Privacy and Information Security Law

Randy Canis

CLASS 9

Privacy and Law Enforcement pt. 2;
Consumer Data pt. 2

Privacy and Law Enforcement pt. 2

2

D. DIGITAL SERARCHES AND SEIZURES

3

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

4

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."

5

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."

6

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

7

Riley v. California

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

8

Riley v. California

- "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. …"

9

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.** …"

10

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

11

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

12

Clipper Chip

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

13

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. …"

14

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."

15

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."

16

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

17

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

18

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. …"

19

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."

20

Keystroke Logging System

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

21

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?

22

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**."

26

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**."

27

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?

28

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."

29

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."

30

US v. Caira

- 7th Cir. 2016
- Background
  - Email address used to buy chemical that can be used to make ecstasy
  - Subpoena sent to Microsoft for information including account login histories (IP Login history)
  - Subpoena sent to Comcast associated with a frequently used IP address

31

US v. Caira

- "Comcast responded that the address was assigned to Anna Caira, and Comcast gave the DEA Anna's home address. The investigation continued from there and culminated in Anna's husband, Frank Caira, being charged with possessing and conspiring to manufacture illegal drugs, in violation of 21 U.S.C. sections 841(a)(1) and 846."

32

US v. Caira

- "Caira moved to suppress evidence obtained through the subpoenas, arguing that the government's inquiry was a 'search' under the Fourth Amendment, and that a warrant was required."

33

US v. Caira

- "Under the Fourth Amendment, a '**search**' occurs when 'the **government violates a subjective expectation of privacy that society recognizes as reasonable**.' .. Caira argues that I.P. addresses reveal information about a computer user's physical location, and people have both a subjective and objectively reasonable expectation of privacy in their physical location."

34

US v. Caira

- "In what has come to be known as the 'third-party doctrine,' the [Supreme] Court held that 'a person has **no legitimate expectation of privacy in information he voluntarily turns over to third parties** … even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.'"

35

US v. Caira

- "Here, Caira shared his I.P. address with a third party—Microsoft. When he used his home computer and sent his username and password to Microsoft, he expected to see his Hotmail inbox displayed on his home computer screen. It would have done him no good if his inbox was instead displayed on the screen attached to his computer at work, or a computer at the public library, or the computer he used years earlier when first signing up for a Hotmail account. So every time he logged in, he sent Microsoft his I.P. address, specifically so that Microsoft could send back information to be displayed where Caira was physically present."

36

US v. Caira

- So
  - IP address released to third party when accessing the internet
  - No reasonable expectation of privacy in the release of such information

37

In re Microsoft Email Search

- 2nd Cir. 2016
- Warrant applicability under Stored Communications Act (SCA) to product contents under an email account

38

In re Microsoft Email Search

- "Microsoft produced its customer's non-content information to the government, as directed. That data was stored in the United States. But Microsoft ascertained that, to comply fully with the Warrant, it would need to access customer content that it stores and maintains in Ireland and to import that data into the United States for delivery to federal authorities. It declined to do so. Instead, it moved to quash the Warrant."

39

In re Microsoft Email Search

- "When, in 1986, Congress passed the Stored Communications Act as part of the broader Electronic Communications Privacy Act, its aim was to protect user privacy in the context of new technology that required a user's interaction with a service provider. Neither explicitly nor implicitly does the statute envision the application of its warrant provisions overseas. … Rather, in keeping with the pressing needs of the day, Congress focused on providing basic safeguards for the privacy of domestic users."

40

In re Microsoft Email Search

- "[T]he [Stored Communications] Act imposes general obligations of non-disclosure on service providers and creates several exceptions to those obligations. Thus, its initial provision, §2701, prohibits unauthorized third parties from, among other things, **obtaining or altering electronic communications stored by an ECS**, and imposes criminal penalties for its violation. Section 2702 restricts the circumstances in which service providers may **disclose information associated with and contents of stored communications** to listed exceptions, such as with the consent of the originator or upon notice to the intended recipient, or pursuant to §2703. Section 2703 then establishes **conditions under which the government may require a service provider to disclose the contents of stored communications** and related obligations to notify a customer whose material has been accessed. Section 2707 authorizes **civil actions** by entities aggrieved by violations of the Act, and makes 'good faith reliance' on a court warrant or order 'a complete defense.' 18 U.S.C. §2707(e)"

41

In re Microsoft Email Search

- "We conclude that §2703 of the Stored Communications Act does not authorize courts to issue and enforce against U.S.-based service providers warrants for the seizure of customer e-mail content that is stored exclusively on foreign servers."

