Privacy and Information Security Law

Randy Canis

CLASS 7

Privacy and Law Enforcement pt. 2; Education Privacy
Privacy and Law Enforcement pt. 2

D. DIGITAL SEARCHES AND SEIZURES

Computer Searches

- Generic warrants may be upheld when a “more precise description is not possible”
- However, a search for drug files expanded to a search for pornographic files required a second warrant
Copying of Computer Files

- 4th Amendment violation for copying of a computer file?
  - “The agents’ act of copying the data on the Russian computers was not a seizure under the Fourth Amendment because it did not interfere with Defendant’s or anyone else’s possessory interest in the data.”

3rd Party Search Permission?

- Consent to a police search is an exception to the warrant requirement
- “A third party has actual authority to consent to a search ‘if that third party has either (1) mutual use of the property by virtue of joint access, or (2) control for most purposes.’ Even where actual authority is lacking, however, a third party has apparent authority to consent to a search when an officer reasonably, even if erroneously, believes the third party possesses authority to consent.”

Computer Searches at the Border

- Government does not need a warrant or even reasonable suspicion to justify searches of a person or property at an international border
Riley v. California

• Issue
  – Can police search a cell phone seized from an arrested individual without a warrant?

“Where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, . . . reasonableness generally requires the obtaining of a judicial warrant.” … In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement. …”

Riley v. California

• Reasonableness of a warrantless search incident to an arrest
  – “When an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape . . . . In addition, it is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee’s person in order to prevent its concealment or destruction.”
Riley v. California

- Search incident to arrest limited to personal property immediately associated with the arrested person
- Issue of prevention of destruction of evidence v. remote wiping and encryption

Riley v. California

- “Our holding, of course, is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search, even when a cell phone is seized incident to arrest.”
- Other case specific exceptions may apply

Clipper Chip

- Encryption where the US government has a key
- Standard not widely used…
Encryption as Protected Speech

• “[E]ncryption software, in its source code form and as employed by those in the field of cryptography, must be viewed as expressive for First Amendment purposes. …”
• “[T]he Court holds that the regulation of the plaintiff’s diskette is narrowly tailored to the goal of limiting the proliferation of cryptographic products and that the regulation is justified. …”

Video Surveillance

• “[I]f the government intercepts a communication consisting of video images (such as a transmission of a webcam image or an e-mail containing a video clip), then the Wiretap Act applies. If the government accesses an individual’s stored video clip, then the SCA applies. However, being watched by video surveillance (such as a surveillance camera) does not involve an interception or an accessing of stored images. The video surveillance must be silent video surveillance, or else it could be an “oral” communication subject to the Wiretap Act. In sum, silent video surveillance is not covered under federal electronic surveillance law.”

Criminal Enforcement and Email

• “In the criminal law context, the Stored Communications Act requires a warrant to obtain e-mails stored at the ISP for 180 days or less. If the e-mails have been stored over 180 days, then the government can obtain them with a mere subpoena.”
United States v. Warshak

• Issue
  – Suspect ran a business the sold herbal supplement and filed false applications to banks
  – Suspect tried to exclude 27K private emails from his commercial ISP

United States v. Warshak

• Gov’t obtaining content of emails
  – 180 days or less – only with a warrant
  – More than 180 days – warrant, subpoena, or under a court order

United States v. Warshak

• “[W]e hold that a subscriber enjoys a reasonable expectation of privacy in the contents of emails “that are stored with, or sent or received through, a commercial ISP.” The government may not compel a commercial ISP to turn over the contents of a subscriber’s emails without first obtaining a warrant based on probable cause. Therefore, because they did not obtain a warrant, the government agents violated the Fourth Amendment when they obtained the contents of Warshak’s emails. Moreover, to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional. ...”
United States v. Warshak

- Are the emails excluded?
- “Even though the government’s search of Warshak’s emails violated the Fourth Amendment, the emails are not subject to the exclusionary remedy if the officers relied in good faith on the SCA to obtain them.”

Keystroke Logging System

- Keystroke logging does not violate the Wiretap Act because only logged when not connected to the network

United States v. Hambrick

- Issue
  - Defendant seeks to suppress evidence obtained from ISP and from defendant’s home pursuant to a warrant
  - Warrant was invalid; should information that flowed from it be excluded?
United States v. Hambrick

• “The government may require that an ISP provide stored communications and transactional records only if (1) it obtains a warrant issued under the Federal Rules of Criminal Procedure or state equivalent, or (2) it gives prior notice to the online subscriber and then issues a subpoena or receives a court order authorizing disclosure of the information in question. … When an ISP discloses stored communications or transactional records to a government entity without the requisite authority, the aggrieved customer’s sole remedy is damages.”

23

United States v. Hambrick

• “To have any interest in privacy, there must be some exclusion of others. To have a reasonable expectation of privacy under the Supreme Court’s risk-analysis approach to the Fourth Amendment, two conditions must be met: (1) the data must not be knowingly exposed to others, and (2) the Internet service provider’s ability to access the data must not constitute a disclosure.”

24

United States v. Hambrick

• “[T]here is nothing in the record to suggest that there was a restrictive agreement between the defendant and MindSpring that would limit the right of MindSpring to reveal the defendant’s personal information to nongovernmental entities. Where such dissemination of information to nongovernment entities is not prohibited, there can be no reasonable expectation of privacy in that information.”

