CSE 410 Privacy-Enhancing Technologies
Spring 2025

Marina Blanton

Department of Computer Science and Engineering
University at Buffalo

Lecture 1: Introduction to Privacy

What is Privacy?

Privacy is the ability of a person or group of people to seclude themselves or information about themselves from public view

Discussions of privacy date centuries back and privacy is viewed as an important human right

- privacy cannot be uniformly defined for all individuals
- privacy expectations depend on the societal values and change over time
- discussing privacy in the digital age is particularly important

Privacy as a Fundamental Right

In this course, we'll take the notion of privacy broadly

Unvoluntary collection or disclosure of information about an individual is considered privacy abuse

- surveillance
- network traffic capture
- stalking
- malware with spying capabilities (spyware, keyloggers, etc.)
- data breaches
- web tracking

The Internet and Privacy

In the interconnected world, we can think of two types of information available about us online

- Information we made available about ourselves

The Internet and Privacy

In the interconnected world, we can think of two types of information available about us online

- Information we made available about ourselves
- Information others produced and/or made available about us
  - this can be with or without our knowledge and with or without our consent

The Internet and Privacy

In the interconnected world, we can think of two types of information available about us online

- Information we made available about ourselves
- Information others produced and/or made available about us
  - this can be with or without our knowledge and with or without our consent
  - examples:
    - employer published information
    - medical records
    - credit reporting agencies data
    - social networks

The Internet and Privacy

However, what is more difficult to assess and control is information deduced about us from using either or both types of the sources above

The Internet and Privacy

However, what is more difficult to assess and control is information deduced about us from using either or both types of the sources above

Exercise: what does Google know about me?

- Gmail, Google Search, Google Maps, Google Docs, Google Drive, YouTube, Chrome, Hangout/Meet, Photos, Shopping, ...

The Internet and Privacy

However, what is more difficult to assess and control is information deduced about us from using either or both types of the sources above

Exercise: what does Google know about me?

- Gmail, Google Search, Google Maps, Google Docs, Google Drive, YouTube, Chrome, Hangout/Meet, Photos, Shopping, ...

With many free services, we are not customers, we are products

The Internet and Privacy

However, what is more difficult to assess and control is information deduced about us from using either or both types of the sources above

Exercise: what does Google know about me?

- Gmail, Google Search, Google Maps, Google Docs, Google Drive, YouTube, Chrome, Hangout/Meet, Photos, Shopping, ...

With many free services, we are not customers, we are products

Think about what the future with IoT devices hold

Information Disclosure

Information disclosure can also take different forms:

