Privacy and Information Security Law

Randy Canis

CLASS 14 pt. 1

National Security and Foreign Intelligence; Government Records

National Security and Foreign Intelligence

2

Application of Laws

- “Ordinarily, government information gathering activities would fall under the Fourth Amendment rules discussed in the previous chapter on law enforcement, and government electronic surveillance would be regulated by ECPA. However, with national security and foreign intelligence gathering, the Fourth Amendment rules are different, and ECPA often does not apply. Instead, other statutes and regulations apply.”

3

A. THE INTELLIGENCE COMMUNITY

4

Major Intelligence Agencies

- Federal Bureau of Investigation (FBI)
- Central Intelligence Agency (CIA)
- National Security Agency (NSA)
- Plus others…

5

B. THE FOURTH AMENDMENT FRAMEWORK

6

The Keith Case

- 1972 Supreme Court
- Issue
  - Electronic surveillance in internal security matters without prior judicial approval

7

The Keith Case

- "Title III of the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. §§2510-2520, authorizes the **use of electronic surveillance for classes of crimes carefully specified in 18 U.S.C. §2516**. Such surveillance is **subject to prior court order**. Section 2518 sets forth the detailed and particularized application necessary to obtain such an order as well as carefully circumscribed conditions for its use. The Act represents a comprehensive attempt by Congress to promote more effective control of crime while protecting the privacy of individual thought and expression."

8

The Keith Case

- "The Government relies on §2511(3). It argues that 'in **excepting national security surveillances from the Act's warrant requirement Congress recognized the President's authority to conduct such surveillances without prior judicial approval**.' The section thus is viewed as a recognition or affirmance of a constitutional authority in the President to conduct warrantless domestic security surveillance such as that involved in this case. We think the language of §2511(3), as well as the legislative history of the statute, **refutes this interpretation**."

9

The Keith Case

- "We recognize, as we have before, the constitutional basis of the President's domestic security role, but we think it must be **exercised in a manner compatible with the Fourth Amendment**. In this case we hold that this requires an appropriate prior warrant procedure."

10

Keith Case Framework

1) **Criminal investigations** – warrant required
2) **Domestic national security investigations** – warrant required, but standards need not be the same as for criminal
3) **Foreign intelligence gathering** – not addressed

11

C. FOREIGN INTELLIGENCE GATHERING

12

Foreign Intelligence Surveillance Act

- "The Foreign Intelligence Surveillance Act (FISA) of 1978, Pub. L. No. 95511, codified at 50 U.S.C. §§1801-1811, establishes standards and procedures for **use of electronic surveillance to collect 'foreign intelligence' within the United States**. §1804(a)(7)(B). FISA creates a different regime than ECPA, the legal regime that governs electronic surveillance for law enforcement purposes."

13

Applicability of FISA

- "FISA generally applies when **foreign intelligence gathering is 'a significant purpose'** of the investigation. 50 U.S.C. §1804(a)(7)(B) and § 1823(a)(7)(B). The language of 'a significant purpose' comes from the USA PATRIOT Act of 2001. Prior to the USA PATRIOT Act, FISA as interpreted by the courts required that the collection of foreign intelligence be the **primary purpose** for surveillance. After the USA PATRIOT Act, foreign intelligence gathering need no longer be the primary purpose."

14

Foreign Intelligence Surveillance Court (FISC)

- "Requests for FISA orders are reviewed by a special court of federal district court judges. … The proceedings are ex parte, with the Department of Justice (DOJ) making the applications to the court on behalf of the CIA and other agencies. The Court meets in secret, and its proceedings are generally not revealed to the public or to the targets of the surveillance."

15

Court Orders

- "[T]he court must find probable cause that the party to be monitored is a 'foreign power' or 'an agent of a foreign power.' §1801. Therefore, unlike ECPA or the Fourth Amendment, FISA surveillance is not tied to any required showing of a connection to criminal activity. However, if the monitored party is a 'United States person' (a citizen or permanent resident alien), the government must establish probable cause that the party's activities 'may' or 'are about to' involve a criminal violation. §1801(b)(2)(A)."