42

Consumer Data pt. 2

43

F. STATUTORY REGULATION

44

Basic Areas of Federal Legislation

1) Entertainment records
2) Internet use and communications
3) Marketing

45

Video Privacy Protection Act (VPPA)

- 18 U.S. Code § 2710 - Wrongful disclosure of video tape rental or sale records

46

Type of Information Covered

- (a)(3) the term "**personally identifiable information**" includes information which **identifies a person as having requested or obtained specific video materials** or services from a video tape service provider; and

47

Video Tape Service Provider

- (a)(4) the term "**video tape service provider**" means any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of **prerecorded video cassette tapes or similar audio visual materials**, or any person or other entity to whom a disclosure is made under subparagraph (D) or (E) of subsection (b)(2), but only with respect to the information contained in the disclosure.

48

Disclosure Liability

- (b)(1) A video tape service provider who knowingly discloses, to any person, **personally identifiable information concerning any consumer** of such provider shall be liable to the aggrieved person for the relief provided in subsection (d).

49

Written Consent Required for Disclosure

- (b)(2) A video tape service provider may disclose personally identifiable information concerning any consumer— …(B) to any person with the informed, written consent (including through an electronic means using the Internet) of the consumer that—
- (i) is in a form **distinct and separate from any form** setting forth other legal or financial obligations of the consumer;
- (ii) at the election of the consumer— (I) is **given at the time the disclosure is sought**; or (II) is **given in advance** for a set period of time, not to exceed **2 years** or until consent is withdrawn by the consumer, whichever is sooner; and
- (iii) the video tape service provider has provided **an opportunity**, in a clear and conspicuous manner, **for the consumer to withdraw** on a case-by-case basis or to withdraw from ongoing disclosures, at the consumer's election;

50

Enforcement

(c) Civil Action.—

1)Any person aggrieved by any act of a person in violation of this section may bring a civil action in a United States district court.

2)The court may award— (A) **actual damages** but not less than liquidated damages in an amount of **$2,500**; (B) **punitive damages**; (C) **reasonable attorneys' fees** and other litigation costs reasonably incurred; and (D) such other preliminary and **equitable relief** as the court determines to be appropriate.

3)No action may be brought under this subsection unless such action is begun **within 2 years** from the date of the act complained of or the date of discovery.

4)No liability shall result from lawful disclosure permitted by this section.

51

Unique Anonymized IDs

- "[T]he statute, the legislative history, and the case law do not require a name, instead **require the identification of a specific person tied to a specific transaction**, and support the conclusion that a **unique anonymized ID alone is not PII** but context could render it not anonymous and the equivalent of the identification of a specific person. …"
- In re Hulu Privacy Litigation

52

Cable Communications Policy Act (CCPA)

- Applies to cable operators and service providers

53

Notice

- (a) **Notice to subscriber regarding personally identifiable information; definitions** (1) At the time of entering into an agreement to provide any cable service or other service to a subscriber and at least once a year thereafter, a cable operator shall provide notice in the form of a separate, written statement to such subscriber which clearly and conspicuously informs the subscriber of—
- (A) the **nature of personally identifiable information collected** or to be collected with respect to the subscriber and the **nature of the use** of such information;

54

Notice

- (B) the **nature, frequency, and purpose of any disclosure** which may be made of such information, including an identification of the types of persons to whom the disclosure may be made;
- (C) the **period** during which such information will be **maintained** by the cable operator;
- (D) **the times and place at which the subscriber may have access** to such information in accordance with subsection (d) of this section; and
- (E) the **limitations** provided by this section with respect to the collection and disclosure of information by a cable operator and the right of the subscriber under subsections (f) and (h) of this section to enforce such limitations.

55

Written Consent

- (b) **Collection of personally identifiable information using cable system**
- (1) Except as provided in paragraph (2), a cable operator shall **not use the cable system to collect personally identifiable information** concerning any subscriber **without the prior written or electronic consent of the subscriber concerned**.
- (2) A cable operator may use the cable system to collect such information in order to— (A) obtain information necessary to **render a cable service** or other service provided by the cable operator to the subscriber; or (B) detect unauthorized reception of cable communications.

56

Enforcement

- (f) **Civil action in United States district court; damages; attorney's fees and costs; nonexclusive nature of remedy**
- (1) Any person aggrieved by any act of a cable operator in violation of this section may bring a civil action in a United States district court.
- (2) The court may award— (A) **actual damages** but not less than liquidated damages computed at the rate of **$100 a day for each day of violation or $1,000**, whichever is higher; (B) **punitive damages**; and (C) reasonable **attorneys' fees** and other litigation costs reasonably incurred.
- (3) The remedy provided by this section shall be in addition to any other lawful remedy available to a cable subscriber.

57

Cable Providers as ISPs

- "[T]he Court should consider the requirements of the Cable Privacy Act, 47 U.S.C. §551 . The Act generally **prohibits cable operators from disclosing personally identifiable information regarding subscribers without the prior written or electronic consent of the subscriber**. 47 U.S.C. §551(c)(1). A cable operator, however, may disclose such information if the disclosure is made **pursuant to a court order** and the cable operator provides the subscriber with notice of the order. 47 U.S.C. §551(c)(2)(B**). The ISP that Plaintiff intends to subpoena in this case appears to be a cable operator within the meaning of the Act. Providing notice and an opportunity to file a Motion to Quash/Modify** gives the ISP and Defendant an opportunity assert any applicable privilege prior to the information being provided to Plaintiff."
- Rotten Records, Inc. v. John Doe, (W.D.PA 2015)

58

COPPA

- Children's Online Privacy Protection Act of 1998 (COPPA)
- Children's Online Privacy Protection Rule of 2013
- 15 U.S.C. §§6501-6506

59

COPPA Violations

- §6502(a) Acts prohibited (1) In general
- It is unlawful for an operator of a website or **online service directed to children**, or any operator that has **actual knowledge** that it is collecting personal information from a child, **to collect personal information from a child in a manner that violates the regulations** prescribed under subsection (b) of this section.

60

Children under COPPA

- A child under COPPA is a person under the age of 13
  - COPPA is not applicable to children over the age of 13

61

Do You Collect Personal Information from a Child?

- Website is directed to a Child and you collect PI from them (or let others collect PI from them)
- Website is directed to a general audience, but you have actual knowledge you collect PI from Children
- Ad network or plugin and you have actual knowledge you collect PI from Children

62

Personal Information

- What PI fall under COPPA?
  - Full name
  - Home or physical address
  - Online contact information including email address
  - Screen or user name
  - Telephone number
  - Social security number
  - Persistent identifiers including cookies and IP address
  - Phots and videos containing a child's image or voice

63

Must Post a COPPA compliant Privacy Policy

- Link privacy policy on homepage
- Include
  - List of all operators collecting PI
  - Description of the PI collected and how its used
  - Description of parental rights

64

Parental Involvement

- Notify parents directly before collecting PI from their kids
- Obtain parental verifiable consent before collecting PI from their kids
- Honor parents ongoing rights by
  - Allow parents to review collected PI
  - Provide a manner to revoke consent
  - Allow for a requested deletion of child's PI

65

Electronic Communications Privacy Act (ECPA)

1) Wiretap Act
2) Stored Communications Act (SCA)
3) Pen Register Act

Remember?

66

In re Google, Inc. Gmail Litigation

- Issue
  - Does Gmail violate state and federal law?

67

In re Google, Inc. Gmail Litigation

- "[The] Terms of Service reference Google's Privacy Policies … [and] stated that Google could collect information that users provided to Google, cookies, log information, user communications to Google, information that users provide to affiliated sites, and the links that a user follows. The Policies listed Google's provision of 'services to users, including the **display of customized content and advertising'** as one of the reasons for the collection of this information.

68

In re Google, Inc. Gmail Litigation

- "Plaintiffs who are not Gmail or Google Apps **users are not subject to any of Google's express agreements**. Because non-Gmail users exchange emails with Gmail users, however, their communications are nevertheless **subject to the alleged interceptions** at issue in this case."

69

In re Google, Inc. Gmail Litigation

- "[T]he Wiretap Act provides a **private right of action** against any person who '**intentionally intercepts**, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any **wire, oral, or electronic communication**.' 18 U.S.C. §2511(1)(a); *see id.* § 2520 (providing a private right of action for violations of §2511). The Act further defines 'intercept' as 'the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.'"

70

In re Google, Inc. Gmail Litigation

- "Plaintiffs contend that Google violated the Wiretap Act in its operation of the Gmail system by intentionally intercepting the content of emails that were in transit to create profiles of Gmail users and to provide targeted advertising."

71

In re Google, Inc. Gmail Litigation

- Defense #1 – "Ordinary Course of Business" Exception
- Exception is narrow…

72

In re Google, Inc. Gmail Litigation

- "The exception offers protection from liability **only where an electronic communication service provider's interception facilitates the transmission of the communication at issue** or is incidental to the transmission of such communication. Specifically, the exception would apply here only if the alleged interceptions were an instrumental part of the transmission of email."

73

In re Google, Inc. Gmail Litigation

- Defense #2 – Consent
- "The Court rejects Google's contentions with respect to both explicit and implied consent. Rather, the Court finds that it **cannot conclude that any party— Gmail users or non-Gmail users—has consented** to Google's reading of email for the purposes of creating user profiles or providing targeted advertising."

74

Computer Fraud and Abuse Act (CFAA)

- Crimes under the CFAA:
  - Knowingly commit espionage by accessing information without authorization or exceeding authorized access;
  - Access other information without authorization or exceeding authorized access;
  - Access any nonpublic government computer;
  - Access any computer with an intent to commit fraud;
  - Knowingly or intentionally damage a computer;
  - Knowingly traffic in passwords;
  - Threaten to cause damage to a computer with the intent to extort money or other things of value

75

CFAA Penalties

- Obtaining National Security Information Section (a)(1) →10 years
- Accessing a Computer and Obtaining Information Section (a)(2) → 1 or 5 years
- Trespassing in a Government Computer Section (a)(3) → 1 year
- Accessing a Computer to Defraud & Obtain Value Section (a)(4) → 5 years
- Intentionally Damaging by Knowing Transmission Section (a)(5)(A) → 1 or 10 years

76

CFAA Penalties

- Recklessly Damaging by Intentional Access Section (a)(5)(B) → 1 or 5 years
- Negligently Causing Damage & Loss by Intentional Access Section (a)(5)(C) → 1 year
- Trafficking in Passwords Section (a)(6) → 1 year
- Extortion Involving Computers Section (a)(7) → 5 years

77

Protected Computer

- Section 1030(e)(2) defines **protected computer** as:
  a computer—
  (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
  (B) which is used in or affecting interstate or foreign commerce or communication . . . .

78

Insiders v. Outsiders

- Insiders – exceed authorized access
- Outsiders – without authorization

79

Exceeds Authorized Access

- The term "**exceeds authorized access**" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."
- Without authorization is not defined…

80

Exceeds Authorized Access

- "It is relatively easy to prove that a defendant had only limited authority to access a computer in cases where the defendant's access was limited by restrictions that were memorialized in writing, such as terms of service, a computer access policy, a website notice, or an employment agreement or similar contract."

81

Obtaining National Security Information

1030(a)(1) Summary (Felony)

1. Knowingly access computer without or in excess of authorization
2. obtain national security information
3. reason to believe the information could injure the U.S. or benefit a foreign nation
4. willful communication, delivery, transmission (or attempt) *OR* willful retention of the information

82

Accessing a Computer and Obtaining Information

1030(a)(2) Summary (Misd.)

1. Intentionally access a computer
2. without or in excess of authorization
3. obtain information
4. from financial records of financial institution or consumer reporting agency *OR* the U.S. government *OR* a protected computer

83

Accessing a Computer and Obtaining Information

(Felony)

5. committed for commercial advantage or private financial gain *OR* committed in furtherance of any criminal or tortious act *OR* the value of the information obtained exceeds $5,000

84

Trespassing in a Government Computer

1030(a)(3) Summary (Misd.)

1. Intentionally access
2. without authorization
3. a nonpublic computer of the U.S. that was exclusively for the use of U.S. or was used by or for U.S.
4. affected U.S. use of computer

85

Accessing to Defraud and Obtain Value

1030(a)(4) Summary (Felony)

1. Knowingly access a protected computer without or in excess of authorization
2. with intent to defraud
3. access furthered the intended fraud
4. obtained anything of value, including use if value exceeded $5000

86

Damaging a Computer or Information

Summary of (a)(5)(A)

1. Knowingly cause transmission of a program, information, code, or command
2. intentionally cause damage to protected computer without authorization

87

Damaging a Computer or Information

Summary of (a)(5)(B)

1. Intentionally access a protected computer without authorization
2. recklessly cause damage

88

Damaging a Computer or Information

Summary of (a)(5)(C)

1. Intentionally access a protected computer without authorization
2. cause damage
3. cause loss

89

Felony

3. resulting in loss of $5,000 during 1 year *OR* modifies medical care of a person *OR* causes physical injury *OR* threatens public health or safety *OR* damages systems used by or for government entity for administration of justice, national defense, or national security *OR* damages affect 10 or more protected computers during 1 year

90

Trafficking in Passwords

1030(a)(6) Summary (Misd.)