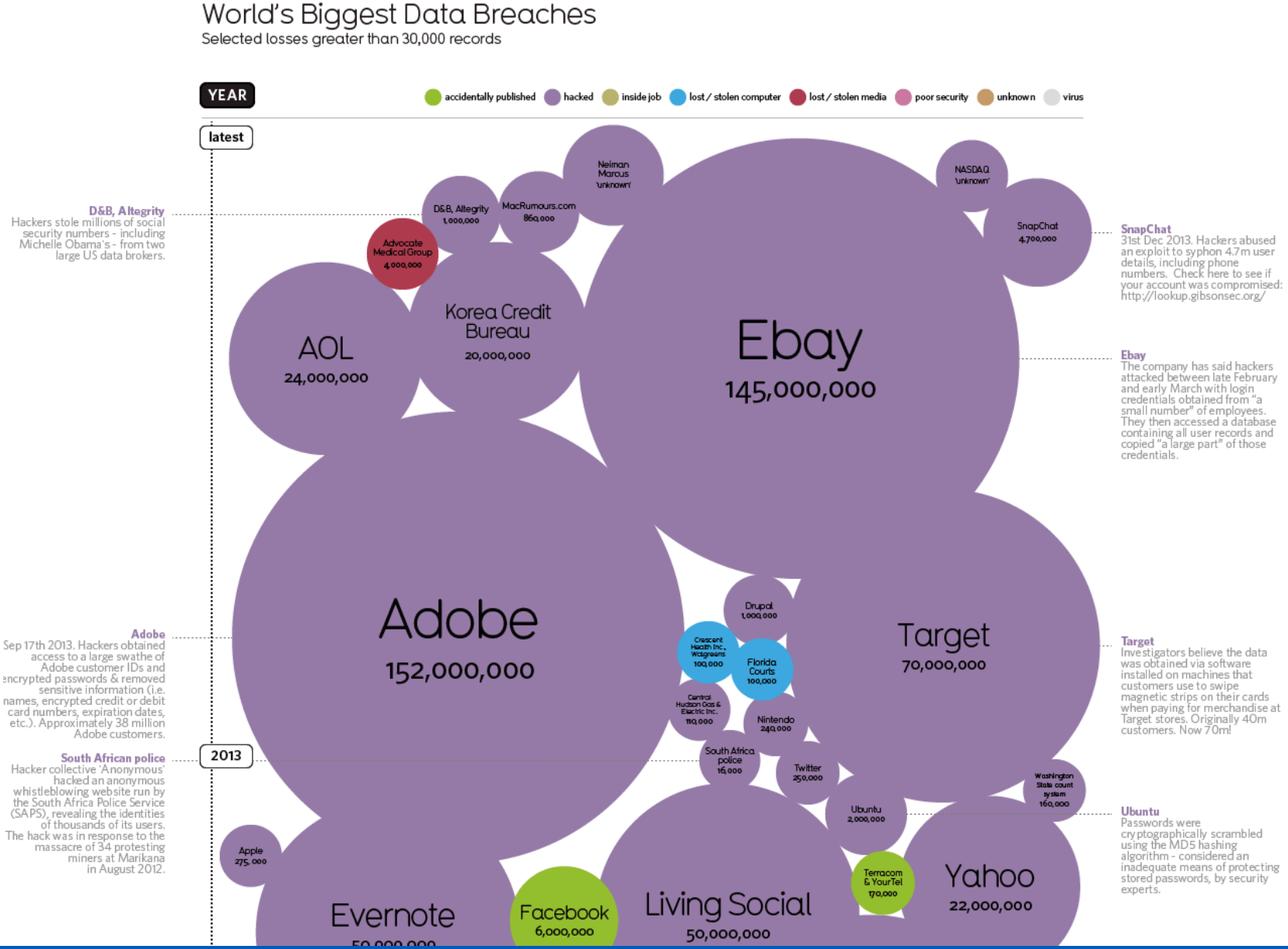
- Legitimate – i.e., according to the terms of service – data sharing can already be problematic
  - privacy policies are traditionally long and incomprehensible
  - you often have no control over what information is collected or how it is used
