

# 2012: The Year High Courts Got Involved in Tech Privacy Law and Made a Mess of IT

Stephen Treglia, Esq.

Legal Counsel, Recovery Services

Absolute Software Corporation

Presented at the 16<sup>th</sup> Annual

Cyber Security Conference

NYS Division of Homeland Security and Emergency  
Services

Office of Cyber Security

June 4, 2013

# Quick survey – Part 1

How many here are from:

- Law enforcement
- Gov't agencies (non-LE)
- Education field
- Private sector (non-schools)
- Communication industry

# Quick survey – Part 2

## How many here have at work:

---

- Computer use policy
- Internet use policy
- In writing
- Signed by each employee

# A Little About the Lecturer

- Concluded 30-year career as a prosecutor in 2010
- 1986 began using computers in mob investigations
- 1996 began doing computer crime investigations
- Created and supervised one of the first computer crime units from 1997-2010
- Fully functional in-house unit, forensics, cybercrime investigators, undercover investigators
- Now performs basically same function (plus others) with Absolute Software Corporation



# A Little About Absolute

- Leading maker of tracking software for stolen devices
- Software embedded in firmware of most laptops
- Software activated upon filing of theft report with police
- Software recently embedded in Samsung Galaxy 4
- Tracks current location and possessor of stolen device through IP addresses, key captures, screen captures, file inspection post-theft
- Absolute Investigators ex-law enforcement > 1000 yrs experience
- Absolute Investigators work worldwide to recover customers' stolen devices – currently nearly 30,000 recovered/100 per week

