LANGLEY & BANACK

INCORPORATED

Attorneys and Counselors at Law

CYBER SECURITY AND PRIVACY

Tales From The Trenches

Lui Chambers

Shareholder

WHY SHOULD YOU CARE

Some cautionary tales from the real world:

- Purchase of a residential home (intermediaries/principals)
- Providing of products and services, e.g. insurance broker (3P vendor requirements); small company (spear-phishing, spoofing)
- Local bank (incident response)
- Company with national reach (US laws)
- Global company (GDPR)

INFORMATION PRIVACY

- Information privacy is concerned with creating rules that govern the collection and handling of personal information
- Understanding what constitutes personal information is key
- Key Issue is the degree of nexus of information to a particular person
  - What is personal information?
  - When does it become non-personal information?

EXAMPLE: CARPENTER VS. U.S.

- 5-4 SCOTUS ruling holds that the Fourth Amendment to the U.S. Constitution requires the government to obtain ***a warrant***, and not merely ***a subpoena*** (as is required under the *Stored Communications Act)* to obtain customer cell site location information from a wireless communications company. The Supreme Court acknowledged that there exists a privacy interest in a cellphone's ***persistent and constant generation of location data*** and found that such interests are ***not waived by involuntarily sharing*** that data with the wireless company

EXAMPLE: CALIFORNIA CONSUMER PRIVACY ACT OF 2018

Adopted by California Legislature on June 28, 2018 and immediately signed into law by the Governor of California

- In return for withdrawing an even more onerous ballot initiative from consideration in November 2018

Effective Date: January 1, 2020

- Adds to the already fragmented privacy legal landscape in California, US and rest of the world
  - Does not amend the 2002 California data breach notification law or the 2004 website privacy policy laws
  - In fact, (new) Cal. Civ. Code §1798.175 provides that in case of any conflicts with any other California laws, the law that affords the greatest privacy protections shall control

THE CALI WAY

- In parts stricter than GDPR
- Data can be protected even if it does not relate to a single individual and if it does not contain a name
- E.g., household consumption of electricity, natural gas, water; IP addresses, a specific employee's job description, web browsing history and purchasing tendencies are regulated as personal information, even if no individual's name is associated with any of these
- Some complex and limited exceptions apply : "publicly available information"; commercial conduct occurring 100% outside of California

CALIFORNIA CONSUMER PRIVACY ACT OF 2018 *Continued*

- **Addresses:** Processing of personal data of California residents
- **Applies to:** Businesses that collect California consumers' personal information, as well as to those that sell consumers' personal information or disclose it for a business purpose (data brokers)
- **Act contains:**
  - right to data collection transparency
  - right to be forgotten (i.e. "deleted")
  - right to data portability, and
  - right to opt out of having your data sold (affirmative opt in for minors) without being discriminated against financially or otherwise

"PERSONAL INFORMATION" EXTREMELY BROADLY DEFINED

- "Personal information" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household
- Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier IP address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers
- Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchase/consumption histories or patterns
- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with any internet web site, application, or advertisement
- Geolocation data
- Audio, electronic, visual, thermal, olfactory, or similar information
- Professional or employment-related information.

"PERSONAL INFORMATION" EXTREMELY BROADLY DEFINED *Continued*

- Education information, that is not publicly available and personally identifiable
- Inferences drawn from any of the information identified to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes
- "Personal information" does not include "publicly available" information.
- "Publicly available" means information that is lawfully made available from federal, state, or local government records
- "Publicly available" does not mean:
  - Biometric information collected by a business about a consumer without the consumer's knowledge
  - Data used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained
  - Consumer information that is de-identified, or aggregate consumer information

U.S. CYBERSPACE REGULATORS


50
AGs

HOW DID WE GET HERE?

Let's step back in time…

THE PRIVACY RIGHT

- Concept is not spelled out in the U.S. Constitution
- BUT, a number of provisions relate to "privacy"
  - 3rd Amendment: Bans the mandatory housing of soldiers in a person's home
  - 4th Amendment: Requires a search warrant before a search and seizure
  - 5th Amendment: Prohibits persons from being forced to testify against themselves
  - 14th Amendment: Mandates due process under the law

A MAN'S HOUSE IS HIS CASTLE

- In 1890 Samuel D. Warren and Louis D. Brandeis published their article "The Right to Privacy" (*Harvard Law Review*, Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220)
- Privacy: A Definition Articulated

Privacy = "The right to be let alone"


UNITED NATIONS
NATIONS UNIES

UNITED NATIONS 1948

- **Universal Declaration of Human Rights** (December 1948)

  Article 12

  – No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour [sic] and reputation. Everyone has the right to the protection of the law against such interference or attacks.