  - information about you is shared with or sold to third parties
  - examples: retailers, Facebook and apps on Facebook

Information Disclosure

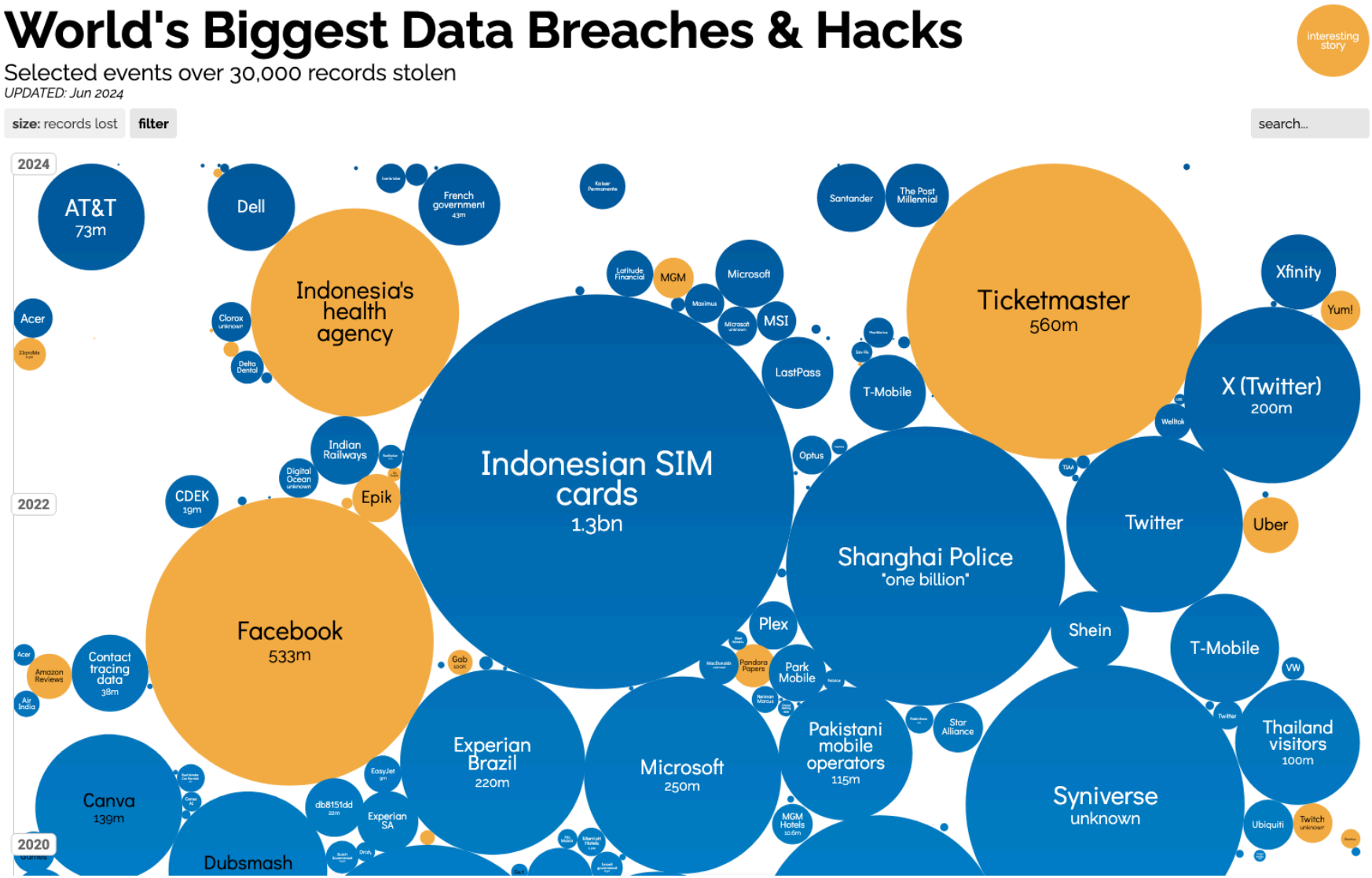
Information disclosure can also take different forms:

- Legitimate – i.e., according to the terms of service – data sharing can already be problematic
  - privacy policies are traditionally long and incomprehensible
  - you often have no control over what information is collected or how it is used
  - information about you is shared with or sold to third parties
  - examples: retailers, Facebook and apps on Facebook
- Unintended data breaches and information leaks present much bigger problems
  - personal examples: medical data, OPM data breach, Equifax

Data Breaches Illustrated

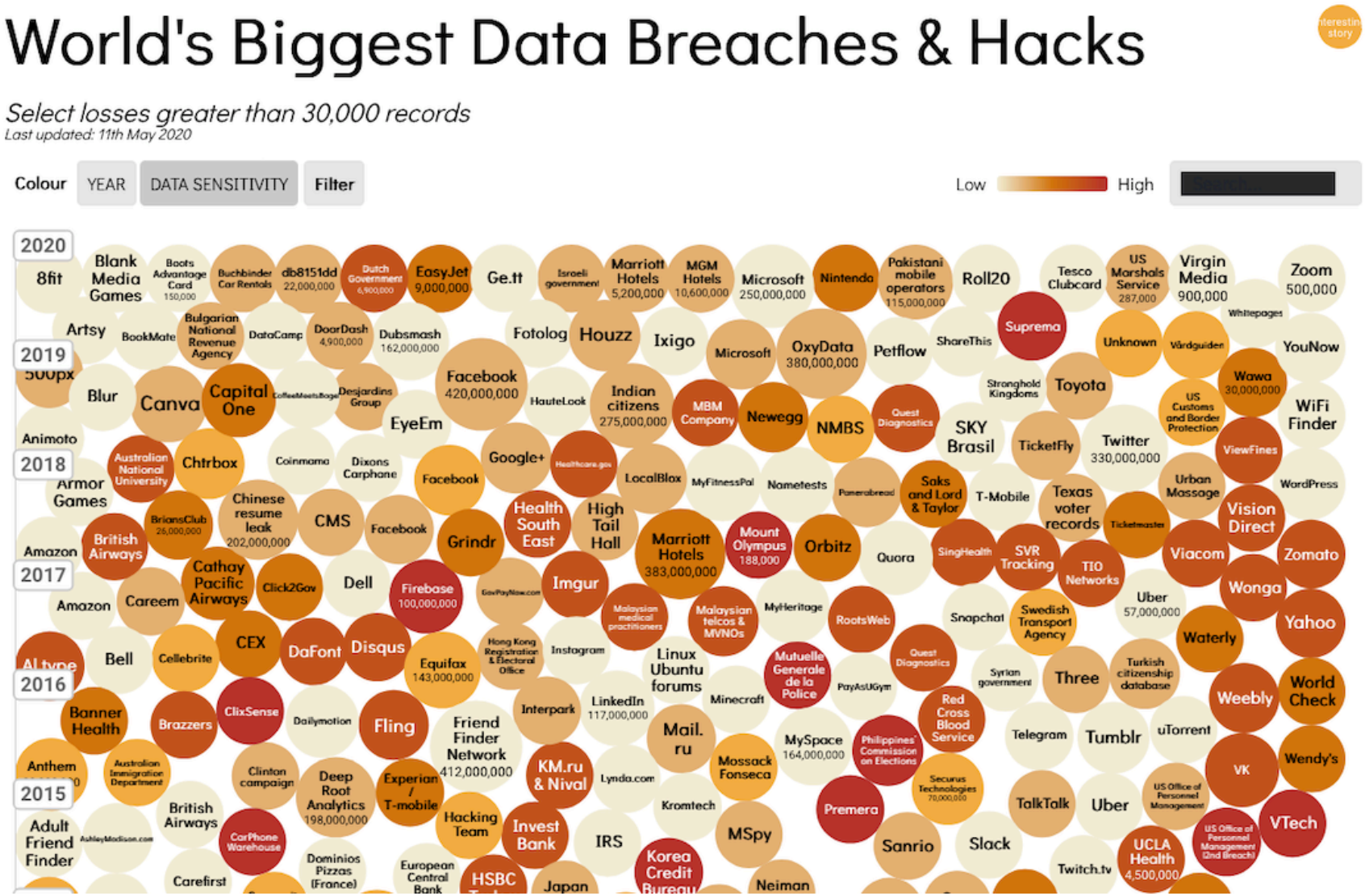


Data Breaches Illustrated



Data Breaches Illustrated

www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/



Consequences of Data Breaches

- Stolen data sets are sold on the black market
- Data lost by organizations becomes a headache for the affected individuals
- Consequences include:
  - purchases using stolen credit cards and bank accounts
  - identity theft
  - robbery
  - access to secure facilities
  - blackmail
  - spam/scam/phishing

Surveillance

Surveillance

Edward Snowden's classified documents' leak in 2013 disclosed details of mass data collection and mining

- many tech companies cooperated with the NSA to provide data at NSA's request
- phone companies must turn in bulk phone data at NSA's request
- the NSA hacked into Google and Yahoo data centers
- the NSA intercepts deliveries and installs backdoors
- the NSA collects email and IM contact lists

Surveillance

- Encrypting network data is insufficient
- Meta-data – or who is talking to whom, when, etc. – needs to be protected as well
  - one can get killed based on meta-data
- Censorship also denies access based on the end points
- Protecting meta-data can protect against both surveillance and censorship

Privacy Laws

A number of laws exist to protect personal privacy

- Europe's approach: general federal-level protection
  - privacy law at the level of the entire European Union (EU)
- US approach: no general federal-level protection
  - scarce protection by some industry/government sectors
  - protection for minors
  - new state-level laws

US Privacy Laws

- US Privacy Act, 1974
  - it states rights of individuals when their personal information is collected and used by federal agencies
  - citizens can access data held by government agencies and correct any errors
  - agencies should minimize data collection
  - access to data is restricted on a need to know basis
- FERPA, 1974
  - stands for Family Educational Rights and Privacy Act
  - generally prohibits disclosure of personally identifying information contained in education records to third parties
  - access can be granted with a parent's or student's written consent
  - this means colleges cannot disclose student performance

US Privacy Laws

- HIPAA, 1996
  - stands for Health Insurance Portability and Accountability Act
  - complex law that protects medical and health insurance records
  - includes privacy and security sections
  - health care providers generally have permission to use patient data for
    - treatment
    - payment
    - health care operations
  - additional uses require explicit authorization

US Privacy Laws

- GLBA, 1999
  - stands for Gramm-Leach-Bliley Act
  - complicated banking and financial law that includes data privacy and security requirements
  - protects nonpublic personal information collected in connection to providing financial service
  - can opt out of data sharing with non-affiliated parties, but not with other entities (limited protection)
- COPPA, 2000
  - stands for Children's Online Privacy Protection Act
  - restricts collection of data from children under 13
  - personal information is not to be collected from minors without verifiable parental consent
  - the law was updated to expand the scope of personal data

US Privacy Laws

No comprehensive law that protects us from our information being collected without authorization, abused, or lost

- current business model: data = money, collect if you can
- contrast this with European laws where data has to be collected for a purpose
- no legal framework to prosecute privacy abuses
- privacy policies are often vague or ambiguous
- explanation of privacy policies is not easy to get
- usage of personal information is decided without user consent
- the government can buy information compiled by non-government entities