16

The 9/11 Commission Report

- "It is now clear that everyone involved was confused about the rules governing the sharing and use of information gathered in intelligence channels."
- "The agent concluded that Moussaoui was 'an Islamic extremist preparing for some future act in furtherance of radical fundamentalist goals.' He also believed Moussaoui's plan was related to his flight training."
- "Although the Minneapolis agents wanted to tell the FAA from the beginning about Moussaoui, FBI headquarters instructed Minneapolis that it could not share the more complete report the case agent had prepared for the FAA."

17

Probable Cause Comparison

- "**Title III** allows a court to enter an *ex parte* order authorizing electronic surveillance if it determines on the basis of the facts submitted in the government's application that 'there is **probable cause for belief that an individual is committing, has committed, or is about to commit' a specified predicate offense**. 18 U.S.C. §2518(3)(a). FISA by contrast requires a showing of **probable cause that the target is a foreign power or an agent of a foreign power**. 50 U.S.C. §1805(a)(3)."

18

National Security Letters

- "Provisions in several laws permit the FBI to obtain personal information from third parties merely by making a written request in cases involving national security. No court order is required. These requests are called 'National Security Letters' (NSLs)."

19

NSL for Stored Communications

- "[A]llows the FBI to compel communications companies (ISPs, telephone companies) to release customer records when the FBI makes a particular certification."
- "FBI now needs to certify that the **records are 'relevant to an authorized investigation to protect against terrorism or clandestine intelligence activities**, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States.' 18 U.S.C. §2709."

20

Financial Related

- Similar provisions for the Financial Privacy Act and the Fair Credit Reporting Act

21

Gag Orders

- Stored Communications, Financial Privacy, and Fair Credit Reporting all have gag orders that prevent organizations from telling others that the FBI has sought or obtained information under NSL.

22

D. NSA SURVEILLANCE

23

Clapper v. Amnesty International USA

- 2013 Supreme Court
- Issue
  - Do citizen's have standing to sue that their conversations with non-US persons are likely being acquired?

24

Clapper v. Amnesty International USA

- "In 1978, after years of debate, Congress enacted the Foreign Intelligence Surveillance Act (FISA) to authorize and regulate certain governmental electronic surveillance of communications for foreign intelligence purposes."

25

Clapper v. Amnesty International USA

- "As relevant here, §702 of FISA, 50 U.S.C. §1881a, which was enacted as part of the FISA Amendments Act, supplements pre-existing FISA authority by creating a new framework under which the Government may seek the FISC's authorization of certain foreign intelligence surveillance targeting the communications of non-U.S. persons located abroad. Unlike traditional FISA surveillance, §1881a does not require the Government to demonstrate probable cause that the target of the electronic surveillance is a foreign power or agent of a foreign power. And, unlike traditional FISA, §1881a does not require the Government to specify the nature and location of each of the particular facilities or places at which the electronic surveillance will occur."

26

Clapper v. Amnesty International USA

- "Yet respondents have no actual knowledge of the Government's §1881a targeting practices. Instead, respondents merely speculate and make assumptions about whether their communications with their foreign contacts will be acquired under §1881a. . . . Moreover, because §1881a at most *authorizes*—but does not *mandate* or *direct*—the surveillance that respondents fear, respondents' allegations are necessarily conjectural. Simply put, respondents can only speculate as to how the Attorney General and the Director of National Intelligence will exercise their discretion in determining which communications to target."

27

Clapper v. Amnesty International USA

- Dissent
- "[U]sing the authority of §1881a, the Government can obtain court approval for its surveillance of electronic communications between places within the United States and targets in foreign territories by showing the court (1) that 'a significant purpose of the acquisition is to obtain foreign intelligence information,' and (2) that it will use general targeting and privacy-intrusion minimization procedures of a kind that the court had previously approved. §1881a(g)."

28

Snowden Revelations

- NSA

1) "targeting of non-U.S. persons outside the United States through surveillance occurring in the United States (pursuant to Section 702 of FISA);
2) collecting telephone metadata (pursuant to Section 215 of the Patriot Act);
3) spying on foreign countries and their leadership; and
4) acting to weaken encryption standards."

