

Has the Court Moved too far from Reasonableness?

HDSE Summit #9

Keith G. Logan, Kutztown Univ. of PA

- Homeland security is not just about terrorism and counterterrorism.
- It is an amalgam of several distinct yet interrelated areas that include the gathering of intelligence for both law enforcement and national security.
- Of critical concern is the ability of the government to collect data that may, at the time of collection, not necessarily reflect an immediate indication of criminal or terrorist activity.
- But the courts are restricting the gathering of certain intelligence information without a search warrant

- A significant factor in maintaining an effective homeland security program is ensuring the development of intelligence data base.
- A large part of an intelligence program is “collecting” the dots or bits of information, so that, when the time is right, you can “connect” the dots
- Pen Registers
- Surveillance
- Search Incident to Arrest
- “telephony meta data”

- Recent Supreme Court decisions exhibit a new level of restriction on law enforcement investigation and intelligence that may quickly creep into national security to an even greater degree.
- (*Smith v. Maryland*, 442 U.S. 735 (1979)). Both the *Intelligence Reform and Terrorist Prevention Act of 2004* and the *9/11 Commission Report* emphasize the sharing of information, but the government must first have it before it can be shared

Background

- Domestic Intelligence
- MINARET
- SHAMROCK
- COINTELPRO
- Colonial History
 - General Warrants
 - Constitution
 - Bill of Rights
 - Right to Privacy
- Trend Away from Federal Police

Background

- Joe McCarthy-pocket list of communists
- J. Edgar Hoover-from the War Emergency Division to FBI Director-secret files, communist hunter, deporter of aliens, COINTELPRO
- Church Comm., Pike Comm., Rockefeller Commission
- Resignation of a President

Intelligence Gathering and a Reasonable Expectation of Privacy

- Law Enforcement
- National Security
- Constitution-originalist-constructionist
- Privacy: 1,3,4,5,9,14
- Home to a telephone booth
- Smith v. Maryland (1979)-pen register
- Kyllo v. US (2001)-thermal imaging
- Maryland v. King (2013)-DNA

“telephony meta data”

- Pen Register-no privacy with numbers
 - No expectation
 - Smith v. Maryland
- “snowdened”
- NSA
- FISA warrants
- FISC orders under which the telephony metadata program has operated have generally permitted searching the database for a particular number only if it can be demonstrated that there are facts giving rise to a reasonable articulable suspicion (RAS) that the telephone number in question, referred to as the “seed,” is associated with one of the foreign intelligence targets referenced in the court order

Riley v. California & US v. Brima Wurie

- Conflict with Circuit opinions: 1st and 9th
- Wurie: cell phone data resulted in the issuance of a search warrant and the subsequent seizure of a cache of drugs, a gun and cash
- Riley: Police arrested Riley after a lawful stop, subsequent discovery of a firearm under the car's hood, appeals affirmed the warrantless search of his cell phone incident to a lawful arrest; search yielded evidence of gang ties and a shooting, which resulted in his conviction for attempted murder

Riley v. California & US v. Brima Wurie

1. Digital content-no officer safety issue;
2. Digital data loss could be prevented without having to search the device;
3. There is a reduced expectation of privacy incident to an arrest, but that the immense storage capacity of a cell phone is likely to reveal “detained information about all aspects of a person’s life”
4. Following the *AZ v. Gant* (2009) standard-not realistic because of the quantitative and qualitative; and
5. The court should not accept a rule used in the predigital era regarding a search incident to a person’s arrest

United States v. Jones

- “The Government’s attachment of the GPS device to the vehicle, and its use of that device to monitor the vehicle’s movements, constitutes a search under the Fourth Amendment.”
- Found a simple trespass of a car by the government because it failed to get a search warrant to affix the GPS tracking device.
- The car was not in the defendant’s name, when the government affixed a GPS device to the car to track Jones’ movements.
- Harlan’s analysis- concurrence in *Katz* noting that the 4th A protects a person’s “reasonable expectation of privacy”

United States v. Jones

- Court avoided a definitive focus on the government's contention that Jones had no "reason-able expectation of privacy," because Jones's Fourth Amendment rights do not rest with *Katz*.
- Does appear that after Jones, *Katz* may now include a common law trespass test
- Device did no more than actual police surveillance, following the vehicle
- Government argued that Jones could not have a privacy expectation on public roads

United States v. Jones

- J. Sotomayor: device did no more than actual police surveillance, following the vehicle, the government argued that Jones could not have a privacy expectation on public roads
- She wrote that the Government usurped Jones' property for the purpose of conducting surveillance on him, thereby invading privacy interests long afforded, and undoubtedly entitled to, Fourth Amendment protection
- Justice Sotomayor relied on language found in *Kyllo v. U.S.*, relying on a **subjective expectation** of privacy

United States v. Jones

- J. Alito: "Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: 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."
- Alito: Government can store such records and efficiently mine them for information years into the future
- The lengthy monitoring that occurred in this case constituted a search under the Fourth Amendment.

Privacy Expectation?

- Information is being retained on servers, in business records, on unprotected cell phones that can be hacked or stolen, and used for profit in many industries in many markets.
- Some of the information that the court is attempting to protect is already public based on where the event has taken place or the fact that it has already been shared with others.
- None of this even addresses all of the day-to-day hacking that takes place by individuals, companies, and foreign governments. So where does that leave law enforcement?

Court Permitted Search

Incident to an arrest and without the issuance of an additional search warrant, courts have permitted a search of:

1. A defendant, as well as his/her clothing, regardless if it is on their body at the time;
2. The wing or lunge area around a defendant;
3. The passenger compartment of a car and the containers located in the car;
4. Any part of a car if they believe they have probable cause;
5. People who arrested and are recent occupants of a car- then the car is searched (if the arrest has a nexus to the car);
6. Bags or luggage in a person's possession at the time of their arrest;

Court Permitted Search

1. Bags or luggage in a person's possession at the time of their arrest;
2. Any item the suspect gives permission for them to search (consent) or may be in plain view;
3. Open fields;
4. Abandoned property, bags, cigarettes, cups, cans, or cars;
5. Property, such as automobiles that are seized and searched (inventory);
6. Visual searches with binoculars or cameras during a fly-over;
7. Contents of books, wallets and cigarette packs in the defendant's possession; and
8. The usual border and jail searches that can be very "intimate."

Special needs searches

- special needs, beyond the normal need for law enforcement, make the warrant requirement and probable-cause requirement impracticable.”
- suspicionless drug testing of high school students and railroad personnel,
- automobile checkpoints for illegal immigrants (extension of border searches),
- drunk drivers, and the
- search of airplane, subway, and train passengers' carry-on bag

NSA & meta data

- *Klayman v. Obama*, Judge Leon accepted that the plaintiffs had significant privacy interests in the aggregation of their telephone data and that the government's interest in identifying unknown terrorists was of the "highest order"-reversed on appeal
- *United States v. Moalin*, (S.D. Cal. Nov. 18, 2013), Judge Jeffrey Miller reached the opposite conclusion, following *Smith v. Maryland, supra*, and holding that the NSA's collection of a defendant's telephone metadata does not constitute a search because he "had no legitimate expectation of privacy in the telephone numbers dialed"

- With all the material that can be legally secured by the government and in the possession of private industry and hackers, there needs to be a fresh look at the Fourth Amendment, bringing it back to its true meaning.