COUNCIL OF EUROPE 1950

European Convention for the Protection of Human Rights and Fundamental Freedoms

Article 8 – Right to respect for **private** and family life

1. Everyone has the right to respect for his **private** and family life, his home and his correspondence.

1. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

CALIFORNIA 1972

Added by ballot in November 1972, the California Constitution contains an express guarantee to the right of privacy:

ARTICLE 1 DECLARATION OF RIGHTS

Section 1: All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and **privacy**.

COUNCIL OF EUROPE 1981

- Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Convention 108)
- First legally binding international instrument in the field of data protection
- Under the Convention, member states were required to incorporate certain data protection provisions into their respective domestic laws

EUROPE NOW = GDPR

- General Data Protection Regulation
- Comprehensive model (all sectors; one regulator per country)

Effective Since: May 25, 2018

WHAT ABOUT THE U.S.?

- Sectoral, state-level and co-regulatory model
- Justification of sectoral approach: Different parts of the economy face different privacy security challenges
- Critique of sectoral approach: lack of a single data protection regulator to oversee privacy issues

KEY U.S. PRIVACY REGULATORS

- U.S. Federal Trade Commission (FTC)
  - FTC has played significant role in the development of the U.S. privacy regulatory framework
  - Under Section 5 of the FTC Act, which prohibits unfair and deceptive trade practices
- Federal Communications Commission (FCC)
  - CAN-SPAM (with FTC)
  - Children's Online Privacy Protection Act (COPPA) (FTC)
  - Telephone Consumer Protection Act (FCC &FTC)

PRIVACY REGULATORS
Continued

- Consumer Financial Protection Bureau
  - Consumer financial privacy in general
- Federal Reserve System
  - Financial privacy/institutions – Gramm-Leach-Bliley Act (GLBA)
- Office of the Comptroller of the Currency
  - Financial privacy/institutions – Gramm-Leach-Bliley Act (GLBA)
- U.S. Department of Transportation
  - Enforces Privacy Shield Framework between U.S. and EU for some transportation companies
  - FAA (drones)

PRIVACY REGULATORS
Continued

- U.S. Department of Health and Human Services (through Office of Civil Rights)
  - Medical privacy – Health Insurance Portability and Accountability Act (HIPAA)
- Department of Education
  - Education privacy – Family Educational Rights and Privacy Act
- Equal Employment Opportunity Commission et al.
  - Workplace privacy
- U.S. Office of Management and Budget (OMB)
  - Lead agency to interpret the Privacy Act of 1974 (applies to federal agencies and private-sector contractors (data breach disclosure, privacy impact assessment))

PRIVACY REGULATORS
Continued

- Internal Revenue Service
- U.S. Department of Homeland Security
  - e-verify; air traveler records
- But not: U.S. Department of Commerce. Has no privacy regulatory authority!
- State attorneys general
- *Self-regulatory regimes (Network Advertising Initiative, Direct Marketing Association, Children's Advertising Review Unit)
- *Trade associations
- Others

REGULATIONS PROMULGATED BY FTC

The FTC has authority to issue rules that regulate specific areas of consumer privacy and security:

- **Health Breach Notification Rule:** Requires certain web-based businesses to notify consumers when the security of their electronic health information is breached
- **Red Flags Rule:** Requires financial institutions/certain creditors to have identity theft prevention programs to identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft
- **COPPA Rule:** Requires websites and apps to get parental consent before collecting personal information from kids under 13
- **GLB Privacy Rule:** Sets forth when car dealerships must provide consumers with initial and annual notices explaining the dealer's privacy policies and practices and provide a consumer with an opportunity to opt out of disclosures of certain information to nonaffiliated third parties.

Source: FTC

REGULATIONS PROMULGATED BY FTC

Continued

- **GLB Safeguards Rule:** Requires financial institutions over which the FTC has jurisdiction to develop, implement, and maintain a comprehensive information security program that contains administrative, technical, and physical safeguards
- **Telemarketing Sales Rule:** Requires telemarketers to make specific disclosures of material information; prohibits misrepresentations; limits the hours that telemarketers may call consumers; and sets payment restrictions for the sale of certain goods and services. Do Not Call provisions of the Rule prohibit sellers and telemarketers from calling an individual whose number is listed with the Do Not Call Registry or who has asked not to receive telemarketing calls from a particular company. The Rule also prohibits robocalls, unless the telemarketer has obtained permission in writing from consumers who want to receive such calls

Source: FTC

REGULATIONS PROMULGATED BY FTC

Continued

- **Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM)** Designed to protect consumers from deceptive commercial email and requires companies to have opt out mechanisms in place
- **Disposal Rule** under the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), which amended the FCRA, requires that companies dispose of credit reports and information derived from them in a safe and secure manner
- **Pre-screen Opt-out Rule under FACTA** requires companies that send "prescreened" solicitations of credit or insurance to consumers to provide simple and easy-to-understand notices that explain consumers' right to opt out of receiving future offers