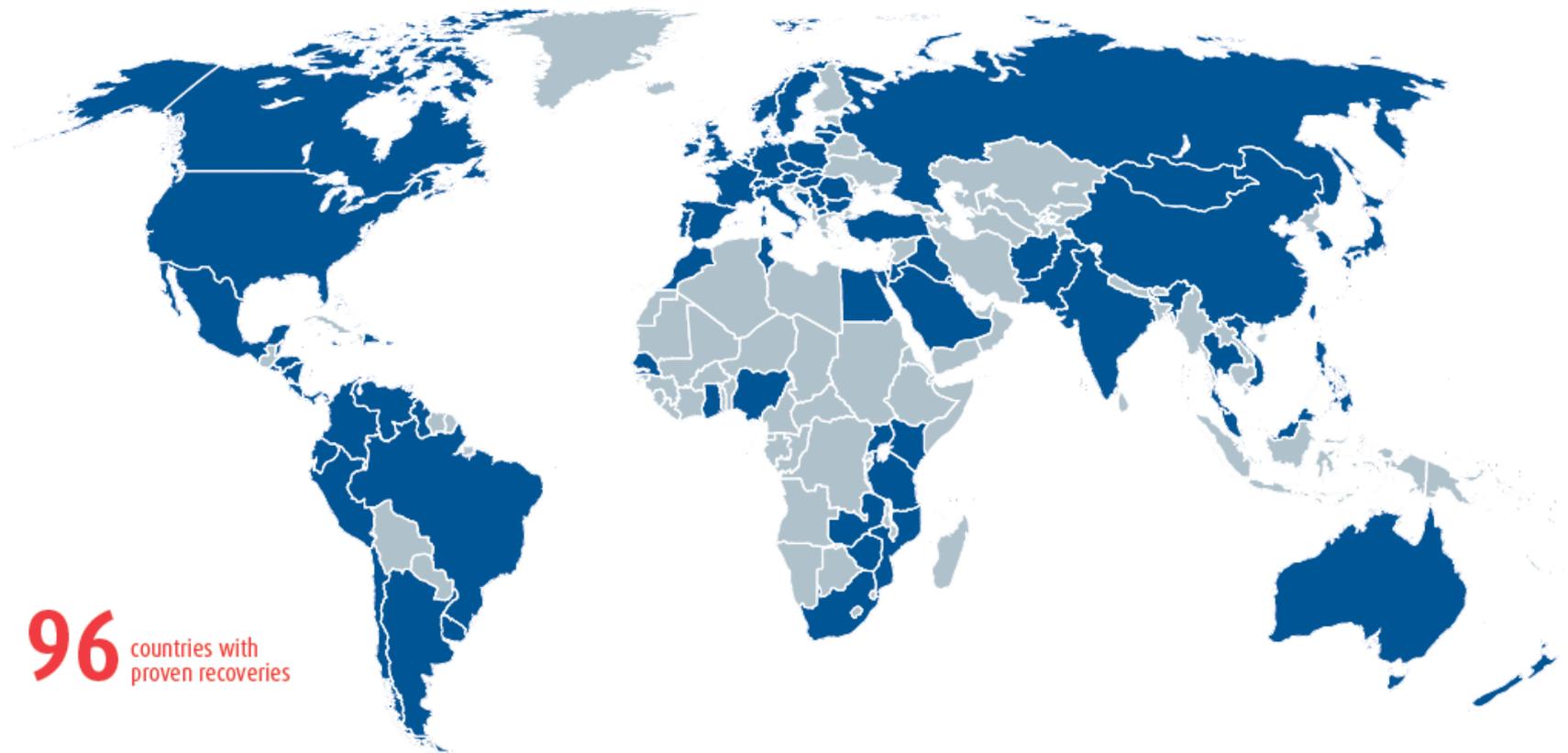
**Absolute**®Software

**Computrace**®  
BY **Absolute**Software

**LO/JACK**®  
FOR LAPTOPS  
BY **Absolute**Software

# Geographic reach of Absolute's recovery process

## Absolute Software Global Recovery Map



**96** countries with proven recoveries

Region	Territory	Country
	North America	Canada, Guam, Mexico, Puerto Rico, USA, Virgin Islands (U.S.)
	Latam-Caribbean	Bahamas, Cayman Islands, Curacao, Dominican Republic, Jamaica, Saint Kitts & Nevis, Saint Lucia, Trinidad & Tobago, Turks & Caicos Islands

Region	Territory	Country
	Europe	Austria, Belgium, Bosnia and Herzegovina, Bulgaria, Czech Republic, Denmark, France, Germany, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Macedonia, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Russian Federation, Serbia, Slovakia, Spain,

Region	Territory	Country
APAC	Asia-Central	China, Hong Kong, India, Japan, Mongolia, Singapore, South Korea, Taiwan
	Asia-SE	Australia, Fiji, Malaysia, New Zealand

# This is My 14<sup>th</sup> NYS Cyber Security Conference

And each year I feel like I'm increasingly screaming:



# I Fear It's Only Getting Worse

- Court decisions since the beginning of 2012 are proving me right
- Point of critical mass in the law
- My recurring theme today
- Unsure if courts can deal with it
- Unsure if democracy can deal with it
- We may not know for some time

# To Paraphrase Betty Davis in “All About Eve”

Fasten your seat belts, it’s gonna be a bumpy generation



# Interesting How Law Has Developed

- For several years I've lectured before this conference and many others
- That courts have been slow to issue decisions
- Until fairly recently, even the courts acknowledged this
- Suddenly there seems to be an abundance of it!!!
- Even significant case law

# No too long ago, the US Supreme Court expressed hesitation

- City of Ontario v Quon, 130 S.Ct. 2619 (2010)
- “The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear... Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior,” at 130 S.Ct. 2629

# The Age of Caution has Clearly Ended

- 2012 – period of most significant decisions?
- Focus on 3
- 2012 Supreme Court GPS decision, US v Jones
- Subsequent 6<sup>th</sup> Circuit GPS decision, US v Skinner
- South Carolina Supreme Court decision, Jennings v Jennings

# Why the GPS Decision?

- US v Jones, 132 S.Ct. 945 (1/23/12)
- Wasn't this a 9-0 decision?
- Sort of
- Yes, they all agreed this was an illegal search under the 4<sup>th</sup> Amendment
- But it's the *WAY* they reached that conclusion that is fascinating
- And may have long-ranging consequences

# We Need to Take a Walk Through Time

- 3 different opinions issued by the Supreme Court justices in Jones
- It's important to appreciate the little nuances of each of the decisions
- And the impact they may have on future events and case decisions
- To do that, you need to understand the different opinions in an historical context

# In the Beginning – Welcome to the 4<sup>th</sup> Amendment

---

The right of the people to be secure in their persons, houses, papers, and *effects*, against *unreasonable* searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the *place to be searched, and the persons or things to be seized.*

# Missing from the 4<sup>th</sup> Amendment

- No mention of privacy in 4<sup>th</sup> Amendment
- No mention of it anywhere in the Constitution
- No mention of communication
- No mention of privacy of communication
- Olmstead v US, 277 US 438 (1928), 4<sup>th</sup> Amendment protects property/persons, not communications
- Vigorous dissent by Justice Louis Brandeis
- Many scholars point to his dissent as the birthplace of America's constitutional "right of privacy"

