? U.S. v. Kramer (8th Cir. 2011) (yes)

External hard drive? Thumb drive? Etc. Etc.

> "includes any data storage facility ... directly related to or operating in conjunction with such device ... ."

Violation of terms of service?

Lori Drew – indicted for obtaining info from FaceBook after violating ToS

Can you go to prison for reading N.Y. Times on line if you don't tell them your true income?

Who reads much less complies with ToS?

Do you know if it limits access to left handed red heads?

Drew involved a situation with difficult facts, but do hard facts make criminals of all of us?

WEC Carolina E. Sol., LLC v. Miller, 687 F.3d 199 (4th Cir. 2012)

Employee allegedly downloaded info and took it to new job

Court held that authority to access is not automatically rescinded by employee's intent to misuse info much less by violation of policy.

If company policy says no use of the system to check sports scores, is an employee who does so a criminal?

CONSENT

Wiretap – one party consent

Interception allowed if

- a "party to the communication has given prior consent to such interception
- **unless** such communication is intercepted for purpose of committing any criminal or tortious act"

§ 2511(2)(d)

Employee/user consent often found in:

- Banner
- terms of service
- employment agreement/policies

One vs. All Party Consent States

Federal, N.C., & most states – one party

BUT California Supreme Court created a trap for the unwary:

Calls from California (all party) to Ga. (one party); held violation of Calif's law.

Choice of law influenced by fact employees had to call Ga. re their stock options.

No damages for past violations.

Did not decide if criminal penalties apply.

Kearney v. Salomon Smith Barney, 39 Cal. 4th 95 (2006)

Banner/Policies need to be clear

Several cases have shown difficulty in finding consent when there are strong statements on banners, terms of service, employee handbooks, but somewhat contrary statements in the same sources or by supervisors undermine the statements.

A company needs to speak clearly and consistently if it wants to have its employees' consent to read their emails and hard drives.

Bring your own device & connect to LAN

Quon (S.Ct. 2010)

"employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated"

ducked issue whether supervisor's informal, oral statements overrode formal, written policies because "Prudence counsels caution before the facts in the instant case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations enjoyed by employees when using employer-provided communication devices"

Stengart v. Loving Care Agency,

990 A.2d 650 (N.J. S.Ct. 2010)

Employee quit; returned laptop; she had used it for email thru Yahoo; employer found emails with her lawyer, used them against her.

- Written policies very blunt: no privacy on computers, but also: "occasional personal use is permitted."

Court held this ambiguous and she had REP in her password protected web emails.

- Found it unethical for the lawyers to have used them

Implied consent -- secrecy

"Without actual notice, consent can only be implied when the surrounding circumstances convincingly show that the party knew about and consented to the interception."

"Pharmatrak's involvement was meant to be invisible to the user, and it was. Deficient notice will almost always defeat a claim of implied consent."

Pharmatrak Privacy Litigation, 329 F.3d 9 (1st Cir. 2003)

Common sense

"no reasonable employee would harshly criticize the boss if the employee thought that the boss was listening."

Dorris v. Absher, 179 F.3d 420 (6th Cir. 1999)

"Given the often sensitive and sometimes damning substance of his emails, we think it highly unlikely that Warshak expected them to be made public, for people seldom unfurl their dirty laundry in plain view."

U.S. v. Warshak, 631 F.3d 266 (6th Cir. 2010)

Can consent continue after fight?

I'd suggest its easier to imply revocation than consent.

- When married or business partners start yelling at each other and hiring lawyers, can you expect a jury to believe prior consent continues?
- When the system administrator has been fired, does she still have consent to use a back door into the system?

Coercion, fraud, deceit negate consent?

"Permission to access a stored communication does not constitute valid authorization if it would not defeat a trespass claim"

Held: deception negated consent

Assumed coercion would also

Theofel v. Farey-Jones, 341 F.3d 978 (9th Cir. 2003) (Kozinski)

Kroh v. Kroh, 152 N.C. App. 347 (2002)

"a custodial parent [may] vicariously consent to the recording of a minor child's conversations,

as long as the parent

has a good faith, objectively reasonable belief that the interception of [the] conversations is necessary for the best interests of the child"

Lazette v. Kulmatycki,
2013 U.S. Dist. Lexis 81174 (N.D.Oh. 2013)

Employee resigns and turns in Blackberry to supervisor; he uses it to access 48,000 of her personal emails; court rejected defenses that:

- He had right to access the Blackberry and thereby her gmail account
- She "negligently" consented because she didn't delete

If you accidentally leave a key to your house in your desk when you quit a job, do you consent for anyone who gets assigned that desk to visit your home? Make copies of your tax returns?

Van Alstyne v. Elect. Scriptorium, LTD,
560 F.3d 199 (4th Cir. 2009)

Employee sexually harassed and fired; her emails used against her in deposition; they had been obtained in violation of SCA

- jury awarded her $175,000 in statutory damages; $100,000 in punitives
- district court awarded $135,723.56 in attorney's fees and costs.

Fourth Circuit held:

- no statutory damages without actual damages
- allowed punitives and attorneys fees
- remanded re amounts

Internet and new media

Open fields

Fourth Amendment cases say no REP in open fields.

Is the internet an “open field”? Is every site a private “lot” with rules set by its owner?

Can an employer google a prospective employee? A lawyer a client?

Can they peek into their Facebook account?

Can they insist all employees “friend” them?

Social media

The law has hardly begun to cope with these phenomena.

Therefor its risky to predict.

Perhaps more importantly, social mores are developing.

The risks to public reputation and to employee morale are high.

Konop – reprise 1

NJ restaurant supervisors access password protected MySpace page for employees.

- 2 sue under SCA and NJ laws.
- Jury verdict $3,403 back pay and $13,600 punitive.
- Settled during appeal.

Konop – reprise 2

- Employee fired after she criticized her boss on Facebook.
- Policy barred depicting co. in social media.
- NLRB filed a complaint alleging this was unfair labor practice – right to talk jointly about working conditions.
- Settled: co. changed rules & agreed no discipline for workers' talk about work when not on job.

Web promotes knee-jerk reactions so everybody snoops!

questions re proposed spying

- 1. does a federal or state statute prohibit?
- 2. is there a REP?
- 3. is there a “trespass” - including to chattle?
- 4. is there a privacy tort, including one that may be expanded by judicial rulings and changing social norms?
- 5. is it possible that a juror or judge will think it outrageous or despicable, now or by time of trial?
- 6. do you **really** need it?

Privacy law is a mess

Traps for the unwary abound.

Many of the rules seem disconnected from social expectations and public policies.

Change is in the air

- Jones, especially Sotomayor's opinion

Conclusion -- Questions

B. Frederic Williams
James, McElroy & Diehl, P.A
600 South College St.
Charlotte, NC 28202
704-372-9870
fwilliams@jmdlaw.com

Key reference

justice.gov/criminal/cybercrime, the web site of the U.S. DoJ's Computer Crime & Intellectual Property Section, has lots of valuable material on computer law issues

E.g. a 300+ page book on "Searching & Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations"