ECE 498KL: eCrime and Internet Service Abuse

Communications Privacy

Kirill Levchenko

November 6, 2018

ILLINOIS
Electrical & Computer Engineering
COLLEGE OF ENGINEERING

Reading

- **18 U.S. Code § 2511, 2701, 2702, 2703, 2707 —** Interception and disclosure of communications
- Regularly amended (e.g. PATRIOT Act)
- Main law used to prosecute eavesdropping
- Derives authority from Commerce Clause of US Const.
  - "The Congress shall have Power … To regulate Commerce with foreign Nations, and among the several States …"

Reading Questions

- What kind of communication does ECPA protect?
- What acts does ECPA prohibit?
- What kind of communication does SCA protect?
- What kind of acts does SCA prohibit?

18 US Code § 2510, 2511

- 18 US Code § 2510 defines key terms
- 18 US Code § 2511(1) describes offenses
- 18 US Code § 2511(2) describes exclusions
- 18 US Code § 2511(3) pertains to providers
- 18 US Code § 2511(4)–(5) defines punishments

18 US Code § 2510, 2511

- **18 US Code § 2510 defines key terms**
- **18 US Code § 2511(1) describes offenses**
- **18 US Code § 2511(2) describes exclusions**
- **18 US Code § 2511(3) pertains to providers**
- 18 US Code § 2511(4)–(5) defines punishments

18 US Code § 2511(1)(a)

- Except as otherwise specifically provided in this chapter 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;

- *Prohibits eavesdropping*

Definitions

18 US Code § 2050

- (1) **wire communication:** any *aural transfer* made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of *interstate or foreign communications* or *communications affecting interstate or foreign commerce*;

- (18) **aural transfer:** a transfer containing the human voice at any point between and including the point of origin and the point of reception;

Definitions

18 US Code § 2050

- (2) **oral communication:** any *oral communication* uttered by a person exhibiting an *expectation* that such communication is *not subject to interception* under circumstances justifying such expectation, but such term does not include any electronic communication;

Definitions

18 US Code § 2050

- (12) **electronic communication:** any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—
  - (A) any wire or oral communication;
  - (B) any communication made through a tone-only paging device;
  - (C) any communication from a tracking device (as defined in section 3117 of this title); or
  - (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

18 US Code § 2511(1)(b)

- Except as otherwise specifically provided in this chapter any person who—

intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when—

- (i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or
- (ii) such device transmits communications by radio, or interferes with the transmission of such communication; or
- (iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

18 US Code § 2511(1)(b)

- Except as otherwise specifically provided in this chapter any person who—

intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when—

- (iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or
- (v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

18 US Code § 2511(1)(c)

- Except as otherwise specifically provided in this chapter any person who—

  intentionally *discloses*, or *endeavors to disclose*, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

- *Prohibits disclosing illegally obtained communication*

18 US Code § 2511(1)(d)

- Except as otherwise specifically provided in this chapter any person who—

  intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or

- *Prohibits using illegally obtained communication*

18 US Code § 2511(1)(e)

- Except as otherwise specifically provided in this chapter any person who—

  (i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by sections 2511(2)(a)(ii), 2511(2)(b)–(c), 2511(2)(e), 2516, and 2518 of this chapter, (ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation, (iii) having obtained or received the information in connection with a criminal investigation, and (iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation,

- *Prohibits disclosing with intent to obstruct investigation*

18 US Code § 2511(2)(a)(i)

- It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication *in the normal course of his employment* while engaged in any activity which is a *necessary incident to the rendition of his service* or to the *protection of the rights or property of the provider of that service*, except that a provider of wire communication service to the public *shall not utilize service observing or random monitoring except for mechanical or service quality control checks*.

- *Allows some interception necessary to provide service*

18 US Code § 2511(2)(a)(ii)

- Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are **authorized** to provide information, facilities, or technical assistance to persons *authorized by law* to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with …

- *Allows assisting in lawful interception*

18 US Code § 2511(2)(c)

- It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

- *Allows law enforcement interception when one of the parties has consented*

18 US Code § 2511(2)(d)

- It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.
- *Allows interception when one of the parties has consented*

18 US Code § 2511(2)(g)

- It shall not be unlawful under this chapter or chapter 121 of this title for any person—
  - (i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;
  - (ii) to intercept any radio communication which is transmitted—
    - (I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;
    - (II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;
    - (III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or
    - (IV) by any marine or aeronautical communications system;

18 US Code § 2511(2)(h)

- It shall not be unlawful under this chapter—
  - (i) to use a pen register or a trap and trace device (as those terms are defined for the purposes of chapter 206 (relating to pen registers and trap and trace devices) of this title);
- **18 US Code § 3121(a):** Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order …

18 US Code § 2511(2)(h)

- It shall not be unlawful under this chapter—
  - (ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or *abusive use of such service*.

18 US Code § 2701

- (a) Except as provided in subsection (c) of this section whoever—
  - (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
  - (2) intentionally exceeds an authorization to access that facility;
- and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section

18 US Code § 2701

- (c) Subsection (a) of this section does not apply with respect to conduct authorized—
  - (1) by the person or entity providing a wire or electronic communications service;
  - (2) by a user of that service with respect to a communication of or intended for that user;

18 US Code § 2702

- (a) Except as provided in subsection (b) or (c)—
  - (1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and
  - (2) a person or entity providing r*emote computing service* to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—

    …

18 US Code § 2702

- (b) A provider described in subsection (a) may divulge the contents of a communication—
  - (1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

    …
  - (3) with the lawful consent of the originator or an addressee or intended recipient of such communication, *or the subscriber in the case of remote computing service*;

18 US Code § 2702

- (b) A provider described in subsection (a) may divulge the contents of a communication—
  - (7) to a law enforcement agency— (A) if the contents—
    - (i) were inadvertently obtained by the service provider; and
    - appear to pertain to the commission of a crime;

18 US Code § 2702

(c) EXCEPTIONS FOR DISCLOSURE OF CUSTOMER RECORDS.—A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))—

(1) as otherwise authorized in section 2703;

(2) with the lawful consent of the customer or subscriber;

(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(4) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency;

(5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A; or

(6) to any person other than a governmental entity.

18 US Code § 2703(a)

- A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for **one hundred and eighty days or less**, only pursuant to a warrant … A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for **more than one hundred and eighty days** by the means available under subsection (b) of this section.

18 US Code § 2703(b)

- (1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—
  - (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant …

18 US Code § 2703(c)

- (1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—
  - (A) obtains a warrant … ; or
    …
  - (E) seeks information under paragraph (2).

18 US Code § 2703(c)

- (2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—
  - (A) name;
  - (B) address;
  - (C) local and long distance telephone connection records, or records of session times and durations;
  - (D) length of service (including start date) and types of service utilized;
  - (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
  - (F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

18 US Code § 2707

- **(a) Cause of Action.—**
  Except as provided in section 2703(e), any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

Syllabus

NOTE: Where it is feasible, a syllabus (headnote) will be released, as is being done in connection with this case, at the time the opinion is issued. The syllabus constitutes no part of the opinion of the Court but has been prepared by the Reporter of Decisions for the convenience of the reader. See *United States* v. *Detroit Timber & Lumber Co.,* 200 U. S. 321, 337.

SUPREME COURT OF THE UNITED STATES

Syllabus

CITY OF ONTARIO, CALIFORNIA, ET AL. *v.* QUON ET AL.

CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

No. 08–1332. Argued April 19, 2010—Decided June 17, 2010

Petitioner Ontario (hereinafter City) acquired alphanumeric pagers able to send and receive text messages. Its contract with its service provider, Arch Wireless, provided for a monthly limit on the number of characters each pager could send or receive, and specified that usage exceeding that number would result in an additional fee. The City issued the pagers to respondent Quon and other officers in its

Petitioner Ontario (hereinafter City) acquired alphanumeric pagers able to send and receive text messages. Its contract with its service provider, Arch Wireless, provided for a monthly limit on the number of characters each pager could send or receive, and specified that usage exceeding that number would result in an additional fee. The City issued the pagers to respondent Quon and other officers in its police department (OPD), also a petitioner here. When Quon and others exceeded their monthly character limits for several months running, petitioner Scharf, OPD's chief, sought to determine whether the existing limit was too low, *i.e.*, whether the officers had to pay fees for sending work-related messages or, conversely, whether the overages were for personal messages. After Arch Wireless provided transcripts of Quon's and another employee's August and September 2002 text messages, it was discovered that many of Quon's messages were not work related, and some were sexually explicit. Scharf referred the matter to OPD's internal affairs division. The investigating officer used Quon's work schedule to redact from his transcript any messages he sent while off duty, but the transcript showed that few of his on-duty messages related to police business. Quon was disciplined for violating OPD rules.

He and the other respondents—each of whom had exchanged text messages with Quon during August and September—filed this suit,

Ontario v. Quon

- *Do public employees have an expectation of privacy with respect to stored communications (e.g. email)?*
- ECPA generally prohibits interception of communications
- **18 US Code § 2072(b)** allows: A provider described in subsection (a) may divulge the contents of a communication … (3) with the lawful consent of the originator or an addressee or intended recipient of such communication, *or the subscriber in the case of remote computing service*

Ontario v. Quon

Held: Because the search of Quon's text messages was reasonable, petitioners did not violate respondents' Fourth Amendment rights, and the Ninth Circuit erred by concluding otherwise. Pp. 7–17.