## Here's Justice Brandeis's dissent

“The protection guaranteed by the Amendments is much broader in scope [than protecting property]. The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness... They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, **the right to be let alone** – the most comprehensive of rights and the right most valued by civilized men. To protect that right, **every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.**”

# Olmstead is overturned

- We move ahead 39 years
- Katz v. US, 389 US 347 (1967)
- Planting a surreptitious listening device to the outside of a public phone booth without a court order IS a violation of the 4<sup>th</sup> Amendment
- Constitutionally protected area now includes, under Katz, **anything or anywhere there is a “reasonable expectation of privacy”**
- Protection no longer limited only to purely physical objects

# “Reasonable expectation of privacy” theory evolves

- Not all places you would think are private are protected under this theory
- So still subject to LE search w/o warrant
- Some are easy to predict
- E.g., anything visible to the public
- E.g., someone standing on the public sidewalk outside the front of your house can look through an uncovered window, Hester v. US, 265 U.S. 57 (1924)

# “Visible to the public” expands

- Okay to enhance the senses
- Binoculars ok, Hodges v US, 243 F.2d 281 (5<sup>th</sup> Cir. 1957)
- Flashlight ok, US v Dunn, 480 U.S. 294 (1987)
- Searchlight ok, US v Lee, 274 U.S. 559 (1927)
- Drug-sniffing dogs ok, US. v. Bronstein, 521 F.2d 459 (2<sup>nd</sup> Cir. 1975), cert den, 424 US 918
- Surveillance cameras looking in public areas ok, US v. McIver, 186 F.3d 1119 (9<sup>th</sup> Cir. 1999), cert den 528 U.S. 1177

# Even what you might think are not so public places

- “Fly over” camera surveillance to get views of the interior of places that are shielded from public view from the street – OK w/o warrant
- Theory – as long as it’s visible while flying over publicly navigable air space, then it’s capable of being recorded w/o warrant
- Over a heavily secured chemical plant, Dow Chemical Co. v. US, 476 U.S. 227 (1986)
- Over a fenced-in residence to find marihuana plants, California v. Ciraolo, 476 U.S. 207 (1986)

# Info given to “3<sup>rd</sup> party” cases

- Theory – no “reasonable expectation of privacy” in anything one gives to another person
- The “other person” can give that item or information to anyone s/he wants
- So no “expectation of privacy”
- See Smith v Maryland, 442 US 735 (1979); US v Miller, 425 US 435 (1976); Couch v US, 409 US 322 (1973); and Hoffa v US, 385 US 293 (1966)
- Even where person giving up the info doesn’t think receiving person will pass it on to 3<sup>rd</sup> party

# Early mechanical tracking cases

- US v Knotts, 460 U.S. 276 (1983)
- Beeper placed by chloroform manufacturer in barrel before delivery to target of investigation
- (Chloroform is used to manufacture illegal drugs)
- Police track defendant's truck carrying barrel
- Police lose track of truck
- Police reacquire beeper after it's already in target's cabin
- Court of Appeals suppressed evidence
- US Supreme Court overturned suppression

# Interesting language from the Court

- A “person traveling in an automobile has no reasonable expectation of privacy in his movements from one place to another,” at US 281
- The temporary loss of visual surveillance, requiring reacquisition via the beeper is of no moment
- “Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancements as science and technology afforded them in this case,” at US 282

# Even more interesting language

- The Court acknowledge that the importance of the beeper's use, "to ascertain the ultimate resting place of the chloroform when they would not have been able to do had they relied solely on their naked eyes," at US 285
- Nevertheless, "scientific enhancement of this sort raises no constitutional issues which visual surveillance would not also raise," at US 285
- Had the police maintained visual surveillance, they would have just as easily seen the truck arrive there

# Next tracking case

- US v. Karo, 468 U.S. 705 (1984)
- Beeper placed in 50-gallon drum of ether (another narcotics manufacturing substance) by the chemical's manufacturer in advance of delivery to target
- Drum moved inside various residence and private storage facilities
- Non-public warrantless surveillance of barrel's movements inside was a 4<sup>th</sup> Amendment violation
- Open to public view/shielded from public view became an easy standard to follow

# Then came GPS tracking

- People v. Weaver, 12 N.Y.3d 433 (2009)
- Bad facts make bad case law
- 65 consecutive days 24-hour warrantless surveillance
- No reason given for surveillance
- 4-3 decision suppresses GPS results
- As a result, Weaver went free
- Majority stated to allow such uninterrupted surveillance to continue was the equivalent of “millions of additional officers and cameras on every street lamp,” at N.Y.3d 441