29

PRISM Targeting

- "PRISM targets Internet communications and stored data of 'non-US persons' outside the United States. In PRISM collection, the government sends a 'selector,' such as an e-mail address, to a U.S.-based electronic service provider, such as an ISP, and the provider shares communications delivered to that 'selector' with the government. PRISM collection does not include telephone calls."

30

Telephone Metadata

- "Leaks by Snowden detailed the **bulk collection of domestic telephony metadata**. Section 215 of the PATRIOT Act allowed for the collection of individual suspects' 'business records.' The NSA broadened the scope of Section 215 to include all call detail records generated by certain telephone companies in the United States. Although technically requiring FISC warrants, telephone companies generally complied voluntarily until news media reported on the practice in 2006. Snowden's disclosures also revealed the existence of FISC orders authorizing this practice."

31

Klayman v. Obama

- 2013 D.D.C.
- Issue
  - "[C]onstitutionality and statutory authorization of certain intelligence-gathering practices by the United States government relating to the wholesale collection of the phone record metadata of all U.S. citizens."

32

Klayman v. Obama

- "According to the news article, this order 'show[ed] . . . that under the Obama administration the communication records of millions of US citizens are being collected indiscriminately and in bulk—regardless of whether they are suspected of any wrongdoing.'"

33

Klayman v. Obama

- "In broad overview, the Government has developed a 'counterterrorism program' under Section 1861 in which it collect, compiles, retains, and analyzes certain telephone records, which it characterizes as 'business records' created by certain telecommunications companies []. … According to the representations made by the Government, the metadata records collected under the program do *not* include *any* information about the content of those calls, or the names, addresses, or financial information of any party to the calls. Through targeted computerized searches of those metadata records, the NSA tries to **discern connections between terrorist organizations and previously unknown terrorist operatives located in the United States**."

34

Klayman v. Obama

- "[T]he Bulk Telephony Metadata Program is meant to detect: (1) domestic U.S. phone numbers calling *outside* of the U.S. to foreign phone numbers associated with terrorist groups; (2) foreign phone numbers associated with terrorist groups calling *into* the U.S. to U.S. phone numbers; and (3) 'possible terrorist-related communications' between U.S. phone numbers *inside* the U.S. …"

35

Klayman v. Obama

- Plaintiff's have standing
- "Thus, whereas the plaintiffs in *Clapper* could only speculate as to whether they would be surveilled at all, plaintiffs in this case can point to strong evidence that, as Verizon customers, their telephony metadata has been collected for the last seven years (and stored for the last five) and will continue to be collected barring judicial or legislative intervention."

36

Klayman v. Obama

- "The threshold issue that I must address . . . is **whether plaintiffs have a reasonable expectation of privacy that is violated** when the Government indiscriminately collects their telephony metadata along with the metadata of hundreds of millions of other citizens without any particularized suspicion of wrongdoing, retains all of that metadata for five years, and then queries, analyzes, and investigates that data without prior judicial approval of the investigative targets. If they do — and a Fourth Amendment search has thus occurred — then the next step of the analysis will be to determine whether such a search is 'reasonable.'"

37

Klayman v. Obama

- "I believe that bulk telephony metadata collection and analysis almost certainly does violate a reasonable expectation of privacy."

38

Klayman v. Obama

- "[I]n light of the significant national security interests at stake in this case and the novelty of the constitutional issues, I will **stay my order pending appeal**. In doing so, I hereby give the Government fair notice that should my ruling be upheld, this order will go into effect forthwith."

39

In re FBI

- "[B]ecause there is **no cognizable Fourth Amendment interest in a telephone company's metadata that it holds in the course of its business**, the Court finds that there is no Constitutional impediment to the requested production. Finding no Constitutional issue, the Court directs its attention to the statute. The Court concludes that there are facts showing reasonable grounds to believe that the records sought are relevant to authorized investigations. This conclusion is supported not only by the plain text and structure of Section 215, but also by the statutory modifications and framework instituted by Congress. Furthermore, the Court finds that this result is strongly supported, if not required, by the doctrine of legislative re-enactment or ratification."