Source: FTC

CAN-SPAM

- EXAMPLE: CAN-SPAM (Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003)
- Requires senders of unsolicited or unwanted commercial emails to offer an "opt-out" option to recipients of these messages
- CAN-SPAM enforced jointly by FTC and FCC
- CAN-SPAM Factoid: **Preempts** state laws that might otherwise impose greater obligations on senders of unsolicited commercial emails
- Express preemption provisions intended to create a single regulatory treatment of unsolicited/unwanted emails

FTC: PRIVACY AND DATA SECURITY UPDATE 2015

5 best practices:

1. Companies should be cognizant of what digital consumer information they have and who has legitimate access to this information
2. Companies should limit the data they collect and maintain for their legitimate business purposes
3. Companies should protect the data/information they maintain by assessing risks and implementing procedures for
   - electronic security,
   - physical security
   - employee training
   - vendor management
4. Companies should properly dispose of information they no longer need
5. Companies should have plan to respond to security incidents

Source: FTC

FTC: PRIVACY AND DATA SECURITY UPDATE 2016

Focus on three new technology areas:

- Smart TVs (tracking consumer viewing habits)
- Drones
- Ransomware (prevent infiltration/limit impact)

Source: FTC

FTC: PRIVACY AND DATA SECURITY UPDATE 2017

Focus on three new technology areas:

- Peer-to-peer payment systems and crowdfunding platforms
- Artificial Intelligence and Blockchain
- Automated vehicles/connected cars
- Informational Injury*
- Small business outreach*

Source: FTC

FTC: ENFORCEMENT UPDATE 2017

- In 2017, the FTC brought enforcement actions addressing a wide range of privacy issues, including:
  - Spam,
  - Social networking,
  - Behavioral advertising,
  - Pretexting (social engineering, phishing, spear-phishing)
  - Spyware,
  - Peer-to-peer file sharing, and
  - Mobile
- Actions included over 130 spam and spyware cases and more than 50 general privacy lawsuits

Source: FTC

DATA SECURITY – THE UBER CASE

- Since 2002, the FTC has brought over 60 cases against companies that have engaged in unfair or deceptive practices because they failed to adequately protect consumers' personal data despite claiming to do so
- In 2017 brought a complaint against Uber Technologies, Inc., for allegedly deceiving consumers by (in 2014) failing to reasonably secure sensitive consumer data stored in the cloud. The FTC's complaint alleged that despite Uber's claim that data was "securely stored within our databases," Uber's security practices failed to provide reasonable security to prevent unauthorized access to consumers' personal information in databases Uber stored with a third-party cloud provider. In November 2016, intruders again gained access to consumer data:
- *Revised* Consent Decree 2018:
  - Uber must disclose certain future incidents involving consumer data
  - Must submit to the FTC all reports from the required third-party audits of Uber's privacy program (rather than only the initial report as required in the original draft consent decree)
  - Uber must retain certain records related to bug bounty reports regarding vulnerabilities that relate to potential or actual unauthorized access to consumer data

Source: FTC

DATA SECURITY – THE UBER CASE

What happened

- Uber stored sensitive consumer information, including geolocation information, in plain readable text in database back-ups stored in the cloud
- Uber allowed use of a single factor key that gave full administrative access to all data (including sensitive data), and did not require multi-factor authentication for accessing the data, i.e. Uber failed to require engineers and programmers to use distinct/complex access keys to access personal information stored in the cloud
- As a result, an intruder accessed personal information about Uber drivers in May 2014, including more than 100,000 names and driver's license numbers that Uber stored in a cloud operated by Amazon Web Services; in 2016 intruders again gained unauthorized access to data

Source: FTC

ORIGIN OF DATA BREACHES

Types:

- Unintended disclosure
- Hacking or malware
- Payment card fraud
- Physical loss
- Portable device
- Stationary device
- Insider
- Other

DATA BREACH 101

Incident management steps:

- Ascertain whether a breach has actually occurred
- Contain and analyze
- Notify affected parties
- Implement effective follow up methods/lessons learned

THE U.S. DATA BREACH LEGAL FRAMEWORK

- No uniform federal data breach law
- All 50 states, D.C. Puerto Rico and US Virgin Islands have enacted data breach notification laws
- All contain same basic elements that define:
  - What constitutes P(I)I (specific data elements)
  - Which entities are covered
  - Data security breach
  - Level of harm requiring notification
  - When to Notify
  - Whom to notify
  - How to notify
  - What to include in the notification
  - Exception to obligations to notify/delay notification
  - Penalties and rights of action

TYPICAL EXAMPLE OF P(I)I

An individuals first name or first initial and last name in combination with any one or more of the following data:

- SSN
- DL or state identification number; or
- Account number, credit or debit card number in combination with required security/access code or password

DATA BREACH (TX): DEFINED

Texas Business & Commerce Code, CHAPTER 521:
Unauthorized Use of Identifying Information

aka Identity Theft Enforcement and Protection Act

"Personal identifying information" means information that alone or in conjunction with other information identifies an individual, including an individual's:

(A) name, social security number, date of birth, or government-issued identification number;

(B) mother's maiden name;

(C) unique biometric data, including the individual's fingerprint, voice print, and retina or iris image;

(D) unique electronic identification number, address, or routing code; ***and***

(E) telecommunication access device

DATA BREACH (TX): DEFINED

Continued

"Sensitive personal information" defined as:

(A) an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are **not encrypted:**

- social security number;
- driver's license number or government-issued identification number; ***or***
- account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; ***or***

(B) information that identifies an individual and relates to:

- the physical or mental health or condition of the individual;
- the provision of health care to the individual; ***or***
- payment for the provision of health care to the individual.

"Sensitive personal information" does not include **publicly available information** that is **lawfully made available** to the public from the **federal government** or a **state or local government.**

DATA BREACH (TX): DUTY TO PROTECT PII

A person may not obtain, possess, transfer, or use **personal identifying information** of another person without the other person's consent and with intent to obtain a good, a service, insurance, an extension of credit, or any other thing of value in the other person's name.

DATA BREACH (TX): DUTY TO PROTECT SPI

BUSINESS DUTY TO PROTECT SENSITIVE PERSONAL INFORMATION

- A business must implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in its regular course of business
- A business must destroy or arrange for the destruction of customer records containing sensitive personal information within the business's custody or control that are not to be retained by the business by:
  - shredding
  - erasing ***or***
  - otherwise modifying the sensitive personal information in the records to make the information unreadable or indecipherable through any means
- "Business" includes a nonprofit athletic or sports association.
- "Breach of system security" is defined as the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data.
- Violation of statute is a deceptive trade practice

DATA BREACH (TX): NOTIFICATION REQUIREMENT

- A person who **conducts business in Te**xas and **owns or licenses** computerized data that includes **sensitive personal information** must disclose any breach of system security, after discovering or receiving notification of the breach, **to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person**. The disclosure shall be made as quickly as possible, or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

- If the individual whose sensitive personal information was or is reasonably believed to have been acquired by an unauthorized person is a resident **of a state** that requires a person to provide notice of a breach of system security, the notice of the breach of system security required may be provided **under that state's law or the Texas statute**.

DATA BREACH (TX): NOTIFICATION REQUIREMENT

Duty to Notify: Any person who maintains computerized data that includes ***sensitive personal information*** not owned by the person shall notify the owner or license holder of the information of any breach of system security **immediately after discovering the breach**, ***if the sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person***

You may delay providing notice at the request of a law enforcement agency that determines that the notification will impede a criminal investigation. The notification shall be made as soon as the law enforcement agency determines that the notification will not compromise the investigation

DATA BREACH (TX): NOTIFICATION

You may give notice by providing:

- Written notice at the last known address of the individual;
- Electronic notice, if provided in accordance with 15 U.S.C. Section 7001 (electronic records and signatures in interstate commerce);
- Pursuant to Safe Harbor; or
- Pursuant to your own internal data breach notification procedures to the extent it complies with the timing requirements for notice under Subchapter 521

DATA BREACH (TX): NOTIFICATION

Safe Harbor: (1) Demonstrate that the cost of providing notice would exceed $250,000, (2) the number of affected persons exceeds 500,000, or (3) not sufficient contact information, the notice may be given by:

- Email, if you have email addresses for persons affected;
- Conspicuous posting of the notice on your website; **or**
- Notice published in or broadcast on major statewide media.

If you are required to notify at any one time **more than 10,000 persons** of a breach of system security, you must also notify without unreasonable delay, each **consumer reporting agency** that maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notices.

DATA BREACH (TX): VICTIMS RIGHTS

A person who is injured by a data breach may file an application with a district court for the issuance of an order declaring that the person is a **victim of identity theft** and regardless of whether the person is able to identify each person who allegedly transferred or used the person's identifying information in an unlawful manner.

DATA BREACH (TX): PENALTIES

- Civil penalty of at least $2,000 but not more than $50,000 for each violation.

PLUS

- $100 for each individual to whom notification is due for each consecutive day that you fail to take reasonable action to comply with the notification requirement up to a maximum of $250,000 for all individuals to whom notification is due after a single breach.

LANGLEY & BANACK

INCORPORATED

Attorneys and Counselors at Law

THANK YOU

For more information: lchambers@langleybanack.com