# Majority's concern

- Unless such warrantless tracking is prohibited, law enforcement can surveil:
- “trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on”
- Surveillance no longer just becomes seeing where a person is at a given time
- It creates a lifestyle timeline

# Vigorous dissent

- Justice Smith attempted to remind the majority of basic rule of constitutional law for nearly a century
- That no person has a reasonable expectation of privacy over anything visible to the public
- “[t]he proposition that some devices are too modern and sophisticated to be used freely in a police investigation is not a defensible rule of constitutional law”

# Federal case follows

- U.S. v. Jones, 132 S.Ct. 945 (2012)
- Facts of case:
- Joint FBI-D.C. Metro Police narcotics investigation
- Jones a target
- LE gets a search warrant to place a GPS device on his Jeep Cherokee
- Installation of device had to be performed within 10 days while vehicle in DC geographical area
- Device installed on 11<sup>th</sup> day in Maryland
- And accessed again in Maryland to change battery

# Results of tracking

- Vehicle's location tracked for 28 consecutive days
- 24 hours a day
- Tracked within 50-100 feet of actual location
- Results forwarded from tracking satellite to government cell phone to government computer
- Tracking device forwarded over 2000 pages of data
- Jones indicted/eventually convicted as part of a narcotics conspiracy partly through use of GPS data
- Had moved to suppress GPS data during trial
- Motion denied at trial
- Reversed during DC Circuit appeal/suppressed

# Supreme Court agrees 9-0 to suppress

- But 3 different opinions
- Although 9-0, it's a fascinating case
- Sotomayor joined Scalia, Roberts, Kennedy and Thomas in majority opinion
- She also writes her own concurrence
- Alito writes separate concurring opinion joined by Ginsburg, Breyer and Kagan
- If you already know how these judges are philosophically aligned
- You can already get a sense how this is going to go

# Majority opinion

- Scalia promotes a traditionalist constitutional view
- “At bottom we must ‘assure preservation of that degree of privacy against government that existed when the 4<sup>th</sup> Amendment was adopted,’ at S.Ct. 950
- What does that mean?
- Look at footnote 8, “Where... the Government obtains information by physically intruding on a constitutionally protected area, such a search [within the original meaning of the amendment] occurred”
- Majority found a **trespassory violation**

# Alito's minority concurrence

- Ridiculed need to return to “18<sup>th</sup> Century tort law”
- “Is it possible to imagine a case in which a constable secreted himself somewhere in a coach and remained there for a period of time in order to monitor the movements of the coach’s owner?” at S.Ct. 958
- And Alito couldn’t stop there, but immediately followed the jibing above with the following footnote
- “The [majority] suggests that something like this might have occurred in 1791, but this would have required either a gigantic coach, a very tiny constable – or both – not to mention a constable with incredible fortitude and patience”

# So what did the minority hold?

- Wants to do away with 18<sup>th</sup> Century interpretation of the Constitution, and, in this case, the 4<sup>th</sup> Amendment
- Seeks full-blown adoption of the “Katz standard”
- All 4<sup>th</sup> Amendment searches should be judged on the modern “reasonable expectation of privacy” standard
- Protection should no longer be tied into invasion of physical space analysis
- Even majority states both theories are appropriate
- Why are the majority and the minority in disagreement in principle when they agree in the result?
- Here’s the rumored reason

# Interesting (or odd?) part of Alito's decision

- Alito acknowledges SOME form of warrantless GPS tracking is OK!
- “relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable,” at S.Ct. 964
- Doesn't know how much – but 28 days too much
- Why go this way?
- My opinion – doesn't want to overturn Knotts
- Scalia calls Alito out on this difficult uncertainty
- My guess – neither side wants black/white solution

# Sotomayer's concurrence

- Agrees there's a trespass violation to join majority
- Also agrees with Katz's "reasonable expectation of privacy" philosophy
- Is concerned about both Scalia's and Alito's analysis
- "In cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion of property, the majority opinion's trespassory test may provide little guidance," at S.Ct. 955
- Seems to question Alito's short-term permissiveness
- "In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the Katz analysis will require particular attention," at S.Ct. 955

# She goes where no one has gone before

- She joins in the Weaver concerns about tracking one's movements everywhere... but...
- “More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties,” at S.Ct. 957
- “This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks,” at S.Ct. 957

# Rocking the very foundations

- “I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year,” at S.Ct. 957
- “[W]hatever the societal expectations, they can attain constitutionally protected status only if our 4<sup>th</sup> Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy”
- “I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to 4<sup>th</sup> Amendment protection”