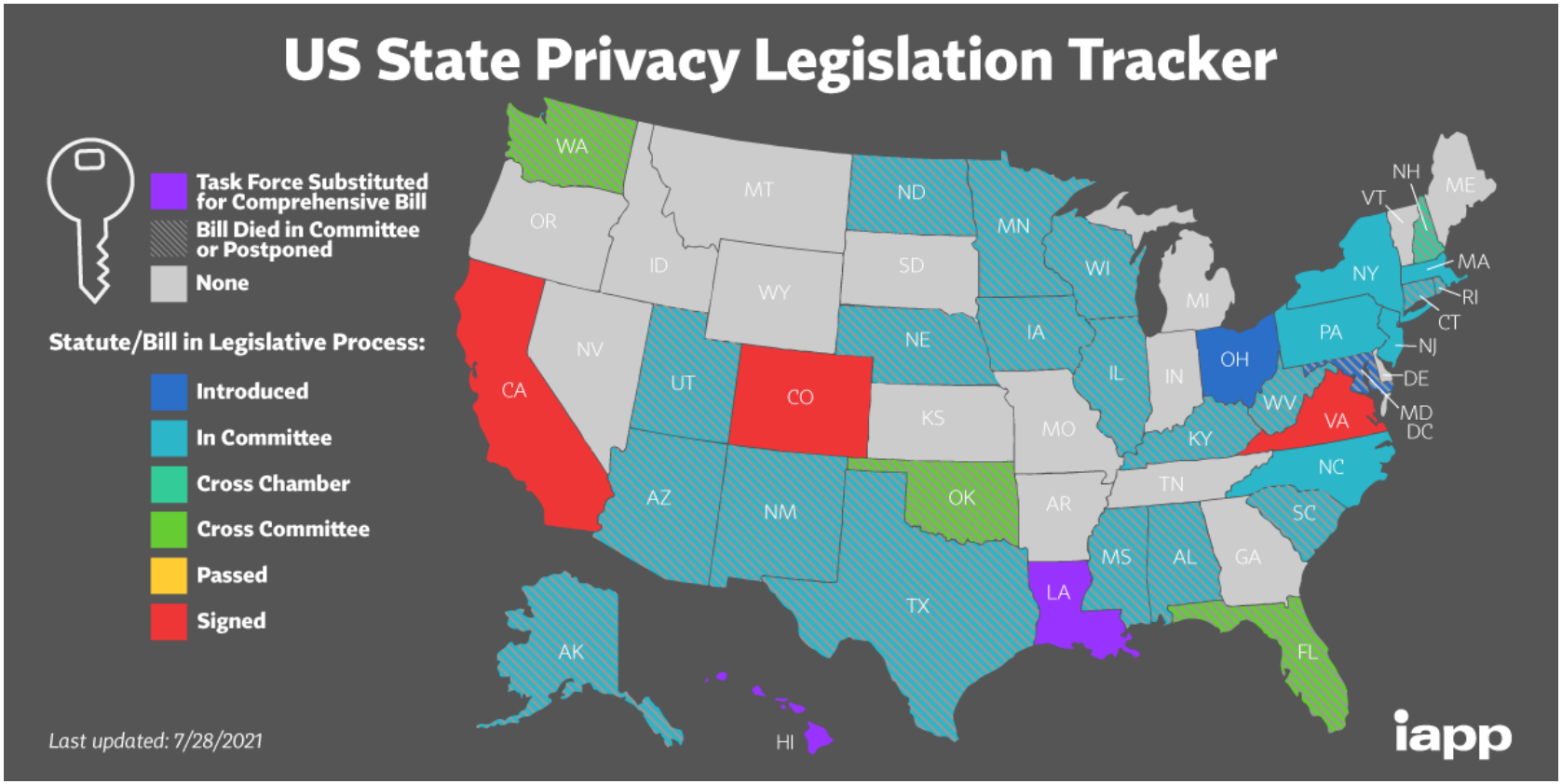
Privacy Laws in Europe

- The introduction of new European Union privacy law had a significant impact on companies world wide
  - EU General Data Protection Regulation (GDPR) was signed into law in 2016 and took effect in May 2018
  - it places users in charge of their data
    - the right to know how their personal data is used
    - the right to data correction and erasure
    - requires explicit consent for data collection
  - privacy policies and personal data use have to be explained in accessible language
- Since its introduction, GDPR had significant impact worldwide
  - violations of that law are common

