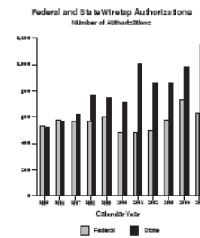


Electronic Surveillance Law, part 2

1



2

- Brad runs a bookstore, and on the side, offers email accounts to his customers. Sensing an opportunity for competitive advantage, Brad scans all the email for messages from “amazon.com” and copies them to his own account.
- Has Brad violated the Wiretap Act?

3

- Konop operates a website for which he gives passwords to Hawaiian Airlines pilots, but not to HA management. VP Davis gets pilots' passwords and accesses the website. Has he violated the SCA?

4

Procedural requirements on law enforcement

- Wiretap
 - “super warrant,” probable cause +
 - “full and complete statement of the facts and circumstances relied on,” and why less intrusive means failed or would fail
 - minimization
 - felony
 - authorization of high-level prosecutor
 - 30-day authorization, post-tap disclosure

5

Procedural requirements on law enforcement

- Stored communications (180 days or less)
 - Warrant, probable cause
- Stored communications (older than 180 days)
 - Notification to subscriber or warrant
- Re-stored communications?

6

Procedural requirements on law enforcement

- Pen Trap/Trace
 - Court order (probable cause -) or warrant
 - If government certifies that "information likely to be obtained by such installation and use is *relevant* to an ongoing investigation"
 - court "*shall* authorize installation and use of a pen register or a trap and trace device"

7

Procedural requirements on law enforcement

- Subscriber information
 - "a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)"
 - Court order (probable cause -), warrant, or consent

8

Alternatives

- Does the Fourth Amendment ever protect electronic communications from government access?
- Should it?

9

Wire and Electronic Communications

What/when	In-flight interception	In "electronic storage" (temporary and intermediate, incidental to delivery)	In remote storage
Oral and wire communications, contents			
Electronic communications, contents			
Dialing, routing, addressing, or signaling information, envelope			

10

Wire and Electronic Communications

	In-flight interception	In "electronic storage" (temporary and intermediate, incidental to delivery)	In remote storage
Oral and wire communications, contents	"wiretap": requires super-warrant, Exclusionary rule		
Electronic communications, contents	Requires super-warrant		
Dialing, routing, addressing, or signaling information, envelope			

11

Wire and Electronic Communications

	In-flight interception	In "electronic storage" (temporary and intermediate, incidental to delivery)	In remote storage
Oral and wire communications, contents	"wiretap": requires super-warrant, Exclusionary rule		
Electronic communications, contents	Requires super-warrant		
Dialing, routing, addressing, or signaling information, envelope	Requires court order (court shall grant on certification of relevance)		

12

Wire and Electronic Communications

	In-flight interception	In "electronic storage" (temporary and intermediate, incidental to delivery)	In remote storage
Oral and wire communications, contents	"wiretap" requires super-warrant, Exclusionary rule	Requires warrant (post-PATRIOT)	
Electronic communications, contents	Requires super-warrant	Requires warrant	
Dialing, routing, addressing, or signaling information, envelope	Requires court order (court shall grant on certification of relevance)		

13

Wire and Electronic Communications

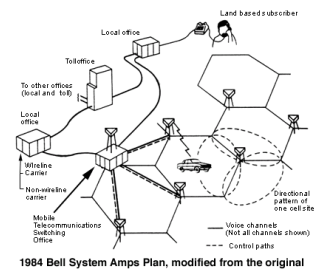
	In-flight interception	In "electronic storage" (temporary and intermediate, incidental to delivery)	In remote storage
Oral and wire communications, contents	"wiretap" requires super-warrant, Exclusionary rule	Requires warrant (post-PATRIOT)	Requires subpoena with notice to subscriber
Electronic communications, contents	Requires super-warrant	Requires warrant	Requires subpoena with notice to subscriber
Dialing, routing, addressing, or signaling information, envelope, Subscriber records	Requires court order (court shall grant on certification of relevance)	Requires court order (court shall grant on certification of relevance)	Requires court order, including on relevance to authorized investigation to protect against international terrorism or clandestine intelligence activities

14

Wire and Electronic Communications

What/when	In-flight interception	In "electronic storage" (temporary and intermediate, incidental to delivery)	In remote storage
Oral and wire communications, contents	"wiretap" requires super-warrant, Exclusionary rule	Requires warrant (post-PATRIOT)	Requires subpoena with notice to subscriber
Electronic communications, contents	Requires super-warrant	Requires warrant	Requires subpoena with notice to subscriber
Dialing, routing, addressing, or signaling information, envelope	Requires court order (court shall grant on certification of relevance)		
Tracking device?			

15



17

CALEA

- Communications Assistance to Law Enforcement Act, 1994
- Telecommunications carriers must "facilitat[e] authorized communications interceptions and access to call-identifying information."
 - Telecommunications carriers include those that are "replacement for a substantial portion of the local telephone exchange service."

18

FISA

- Foreign Intelligence Surveillance Act, 1978
- Authorizes searches of parties who are "foreign powers" or "agents of a foreign power"
 - Upon showing of probable cause that the person to be searched is a foreign power and a significant purpose of the investigation is to gather "foreign intelligence information"
 - Reviewed *ex parte* by FISC court

19

50 U.S.C. Sec. 1801

- e) "Foreign intelligence information" means—
 - (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—
 - (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
 - (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
 - (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
 - (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—
 - (A) the national defense or the security of the United States; or
 - (B) the conduct of the foreign affairs of the United States.

20

- (h) "Minimization procedures", with respect to electronic surveillance, means—
 - (1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;
 - (2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;
 - (3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and
 - (4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 1802 (a) of this title, procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

21