40

Government Records

41

A. PUBLIC ACCESS TO GOVERNMENT RECORDS

42

Court Records

- "For information in **court records**, privacy is protected by way of **protective orders**, which are issued at the discretion of trial court judges. Courts also have the discretion to **seal certain court proceedings** or portions of court proceedings from the public, as well as to permit parties to proceed anonymously under special circumstances.
- Privacy in records maintained by state agencies is protected under each state's freedom of information law."

43

Doe v. Shakur

- 1996 S.D.NY
- Issue
  - "[W]hether the victim of a sexual assault may prosecute a civil suit for damages under a pseudonym"

44

Doe v. Shakur

- "Rule 10(a) of the Federal Rules of Civil Procedure provides that a **complaint shall state the names of all the parties**. The intention of this rule is to apprise parties of who their opponents are and to protect the public's legitimate interest in knowing the facts at issue in court proceedings. Nevertheless, in some circumstances a party **may commence a suit using a fictitious name**."

45

Doe v. Shakur

- "It is **within a court's discretion to allow a plaintiff to proceed anonymously**. [] In exercising its discretion, a court should consider certain factors in determining whether plaintiffs may proceed anonymously. These factors include (1) whether the plaintiff is challenging governmental activity; (2) whether the plaintiff would be required to disclose information of the utmost intimacy; (3) whether the plaintiff would be compelled to admit his or her intention to engage in illegal conduct, thereby risking criminal prosecution; (4) whether the plaintiff would risk suffering injury if identified; and (5) whether the party defending against a suit brought under a pseudonym would be prejudiced."

46

Doe v. Shakur

- "The present case is a difficult one. If the allegations of the complaint are true, plaintiff was the victim of a brutal sexual assault. Quite understandably, she does not want to be publicly identified and she has very legitimate privacy concerns. On balance, however, these concerns are outweighed by [various] considerations."
- "[Plaintiff] contends that disclosure of her name will cause her to be 'publicly humiliated and embarrassed.' Such claims of public humiliation and embarrassment, however, are not sufficient grounds for allowing a plaintiff in a civil suit to proceed anonymously…"

47

Disclosure under FOIA

- Freedom of Information Act
- "OIA grants all persons the **right to inspect and copy records and documents maintained by any federal agency, federal corporation, or federal department**. Certain documents must be disclosed automatically — without anybody explicitly requesting them. FOIA requires disclosure in the Federal Register of descriptions of agency functions, procedures, rules, and policies. 5 U.S.C. §552(a)(1). FOIA also requires that opinions, orders, administrative staff manuals, and other materials be automatically released into the public domain. §552(a)(2)."

48

Obtaining Documents under FOIA

- "To obtain a document under FOIA, a requester must invoke FOIA in the request and follow the 'published rules stating the time, place, fees (if any), and procedures to be followed.' §552(a)(3)(A). The agency must make 'reasonable efforts' to answer any request that 'reasonably describe[s]' the information sought. §§552(a)(3)(A)-(C). A requester can submit a request by mail or through an online form. The agency receiving the request is required to respond to the request within 20 business days unless the agency requests extra time based on 'unusual circumstances.' §552(a)(6)(A). A requester may ask for expedited processing upon a showing of 'compelling need.' §552(a)(6)(E)(i)(I)."

49

FOAI Exemptions and Redaction

- Certain disclosure exemptions apply including materials covered by executive order, internal personnel rules, trade secrets, personnel and medical files, information compiled for law enforcement purposes, and financial institution related information.
- "If a portion of a document that falls under an exemption can be redacted (blacked out), then the remainder of the document must be provided to the requester".

50

Rap Sheets

- Is "the disclosure of the contents of such a file to a third party 'could reasonably be expected to constitute an unwarranted invasion of personal privacy' within the meaning of the Freedom of Information Act (FOIA), 5 U.S.C. §552(b)(7)(C)"?
- "[W]e hold as a categorical matter that a third party's request for law enforcement records or information about a private citizen can reasonably be expected to invade that citizen's privacy, and that when the request seeks no 'official information' about a Government agency, but merely records that the Government happens to be storing, the invasion of privacy is 'unwarranted.' …"

51

Agencies under the FOIA

- Only Agencies
- Not Congress and the President and advisors

52

Death Scene Images

- "[W]e hold that FOIA recognizes surviving family members' right to personal privacy with respect to their close relative's death-scene images. Our holding is consistent with the unanimous view of the Courts of Appeals and other lower courts that have addressed the question."
- "We hold that, where there is a privacy interest protected by Exemption 7(C) and the public interest being asserted is to show that responsible officials acted negligently or otherwise improperly in the performance of their duties, the requester must establish more than a bare suspicion in order to obtain disclosure. Rather, the requester must produce evidence that would warrant a belief by a reasonable person that the alleged Government impropriety might have occurred."