(a) The Amendment guarantees a person's privacy, dignity, and security against arbitrary and invasive governmental acts, without regard to whether the government actor is investigating crime or performing another function. *Skinner* v. *Railway Labor Executives'*

Ontario v. Quon

(1) The Court does not resolve the parties' disagreement over Quon's privacy expectation. Prudence counsels caution before the facts in this case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations of employees using employer-provided communication devices. Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior. At present, it is uncertain how workplace norms, and the law's treatment of them, will evolve. Because it is therefore preferable to dispose of this case on narrower grounds, the Court assumes, *arguendo,* that: (1) Quon had a reasonable privacy expectation; (2) petitioners' review of the transcript constituted a Fourth Amendment search; and (3) the principles applicable to a government employer's search of an employee's physical office apply as well in the electronic sphere. Pp. 9–12.

(2) Petitioners' warrantless review of Quon's pager transcript was reasonable under the *O'Connor* plurality's approach because it was motivated by a legitimate work-related purpose, and because it was not excessive in scope. See 480 U. S., at 726. There were "reasonable

GALLO LLP
1299 Fourth St., Suite 505
San Rafael, CA 94901
Telephone: 415.257.8800

Attorneys for Plaintiff,
individually and on behalf of
all others similarly situated

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

DANIEL MATERA, as an individual, and on behalf of other persons similarly situated,

Plaintiff,

v.

GOOGLE, INC.,

Defendant.

Case No. 5:15-cv-04062

CLASS ACTION COMPLAINT FOR:

1. Violations of the California Invasion of Privacy Act, Cal. Pen. Code §630 *et seq*.

2. Violations of the Electronic Communications Privacy Act, 18 U.S.C. §2510 *et seq*.

DEMAND FOR JURY TRIAL

I. INTRODUCTION

1. Defendant Google, Inc. ("Google," "Defendant," or "the Company") has created a business model that relies upon intercepting, reading, and analyzing the content of private email messages. Specifically, in offering its web-based email service ("Gmail")[1] to users, Google elected to forego charging money for the service, instead employing a system architecture that scans each email sent to or from a Gmail accountholder, then deriving and cataloging the content of that email in order to create data profiles of the communicants for purposes of selling to paying customers, and sending to the profiled communicants, targeted advertising based upon analysis of these profiles.

2. In so doing, Google secretly and systematically diverts the transmission of email messages to devices—separate from the devices that are instrumental to sending and receiving email—that are designed to and do extract the messages' content. Google analyzes the content of users' email messages to predict their behavior, and to influence and manipulate them in order to gain an economic advantage over them. As Google's former CEO Eric Schmidt described it: "We know where you are. We know where you've been. We can more or less know what you're thinking about."[2]

architecture that scans each email sent to or from a Gmail accountholder, then deriving and cataloging the content of that email in order to create data profiles of the communicants for purposes of selling to paying customers, and sending to the profiled communicants, targeted advertising based upon analysis of these profiles.

2. In so doing, Google secretly and systematically diverts the transmission of email messages to devices—separate from the devices that are instrumental to sending and receiving email—that are designed to and do extract the messages' content. Google analyzes the content of users' email messages to predict their behavior, and to influence and manipulate them in order to gain an economic advantage over them. As Google's former CEO Eric Schmidt described it: "We know where you are. We know where you've been. We can more or less know what you're thinking about."[2]

3. Google has not obtained any consent from non-Gmail users to having their emails scanned, analyzed, and cataloged indefinitely. These individuals have never agreed to Google's terms of service and have not at any point or in any fashion agreed to allow Google to acquire and indefinitely store the contents of their emails. Yet, whenever these individuals send or receive email messages from a Gmail accountholder, this is precisely what Google does.

4. Google's practice of intercepting, extracting, reading, and using the private email content of individuals who do not have email accounts with Google violates the

64. Google used one or more "devices," as defined pursuant to 18 U.S.C. § 2510(5), to intercept the electronic communications transmitted to Google mail users by Plaintiff and the Class members, and each of them. Such devices include, but are not limited to, the distinct pieces of Google infrastructure comprising the COB process, Changeling, the "Nemo" process, and PHIL.

65. The devices were not used by Google, operating as an electronic communication service, in the ordinary course of providing electronic communication services. Specifically, Google's interception of electronic communications sent by and to Plaintiff and the Class members, and each of them was, among other things, (a) for undisclosed purposes; (b) for purposes of acquiring, cataloging and retaining user data; (c) for purposes beyond facilitating the transmission of emails sent or received by either Gmail users or Plaintiff and the Class members; (f) contrary to Google's public statements; (g) in violation of federal law; and (h) in violation of the property rights of Plaintiff and Class members in their private information. These activities are not within the ordinary course of business of a provider of an electronic communication service.