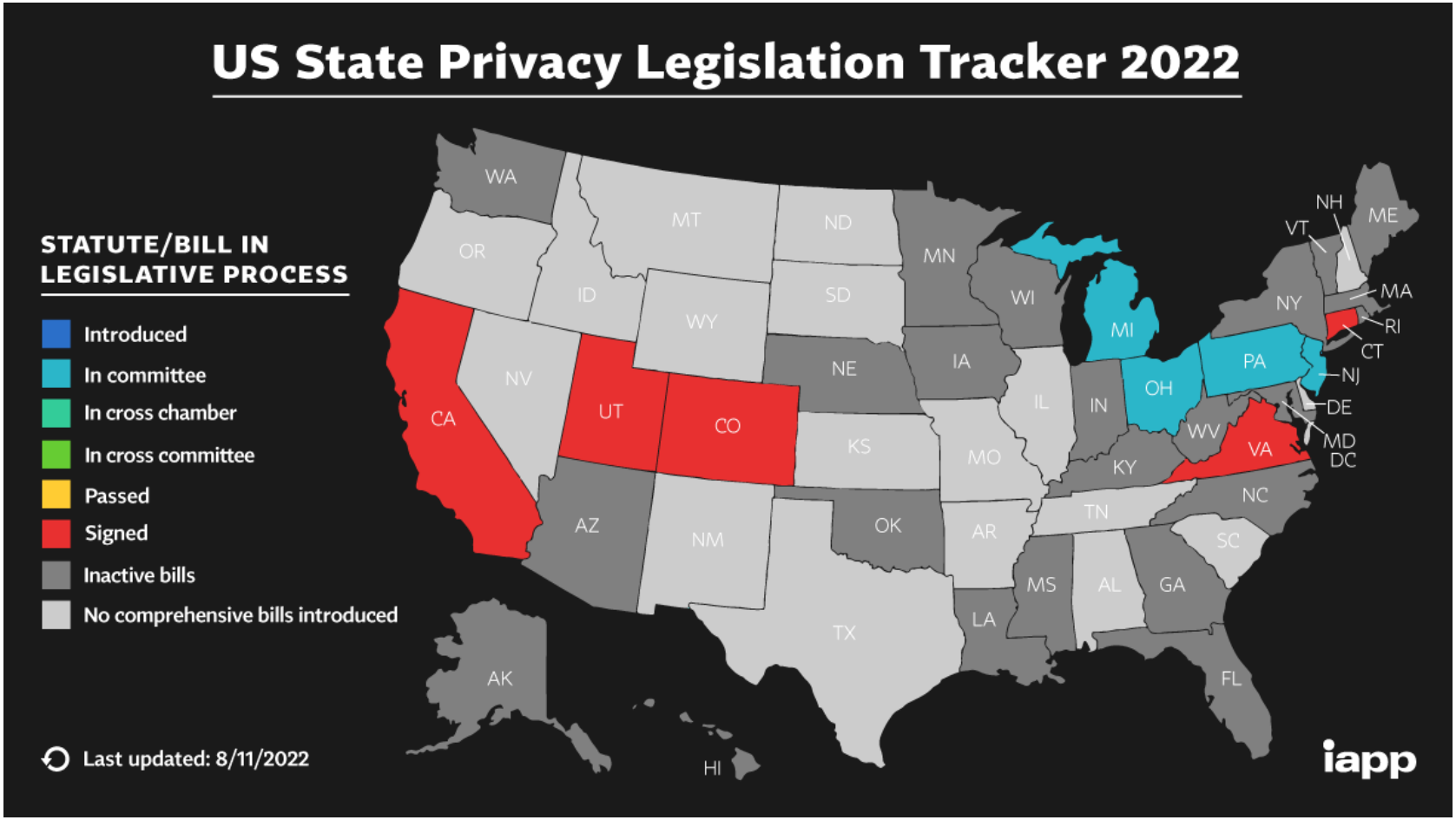
US States Privacy Laws

- California was the first state to offer privacy protection to its residents
  - California Consumer Privacy Act (CCPA) was signed into law in 2018 and took effect in 2020
  - it is the most comprehensive internet-focused data privacy legislation in the US
  - consumers can request access to and deletion of personal information held by businesses
  - businesses cannot sell personal information without
    - providing a web notice and
    - giving an opportunity to opt out
  - CCPA uses a broad notion of personal information and introduces probabilistic identifiers
- A number of other states are following with their own privacy laws

