Privacy

INTRODUCTION TO DATA PRIVACY

Tiffany Lewis
Security and Privacy Instructor

datacamp

Privacy's origin story

- 1800s conversations about technology and Privacy:
  - Individuals' rights
  - Sensationalist reporting
- **Privacy** - The right to be left alone, or freedom from interference or intrusion.

[1] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," Harvard Law Review, 4 (5), (1890): 193-220, p. 195, citing Judge Cooley in Cooley on Torts, 2nd ed.

Digging into today's definition of Privacy

- ***Data Privacy*** - control over how personal data is collected and used.
- "The authorized and valid processing of personal information."

[1] Bhajaria, Nishant, and Neil Hunt. Data Privacy: A Runbook for Engineers. Manning Publications Co., 2022.

Personal data

- ***Personal data*** - data related to a person or can be used to identify an individual.
  - Examples:
    - Date of birth (DOB)
    - Name
    - Geolocation
- Goal to keep personal data safe

Privacy's expanding implications

- Increase discussions in 21st-century due to:
  - Internet
  - Applications
  - Larger data footprint
- Privacy concerns include:
  - Surveillance
  - Big data analytics
  - 3rd party providers

State of Privacy today

- 59%+ of Americans do not know what is being done with their data.
- 81% of Americans say that the risks of collecting data about them outweigh the benefits.

- Potential causes:
  - Lack of Privacy knowledge
  - Lack of trust
  - Lack of standardized regulation

Privacy Implications

Privacy has different implications for different groups

Personas	Why Privacy Matters	Consequences
User	• User Trust • Confidence	• Violation of individual's rights • Increased risk of data misuse
Company	• Compliance • Protecting Users	• Financial loss • Legal repercussions
Regulator	• Standardization • Protecting Users	• Loss of public confidence • Exploitation of the public

PREACH

- **P (Purpose)** - Why is the company asking to use your data?
- **R (Right to Request)** - Do you have the ability to request changes to your information?
- **E (Easy to understand)** - Is it easy to understand a company's policies?
- **A (Alerting)** - Will you be alerted if the company mishandles your data?
- **C (Consent)** - Have you given consent (i.e., permission) for your information to be used?
- **H (How)** - How is the company or service planning to use your data?

Let's practice!

INTRODUCTION TO DATA PRIVACY

Security

INTRODUCTION TO DATA PRIVACY

Tiffany Lewis
Security and Privacy Instructor

datacamp

Why are we talking about Security?

- Security is a precursor to Privacy.
- Security and Privacy programs are like an ice cream sundae:
  - Security = ice cream
  - Privacy = toppings

What is Information Security?

> ***Information Security (InfoSec)*** - "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."

[1] https://www.nist.gov/blogs/cybersecurity-insights/next-generation-security-and-privacy-controls-protecting-nations

CIA Triad

- Popular security model
- *CIA Triad* helps companies identify and understand security controls
- **Note:** Many security models exist
  - Example - *DIE*
    - Distributed
    - Immutable
    - Ephemeral