1. Trafficking
2. in computer password or similar information
3. knowingly and with intent to defraud
4. trafficking affects interstate or foreign commerce *OR* computer used by or for U.S.

91

Threatening to Damage a Computer

1030(a)(7) Summary (Felony)

1. With intent to extort money or any other thing of value
2. transmits in interstate or foreign commerce a communication
3. containing a: threat to damage a protected computer *OR* threat to obtain or reveal confidential information without or in excess of authorization *OR* demand or request for money or value in relation to damage done in connection with the extortion.

92

Consumer Data pt. 2

93

Spam

- How does the CAN-SPAM Act work?
- FTC Summary
  - http://www.business.ftc.gov/documents/bus61-can-spam-act-compliance-guide-business

94

CAN SPAM Act

- Prohibits sending deceptive or misleading information and using deceptive subject headings
- Requires inclusion of return addresses in email messages, and
- Prohibits sending emails to a recipient after that recipient has indicated he or she does not wish to receive email messages from the sender

95

CAN SPAM Act

- Who is subject to the law?
  - Mail service senders
  - Persons provided content to be sent to mail service providers
  - Persons performing their own mailings
  - More than one person can be subject to the law for the sending of a particular email

96

Commercial Mail Messages

- Is the message a commercial electronic mail message?
  - A ‘‘commercial electronic mail message’’ is any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose).
  - Does not include transactional or relationship messages

97

Transactional/Relationship Qualifications

- Is the message a transactional or relationship message?
  - The primary purpose of the e-mail must meet a defined category
  - Effectuate a transaction, product/service related information for the already purchased product/service, notification of changes, account information (on a regular basis), employment relationship/benefit information, or deliver agreed upon goods/services

98

Transactional/Relationship Qualifications

(i) to facilitate, complete, or confirm a commercial transaction that the recipient has previously agreed to enter into with the sender;

(ii) to provide warranty information, product recall information, or safety or security information with respect to a commercial product or service used or purchased by the recipient;

99

Transactional/Relationship Qualifications

(iii) to provide—

(I) notification concerning a change in the terms or features of;

(II) notification of a change in the recipient's standing or status with respect to; or

(III) at regular periodic intervals, account balance information or other type of account statement with respect to,

a subscription, membership, account, loan, or comparable ongoing commercial relationship involving the ongoing purchase or use by the recipient of products or services offered by the sender;

100

Transactional/Relationship Qualifications

(iv) to provide information directly related to an employment relationship or related benefit plan in which the recipient is currently involved, participating, or enrolled; or

(v) to deliver goods or services, including product updates or upgrades, that the recipient is entitled to receive under the terms of a transaction that the recipient has previously agreed to enter into with the sender.

101

Transactional or Relationship?

- If you don't fit in the bucket of being a transactional or relationship message,
  - Either your message is a commercial electronic mail message and you have the associated enhanced obligations, or
  - Your message does not fall within the purview of the CAN SPAM Act.

102

False or misleading header information

- For commercial electronic mail, transactional, and relationship mail messages
- When email address or domain name is obtained under false pretenses
- When origin of message is disguised due to relay
- Not when from line accurately identifies who initiated the message

103

Deceptive Subject Heading

- Applies only to commercial electronic mail messages
- Cannot have a subject line that would be likely to mislead the recipient about a material fact about the contents or subject matter of the message

104

Return Email Address

- Applies only to commercial electronic mail messages
- Must have a functioning return email address that works for 30 days after transmission
- Alternatively, the message can provide another Internet mechanism to enable opt-out
  - Can provide a menu of options, so long as menu enables opt out of all commercial electronic mail messages from the sender
- Must remove person within 10 business days

105

Opt Out and Physical Address

- Applies only to commercial electronic mail messages
- Message must have

  (i) clear and conspicuous identification that the message is an advertisement or solicitation;

  (ii) clear and conspicuous notice of the opportunity

  to decline to receive further commercial electronic mail messages from the sender; and

  (iii) a valid physical postal address of the sender.

106

CAN SPAM Rule

- The rule "defines the relevant criteria to determine the primary purpose of an electronic mail message. [The] provisions [of this rule] describe types of electronic mail messages that contain commercial content or what the Act terms 'transactional or relationship' content, and establish different criteria for each type."

107

Primary Purpose

- Commercial when
  - Content is exclusively commercial
  - If content is both commercial and transactional/relational, then when:
    - Subject line reflects that the message is commercial, or
    - Transactional or relationship content (or other content) does not substantially appear at the beginning of the message

108

Program Completed

109