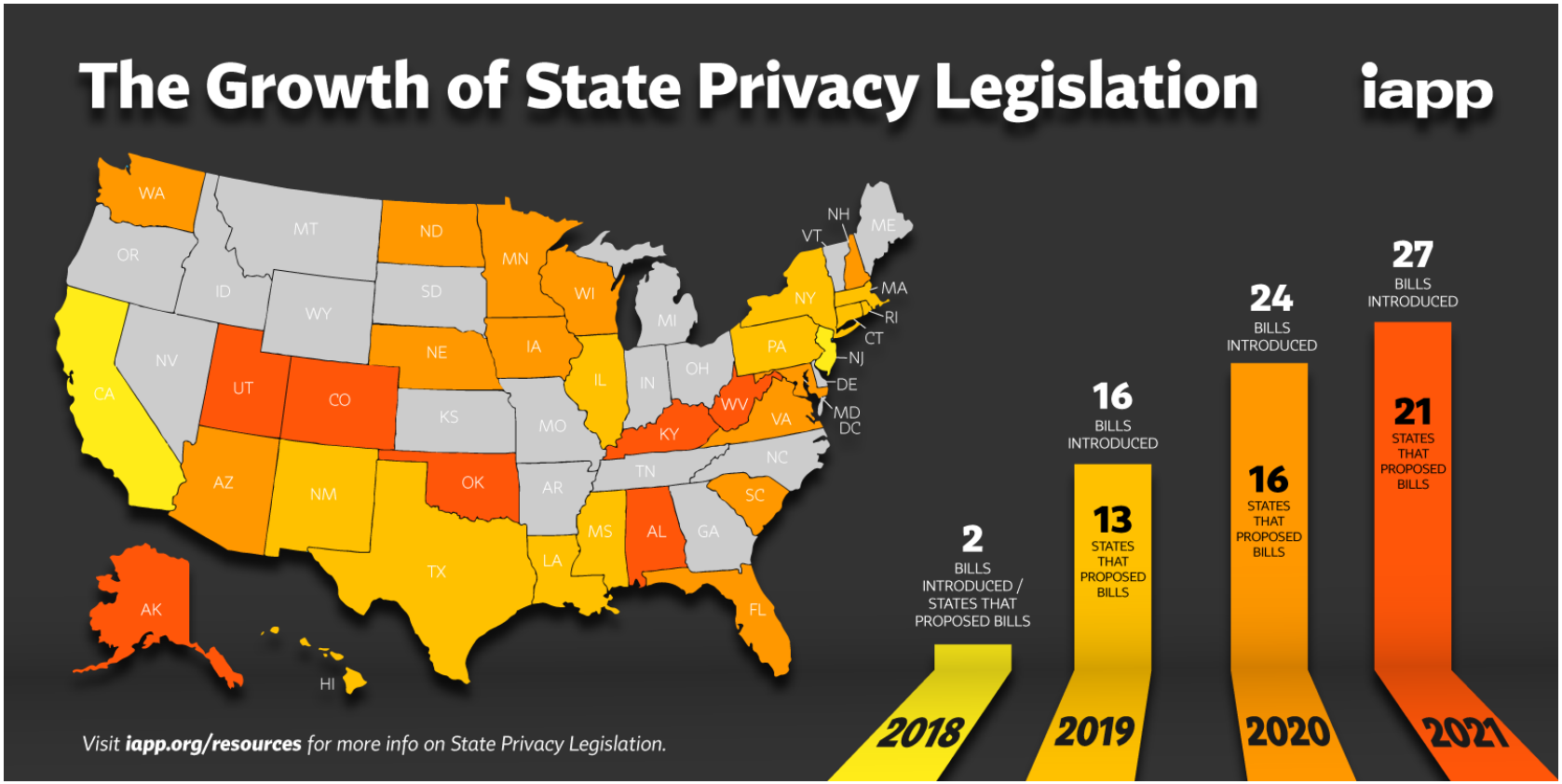
US State Privacy Laws as of 2021



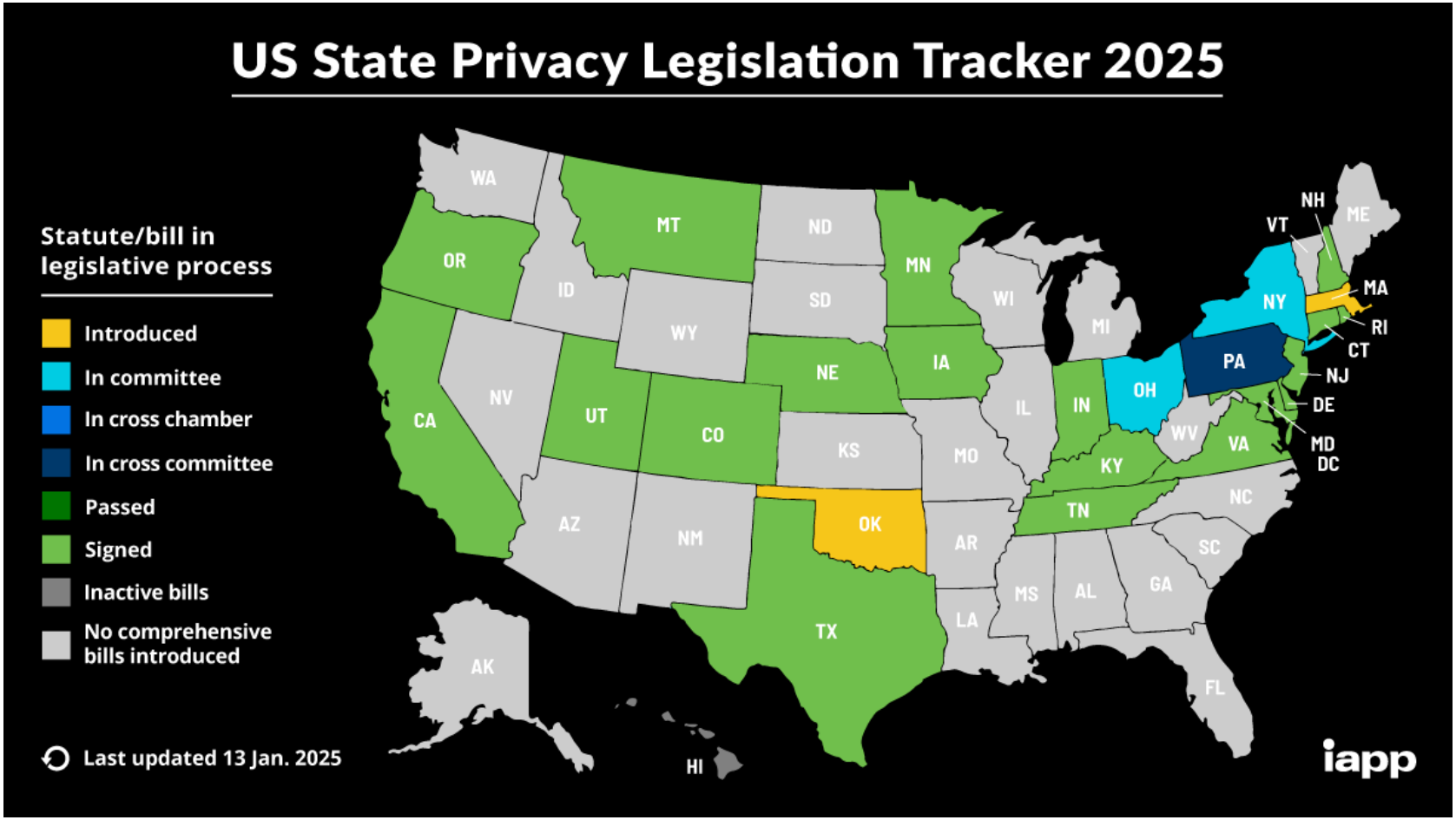
US State Privacy Laws as of 2022



US State Privacy Laws



US State Privacy Laws as of 2025



See https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ for more information

Computer Crime Laws

- Computer crime
  - many types of computer attacks can be considered crimes and carry criminal sanctions
  - the US law and international Convention on Cybercrime categorize computer crime based on the target and actions
- Computers can be used as
  - target of attack
    - illegal access, computer-related forgery or fraud
  - storage device
    - storage of stolen credit cards or other sensitive information
  - communication tool
    - traditional crime committed online (illegal sale of drugs, guns, ...)

Computer Crime

- The nature of computer crime makes investigation very difficult
  - low success rate, achieving a consistent success rate is even harder
- Unique challenges include
  - investigators need to have a good understanding of technology
  - some investigations require significant resources (computing power, storage, or communications)
  - cybercrime is global and might require cooperation of other law enforcement agencies
  - no cybercriminal database to look for likely suspects

Computer Crime

- Low success rate and concerns about corporate reputation result in low reporting rates by cybercrime victims
  - the situation won't improve without cooperation of organizations
  - law enforcement should be viewed as an additional resource in investigation
  - management needs to understand how the investigation process works and positively contribute to the investigation

Summary

Privacy is an important human right, but it is often violated online

Abuses of personal information are common, but there is no legal framework for prosecuting the responsible parties

There is no comprehensive federal data privacy law, and California is the first to pass an internet-focused privacy law