CIA Triad breakdown

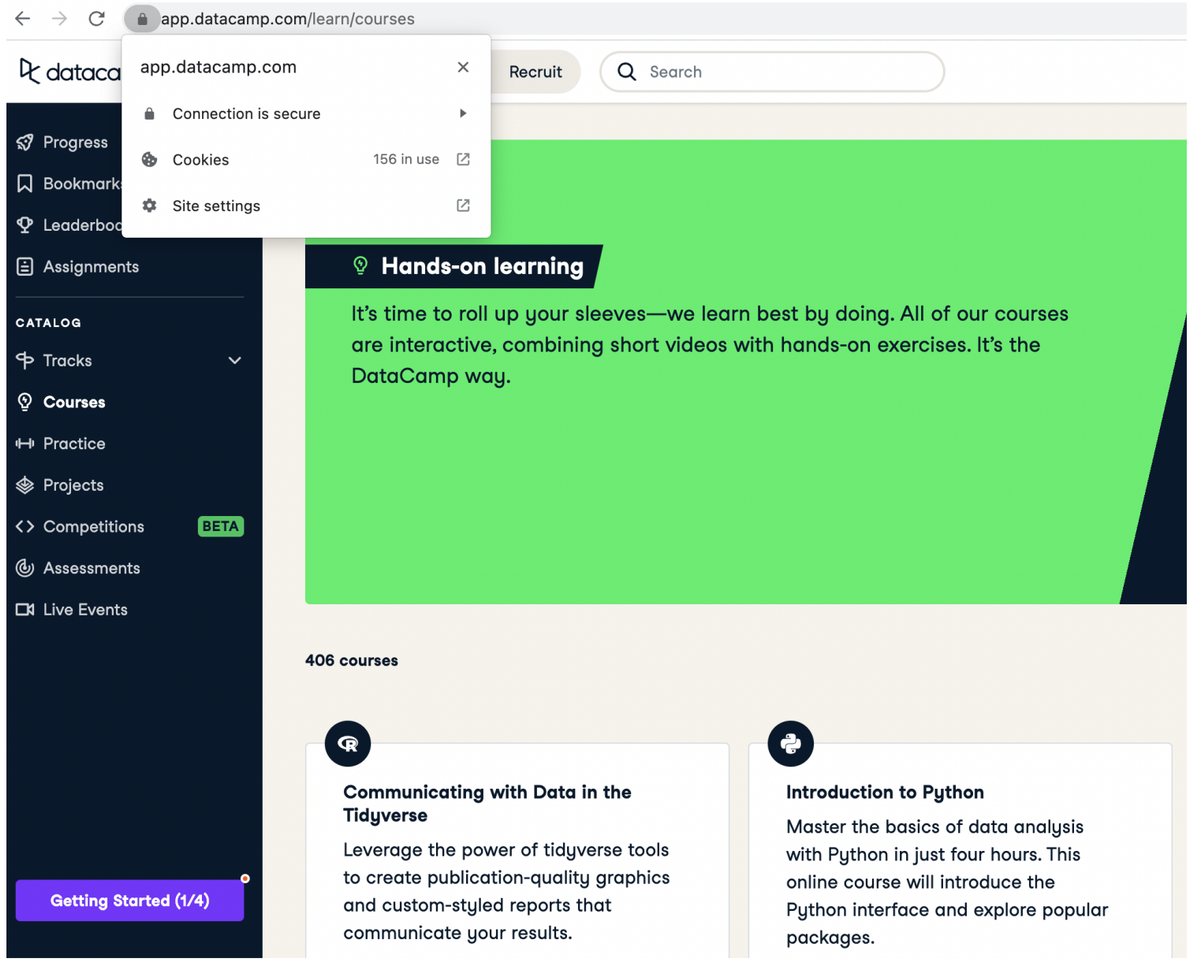
- CIA Triad represents:
  - **Confidentiality** - data is protected and not accessed by unauthorized parties.
  - **Integrity** - data is not altered or modified unexpectedly.
  - **Availability** - data systems are running as expected.

Confidentiality - Identity Access Management (IAM)

- **Confidentiality** system's ability to ensure that only correct users have access to information.
- **Identity Access Management (IAM)**
  - Ensures right people have access to the right resources at the right time.
- Real World Example - Limiting employee access to resources:
  - Company email address
  - Access to corporate network
  - Access during working hours - 8AM to 5PM

Integrity - encryption and hashing

- **Integrity** - data can be trusted and has not been inappropriately modified
  - **Encryption** - is a process that makes readable data undecipherable.
    - "midnight" -> "Y!lay.ig"
  - **Hashing**- converting data to a standardized algorithmic output
- Real World: HTTPS communications



Availability - Business Continuity and Disaster Recovery

- **Availability** systems are accessible and available.
- **Business Continuity and Disaster Recovery (BCDR)** the processes, policies, and people used to help an organization continue during an unplanned event.
- Example - Flood damages data center

Let's practice!