53

Public Access to Judicial Proceedings

- In *Globe Newspaper v. Superior Court*, 457 U.S. 596 (1982), the Supreme Court articulated a test to determine whether the First Amendment requires public access to a proceeding: (1) whether the proceeding "historically has been open to the press and general public" and (2) whether access "plays a particularly significant role in the functioning of the judicial process and the government as a whole." The court in *Globe* concluded that the First Amendment requires public access to criminal trials, and the government can deny access only if "the denial is necessitated by a compelling governmental interest and is narrowly tailored to serve that interest."

54

Availability of Criminal Records

- "There is no violation of the United States Constitution in this case because there is **no constitutional right to privacy in one's criminal record**. Nondisclosure of one's criminal record is not one of those personal rights that is 'fundamental' or 'implicit in the concept of ordered liberty.'"
- Cline v. Rogers, 87 F.3d 176 (6th Cir. 1996)

55

Megan's Laws

- "'Megan's Law,' [] establish[ed] a system for people to learn of the whereabouts of sexual offenders who were released from prison. ...
- In 1996, Congress passed a federal Megan's Law restricting states from receiving federal anti-crime funds unless they agreed to 'release relevant information that is necessary to protect the public' from released sex offenders. [] Today, all 50 states have passed a version of Megan's Law. Sex offender registries under Megan's Law often contain information such as the sex offender's Social Security number, photograph, address, prior convictions, and places of employment. States differ in how they disseminate sexual offender information. … At least 16 states have made their registries available on the Internet."

56

Driver's Privacy Protection Act

- State departments of motor vehicles cannot generally disclose or sell personal information of drivers
- Also applies to anyone who uses data from a motor vehicle record

57

B. GOVERNMENT RECORDS AND USE OF PERSONAL DATA

58

Code of Fair Information Practices

- There must be no personal-data record-keeping systems whose very existence is secret.
- There must be a way for an individual to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.

59

Code of Fair Information Practices

- There must be a way for an individual to correct or amend a record of identifiable information about him.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

60

OECD Guidelines

- "The OECD Guidelines set out eight principles for data protection that are still the benchmark for assessing privacy policy and legislation: Collection Limitation; Data Quality; Purpose Specification; Use Limitation; Security Safeguards; Openness; Individual Participation; and Accountability."

61

The Privacy Act of 1974

- Stated Purposes include:
- "(1) 'permit an individual to determine what records pertaining to him are **collected, maintained, used, or disseminated by [federal] agencies**'; (2) 'permit an individual to prevent records pertaining to him obtained by such agencies **for a particular purpose from being used or made available for another purpose without his consent**'; (3) allow an individual to **access and correct** his personal data maintained by federal agencies; and (4) ensure that information is '**current and accurate** for its intended use, and that adequate safeguards are provided to **prevent misuse** of such information.'"

62

Applicability of the Privacy Act

- Applies to
  - Federal agencies
- Does not apply to:
  - Businesses or private sector organizations
  - State and local agencies
  - Aspects of the federal government that are not agencies

63

Proving Violations of the Privacy Act

1) P "must prove that the agency violated its obligations under the Act"
2) "The information disclosed must be a 'record' contained within a 'system of records.' A 'record' must be identifiable to an individual (contain her name or other identifying information) and must contain information about the individual. §552a(a)(4)."
3) Third, to collect damages, the plaintiff must show that an adverse impact resulted from the Privacy Act violation and that the violation was "willful or intentional."