25
United States v. Hambrick

- “Under the ECPA, Internet Service Providers are civilly liable when they reveal subscriber information or the contents of stored communications to the government without first requiring a warrant, court order, or subpoena.”

Privacy in ISP Records

- “[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” … When defendant entered into an agreement with [his ISP], he knowingly revealed all information connected to [his IP address]. He cannot now claim to have a Fourth Amendment privacy interest in his subscriber information.”

United States v. Forrester

- Issue
  - Court permission to install a pen register against a defendant for surveillance of email and Internet activity
  - Warrant to use imaging and keystroke monitoring
  - Was surveillance a violation of the 4th Amendment?
United States v. Forrester

- "We hold that the surveillance did not constitute a Fourth Amendment search and thus was not unconstitutional. We also hold that whether or not the computer surveillance was covered by the ... pen register statute ... Alba is not entitled to the suppression of any evidence (let alone the reversal of his convictions) as a consequence."

United States v. Forrester

- "[E]-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information. ... [E]-mail to/from addresses and IP addresses are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party's servers."

Education Privacy
A. SCHOOL SEARCHES AND SURVEILLANCE

New Jersey v. T.L.O.

- Issue
  - School caught student smoking in the bathroom
  - School searched the student’s purse and found marijuana and evidence of drug dealing
  - School turns over evidence to police
  - Student confesses
  - Delinquency charges filed against student’s mother

New Jersey v. T.L.O.

- Mother argues search violates 4th amendment and wants all evidence suppressed
- Preliminary issue – Does the 4th Amendment apply to searches conducted by school officials?
  - Answer - Yes
New Jersey v. T.L.O.

• 4th Amendment governs activities of sovereign authorities
  – "We have held the Fourth Amendment applicable to the activities of civil as well as criminal authorities: building inspectors, Occupational Safety and Health Act inspectors, and even firemen entering privately owned premises to battle a fire, are all subject to the restraints imposed by the Fourth Amendment."

New Jersey v. T.L.O.

• "Although the underlying command of the Fourth Amendment is always that searches and seizures be reasonable, what is reasonable depends on the context within which a search takes place. The determination of the standard of reasonableness governing any specific class of searches requires 'balancing the need to search against the invasion which the search entails.' On one side of the balance are arrayed the individual's legitimate expectations of privacy and personal security; on the other, the government's need for effective methods to deal with breaches of public order."

New Jersey v. T.L.O.

• "We have also recognized that searches of closed items of personal luggage are intrusions on protected privacy interests, for 'the Fourth Amendment provides protection to the owner of every container that conceals its contents from plain view.' A search of a child's person or of a closed purse or other bag carried on her person, no less than a similar search carried out on an adult, is undoubtedly a severe violation of subjective expectations of privacy."
New Jersey v. T.L.O.

• “[S]choolchildren may find it necessary to carry with them a variety of legitimate, noncontraband items, and there is no reason to conclude that they have necessarily waived all rights to privacy in such items merely by bringing them onto school grounds.”

New Jersey v. T.L.O.

• “[S]chool officials need not obtain a warrant before searching a student who is under their authority. … [T]he legality of a search of a student should depend simply on the reasonableness, under all the circumstances, of the search. Determining the reasonableness of any search involves a twofold inquiry: first, one must consider whether the . . . action was justified at its inception; second, one must determine whether the search as actually conducted was reasonably related in scope to the circumstances which justified the interference in the first place.”

Strip Searching

• Student suspected of having contraband was made to pull out bra and underwear
• Search violated 4th amendment
• “[B]arring clear and direct evidence that a student is hiding contraband in her undergarments or barring any need to search to promote immediate safety, a strip search is improper.”
B. DRUG TESTING

Student Athletes

• “Somewhat like adults who choose to participate in a "closely regulated industry," students who voluntarily participate in school athletics have reason to expect intrusions upon normal rights and privileges, including privacy. …”


Board of Education v. Earls

• Issue
  – All middle and high school students consent to drug testing to participate in any extracurricular activity
  – Before, random, and upon suspicion
  – "The urinalysis tests are designed to detect only the use of illegal drugs, including amphetamines, marijuana, cocaine, opiates, and barbiturates, not medical conditions or the presence of authorized prescription medications..."
Board of Education v. Earls

• "In Vernonia, this Court held that the suspicionless drug testing of athletes was constitutional. The Court, however, did not simply authorize all school drug testing, but rather conducted a fact-specific balancing of the intrusion on the children’s Fourth Amendment rights against the promotion of legitimate governmental interests. Applying the principles of Vernonia to the somewhat different facts of this case, we conclude that Tecumseh’s Policy is also constitutional…"
The Family Education Rights and Privacy Act

- “The Family Educational Rights and Privacy Act … generally prohibits schools from releasing student ‘education records’ without the authorization of the student and/or parent. Schools may release such ‘directory information’ as names, addresses, dates of attendance, degrees earned, and activities unless the student and/or parent expressly indicates in writing that he or she wants it to remain confidential.”

What are Education Records?

- Directly related to a student and maintained by an education agency/institution
- Does not cover information per se

Whose Right?

- Right belongs to parent until the student is 18 and then the right belongs to the student
- In college, the right always belongs to the student
What Rights?

1) to review the student’s education records;
2) to correct any inaccuracies or misleading information in those records;
3) to control certain disclosures of the information in those records;
4) to file a complaint with the U.S. Department of Education in the event of a violation of the above rights.

Program Completed

All course materials - Copyright 2015 Randy L. Canis, Esq.