INTRODUCTION TO DATA PRIVACY

The relationship between Security and Privacy

INTRODUCTION TO DATA PRIVACY

Tiffany Lewis
Security and Privacy Instructor

datacamp

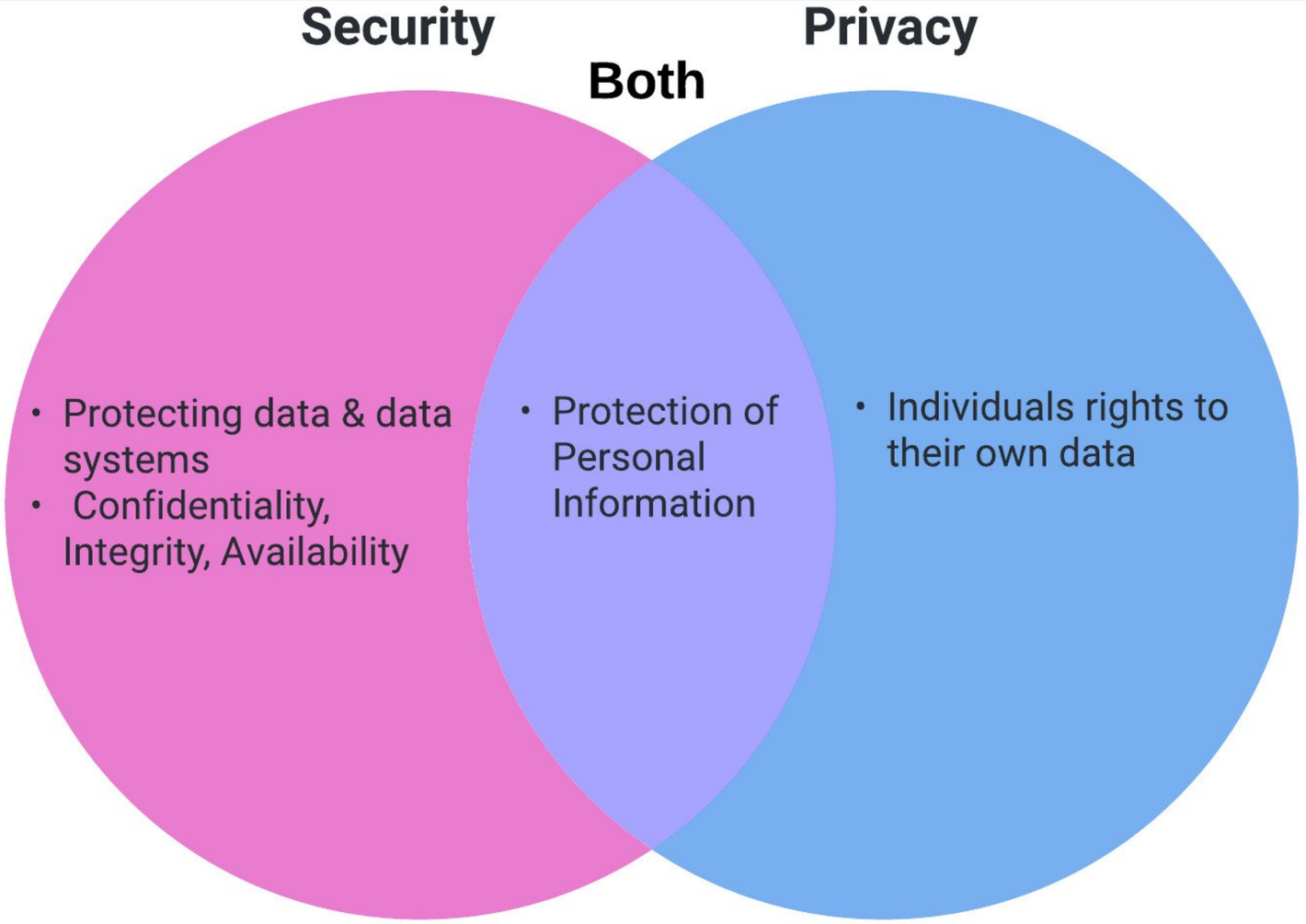
Security fundamentals

- Preventing unauthorized use, disclosure, and alteration of data:
  - CIA Triad
- Examples:
  - Encryption
  - Identity Access Management

Privacy fundamentals

- Data processed in a valid manner that has been authorized by the user
- Examples:
  - Notifications
  - Encryption