64

Limits on Privacy Act Disclosure

- 5 U.S. Code § 552a - Records maintained on individuals
- (b) Conditions of Disclosure. — No agency shall disclose any record which is contained in a system of records **by any means of communication to any person, or to another agency**, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, **unless disclosure of the record would be**—

65

Limits on Privacy Act Disclosure

1) to those **officers and employees of the agency** which maintains the record who have a need for the record in the performance of their duties;
2) required under section 552 of this title;
3) for a **routine use** as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section;
4) to the **Bureau of the Census** …;
5) to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record…;
6) to the National Archives and Records Administration as a record which has sufficient historical or other value…;

66

Limits on Privacy Act Disclosure

7) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law…;
8) to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual …;
9) to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof…;
10) to the Comptroller General…;
11) pursuant to the order of a court of competent jurisdiction; or
12) to a consumer reporting agency….

67

"Routine Use" Exception

- "The broadest exception under the Privacy Act is that information may be disclosed for any '**routine use**' if disclosure is **'compatible' with the purpose** for which the agency collected the information. §552a(b)(3)."

68

Pippinger v. Rubin

- 1997 10th Cir.
- Issue
  - Did certain disclosures of information regarding Pippinger's affair violate the Privacy Act?

69

Pippinger v. Rubin

- Pippinger
  - Affair with a married subordinate
  - Suspended without pay
  - Pippinger's supervisor was also having an affair with a subordinate
  - Supervisor brought up Pippinger's affair in trying to protest his demotion
  - ALERTS system had information about Pippinger's affair and discipline

70

Pippinger v. Rubin

- Privacy Act limits agency disclosure of information contained in records
- "Pippinger, who did not consent to any disclosure, claims that the IRS unlawfully disclosed his employment records on three different occasions. In analyzing each of these three claims, we must decide whether a **record was 'disclosed,'** and, if so, whether it was disclosed **pursuant to an exception** enumerated in 5 U.S.C. §552a(b)."

71

Pippinger v. Rubin

- "As the district court correctly noted, the Privacy Act does not prohibit disclosure of information or knowledge obtained from sources other than 'records.' In particular, it does not prevent federal employees or officials from talking—even gossiping—about anything of which they have non-record-based knowledge."

72

"Routine Use" Exception Loophole

- "An agency can establish a 'routine use' if it determines that a disclosure is compatible with the purpose for which the record was collected. This vague formula has not created much of a substantive barrier to external disclosure of personal information…"
- "[M]ore procedural and more symbolic."

73

Actual Damages Required?

- Are actual damages required to obtain the minimum statutory award of 1K? YES
- "The 'entitle[ment] to recovery' necessary to qualify for the $1,000 minimum is not shown merely by an intentional or willful violation of the Act producing some adverse effect. **The statute guarantees $1,000 only to plaintiffs who have suffered some actual damages**."
- Doe v. Chao, 540 U.S. 614 (2004)

74

Emotional Distress Enough?

- "In *Federal Aviation Administration v. Cooper*, 132 S. Ct. 1441 (2012), the U.S. Supreme Court held that **emotional distress alone did not qualify for 'actual damages' under the Privacy Act**."

75

Privacy Act v. FOIA

- "The Privacy Act does not apply to information that must be disclosed pursuant to FOIA. §552a(k)(1). However, if one of FOIA's privacy exceptions applies, then the Privacy Act would require that the government refrain from disclosing certain information."

76

CMPPA

- Computer Matching and Privacy Protection Act (CMPPA)
- "The CMPPA amends the Privacy Act and provides that in order for agencies to disclose records to engage in computer matching programs, they must establish 'a written agreement between the source agency and the recipient agency or non-Federal agency stating' the purpose and legal authority for the program, a justification for the program, a description of the records to be matched, procedures for the accuracy of the information, and prohibitions on redisclosure of the records. §552a(o)(1). These agreements must be available upon request to the public."

77

Data Mining

- "'**Subject-based' data mining** involves searching the data of a specific identified person. It might involve examining whom that person associates and does business with.
- '**Pattern-based' data mining** involves starting with a particular profile for terrorist activity and then analyzing databases to see which individuals' patterns of activity match that profile."

78

Link Analysis

- "This technique uses **aggregated public records** or other large collections of data **to find links** between a subject — a suspect, an address, or other piece of relevant information — and other people, places, or things. This can provide additional clues for analysts and investigators to follow."