# US v Skinner, 690 F.3d 772

- August, 2012, 6<sup>th</sup> Circuit decision
- Takes Jones decision one step further
- What if the police did nothing to install the GPS tracking?
- Can they benefit from tracking installed by the manufacturer even without the awareness of the user?
- Here, GPS tracking in “throw-away phones”

# Facts of Case

- International marihuana smuggling gang
- Used “pay-as-you-go phones” in false names to discuss transportation and payment
- Wiretap told DEA when one of the members would be transporting a load
- Court-order authorized activating GPS device on transporter’s phone
- Agents “pinged” deliverer’s phone
- Determined deliverer parked at rest stop on Texas interstate

## Facts of Case – Part 2

- Agents approach mobile home with drug dogs
- Request permission to enter
- Permission denied
- Dogs signal presence of drugs
- Agents enter mobile home
- Discover 1100 pounds marijuana

# Jones Distinguished by 2 Judges

- GPS not installed through LE trespass
- Only 3 day surveillance
- “The law cannot be that a criminal is entitled to rely on the expected untrackability of his tools. Otherwise, dogs could not be used to track a fugitive if the fugitive did not know that the dog hounds had his scent. A getaway car could not be identified and followed based on the license plate number if the driver reasonably thought he had gotten away unseen.”

# Concurring Opinion Disagrees

- 1 judge felt this was a 4<sup>th</sup> Amendment violation
- Should have gotten a search warrant
- Under Katz's "reasonable expectation of privacy"
- But search held valid under good faith exception
- Reason?
- Although called a court order, there was sufficient information in the application to be the equivalent of a search warrant
- Unanimous result
- But not for a unified reason

# Jennings v Jennings, 401 SC 1 (Oct., 2012)

- Husband admits to wife that he has been communicating with his paramour over Yahoo
- Wife gets tech-savvy relative to crack his account
- Husband sues wife, helping relative and wife's private investigator for violating the Electronic Communications Privacy Act for invading his email
- How many think they violated his privacy?
- How many disagree?
- How many are disagreeing because you know I'd only bring this case up because it's an unexpected result?

# Interpretation of ECPA Definitions

- Comes down to the definition of “electronic storage”
- 18 USC 2510 (17)
- (A) any temporary, intermediate storage of a wire or electronic communication incident to the electronic transmission thereof; and
- (B) any storage of such communication service for purposes of backup storage of such communications
- All 5 judges agree (A) not violated
- All 5 judges agree no ECPA violation
- But in 3 different opinions
- Part of the dispute is over the meaning of “and”

# One 2-judge Opinion

- “And” DOESN’T literally mean “and”
- Supported by several prior court decisions
- Judicial interpretation of Congressional intent
- Statute makes no sense if a communication has to satisfy both (A) and (B) of 18 USC 2510 (17) to be considered in “electronic storage”
- So if the communication fits either (A) OR (B), it’s in “electronic storage”
- Husband’s emails don’t satisfy (B) because he never downloaded them and intended Yahoo’s possession to be a backup copy

# Second 2-judge Opinion

- “And” literally means “and”
- The communication must satisfy both (A) and (B)
- This is DOJ’s interpretation
- Once husband looked at the email, it’s no longer in temporary storage awaiting transmission, therefore, no longer in “electronic storage”
- In any event, the husband in leaving the email on Yahoo’s server is not the kind of “backup storage” Congress meant
- Congress meant where Yahoo intended backup, not where the customer intended it

# Remaining 1-judge Opinion

- A combination of the two other decisions
- Agreed with first decision that out of sheer necessity the “and” between (A) and (B) HAS to be “OR”
- Congress never intended backup storage to mean an email user leaving his mail on the ISP’s server
- Congress meant that to mean where Yahoo stores its backup of data

# Take a Step Back

- Wait a minute
- Move back from a purely legal analysis for a moment
- Following someone as they travel around in public places gets Constitutional, 4<sup>th</sup> Amendment protection
- Meanwhile, someone can hack his/her way into your online email account and read your email and the only protection you have available is statutory, not Constitutional, and it doesn't protect you
- Is it just me?
- Or does it seem like something doesn't fit?

*Any Questions?*



# Contact Information

---

**Call or email:**

**Stephen Treglia, Esq.**

**Legal Counsel**

**Recovery Services**

**Absolute Software Corporation**

**877-600-2293 ext 577**

**[streglia@absolute.com](mailto:streglia@absolute.com)**