Security and Privacy Venn diagram



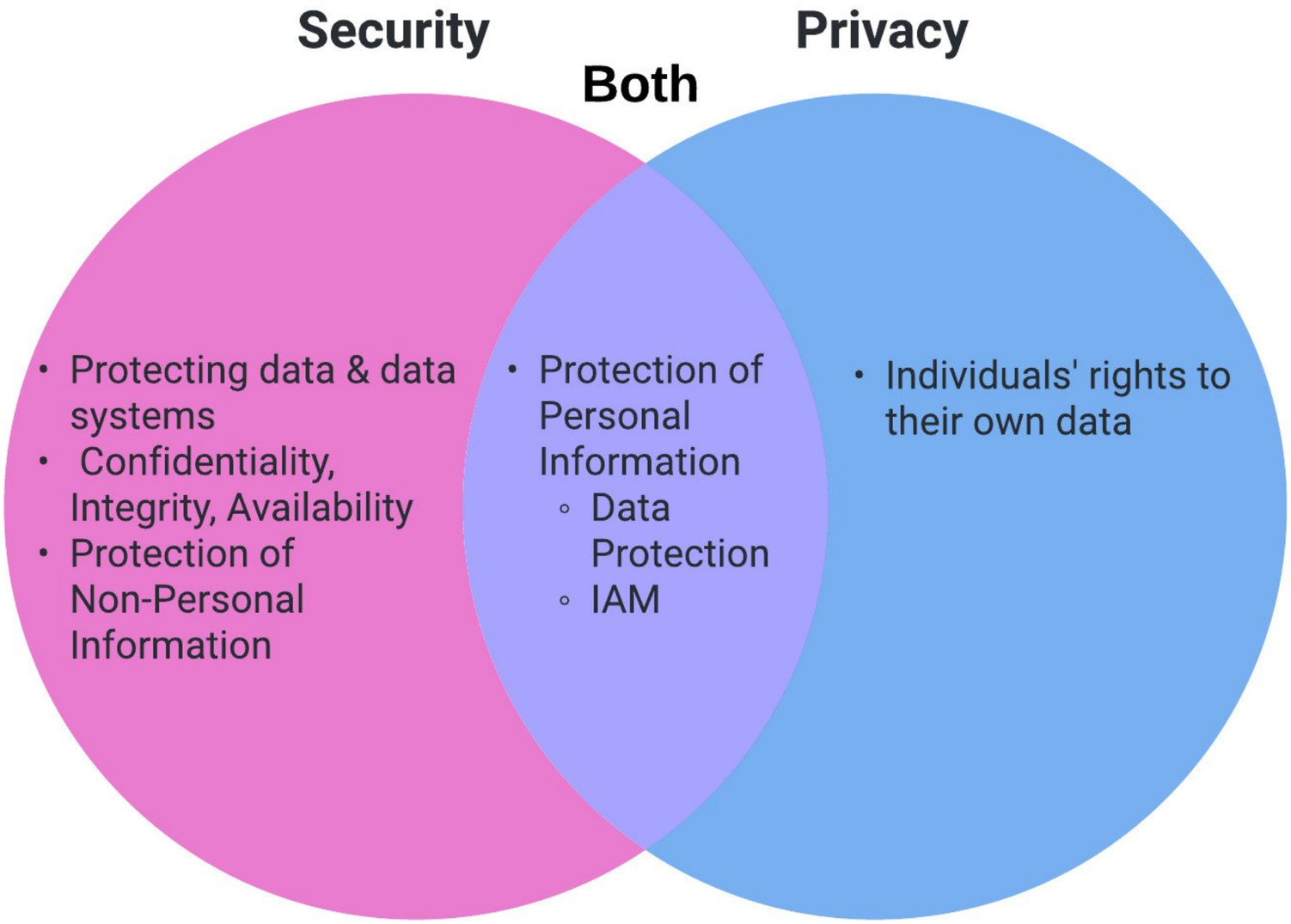
Packing what we've learned

- Backpack startup
- Security and Privacy concerns
- Analyze:
  - Product data
  - Personal information

Security Controls

Privacy Controls

Security and Privacy Venn diagram



Security and Privacy failure

- Privacy requires explicit authorization from users to:
  - disclose
  - alter
  - change how data is used
- Stolen data - no consent or authorization from users

Data breach

> **Data Breach** - a security event where data is unlawfully disclosed, altered, or taken by an unauthorized party.

- Example: Yahoo data breach in 2013
  - Affected over 3 billion users
  - Hackers attempted to sell the data

[1] https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html

Let's practice!

INTRODUCTION TO DATA PRIVACY