79

Reliance on Erroneous Records

- "This case presents the question whether evidence seized in violation of the Fourth Amendment by an officer who acted in reliance on a police record indicating the existence of an outstanding arrest warrant — a record that is later determined to be erroneous — must be suppressed by virtue of the exclusionary rule regardless of the source of the error…"
- ANSWER – NO
- Exclusionary rule not needed for deterrence
- Arizona v. Evans, 514 U.S. 1 (1995)

80

U.S. v. Ellison

- 2006 6th Cir.
- Issue
  - "[W]hether the Fourth Amendment is implicated when a police officer investigates an automobile license plate number using a law enforcement computer database"

81

U.S. v. Ellison

- "'What a person knowingly exposes to the public … is not a subject of Fourth Amendment protection.' It is also settled that 'objects falling in the plain view of an officer who has a right to be in the position to have that view are subject to seizure.' … **No argument can be made that a motorist seeks to keep the information on his license plate private**. The very purpose of a license plate number, like that of a vehicle Identification Number, is to provide identifying information to law enforcement officials and others. . . ."

82

U.S. v. Ellison

- No 4th Amendment search…

83

Crime Scene DNA

- "The fact that a suspect's DNA matches the DNA found at a crime scene does not indicate with certainty that the suspect is likely to be the culprit or even is likely to have been at the crime scene. Statistically, a portion of the population will match the DNA found at a crime scene. **What DNA evidence can determine with near certainty is that certain individuals do not match the DNA at the scene.** In other words, DNA evidence can more accurately exclude individuals as suspects than include them."

84

DNA Profiling

- "Pursuant to the DNA Analysis Backlog Elimination Act of 2000 ('DNA Act'), individuals who have been convicted of certain federal crimes and who are incarcerated, or on parole, probation, or supervised release must provide federal authorities with 'a tissue, fluid, or other bodily sample . . . on which a[n] . . . analysis of the [sample's] deoxyribonucleic acid (DNA) identification information' can be performed. …"
- "[T]he **DNA Act's compulsory profiling** of qualified federal offenders can only be described as **minimally invasive** — both in terms of the bodily intrusion it occasions, and the information it lawfully produces."
- US v. Kincade, 9th Cir. 2004 (en banc)(plurality)

85

DNA Identification of Arrestees

- "[T]he Court concludes that **DNA identification of arrestees is a reasonable search that can be considered part of a routine booking procedure**. When officers make an arrest supported by probable cause to hold for a serious offense and they bring the suspect to the station to be detained in custody, taking and analyzing a cheek swab of the arrestee's DNA is, like fingerprinting and photographing, a legitimate police booking procedure that is **reasonable under the Fourth Amendment**."
- Maryland v. King, 133 S.Ct. 1958 (2013)

86

C. IDENTIFICATION RECORDS AND REQUIREMENTS

87

Identification Required?

- "[S]uch [identification] statutes violate the Fourth Amendment because as a result of the demand for identification, the statutes bootstrap the authority to arrest on less than probable cause and because the serious intrusion on personal security outweighs the mere possibility that identification might provide a link leading to arrest."
- Carey v. Nevada Gaming Control Board, (9th Cir. 2002)

88

Name Disclosure Requirement

- "Asking questions is an essential part of police investigations. In the ordinary course a police officer is free to ask a person for identification without implicating the Fourth Amendment. Beginning with *Terry v. Ohio*, 392 U.S. 1 (1968), the Court has recognized that a law enforcement officer's reasonable suspicion that a person may be involved in criminal activity permits the officer to stop the person for a brief time and take additional steps to investigate further. …**Obtaining a suspect's name in the course of a *Terry* stop serves important government interests**."
- Hiibel v. 6th Judicial District Court, 542 U.S. 177 (2004)

89

Social Security Numbers

- "[G]overnmental use of SSNs is forbidden by Section 7 of the Privacy Act unless an exception applies, but … over the years Congress has made so many exceptions, that the **collection of SSNs in government is quite widespread**. This is the case for two reasons: Congress has passed many mandates of SSN use, and where states or private actors are left to decide whether or not to require the SSN, these entities generally choose to use it…"

90

Program Completed

© 2015-2016 Randy L. Canis

91