

Companies and user data

INTRODUCTION TO DATA PRIVACY



Tiffany Lewis

Security and Privacy Instructor

Investigating the types of data companies collect

- **Personal data** - info about users
- **Engagement data** - how users interact
- **Behavioral data** - what users do
- **Attitudinal data** - how users feel



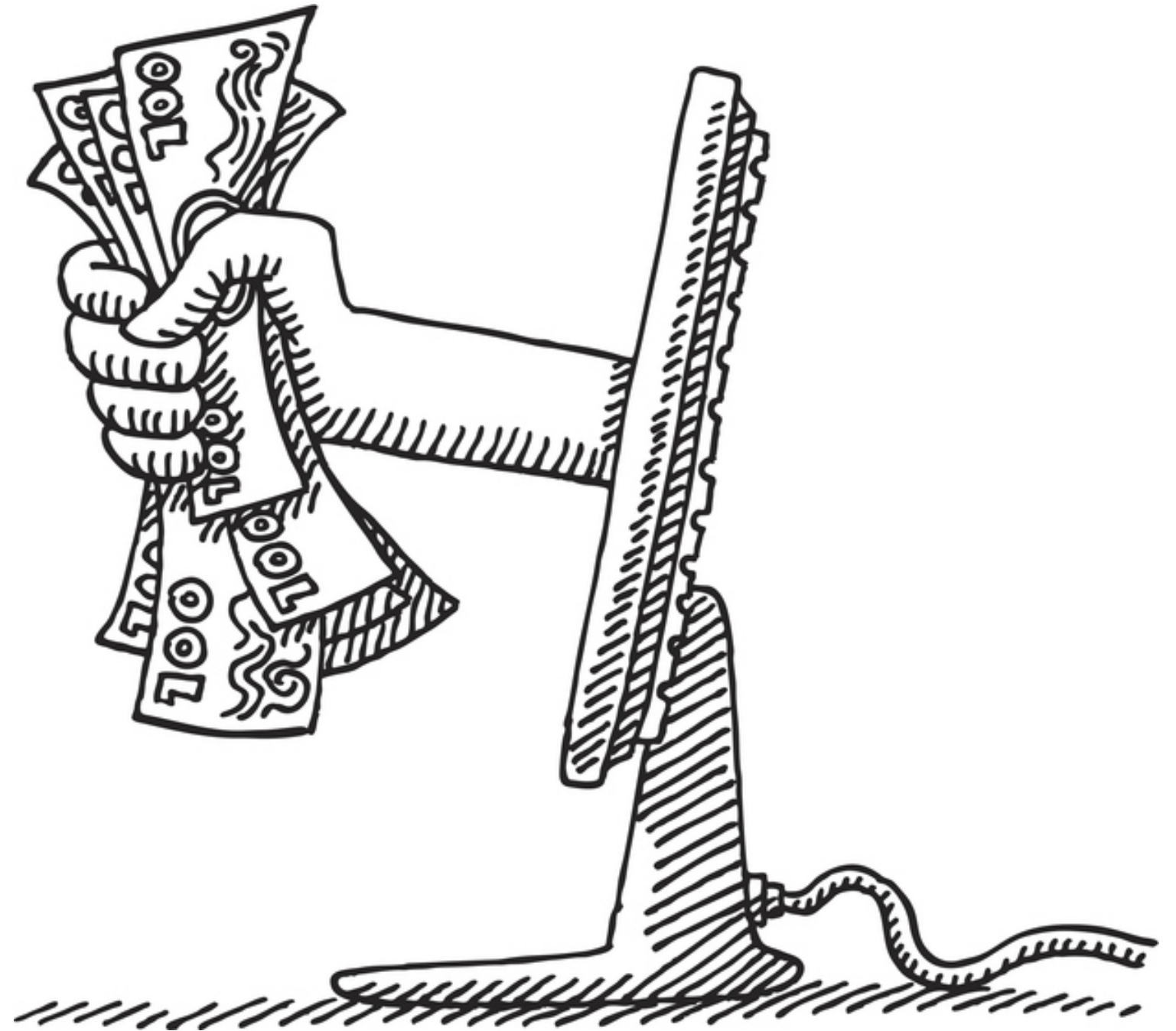
Why do companies want user data?

- Analyze user information
 - Informs business decisions
- Knowledge is power... so is data



What do companies do with the data?

1. Optimize customer experience
2. Targeted advertising
3. Resell the data
4. Product development
5. Improve business strategy



User experience and product development

- Understand the user base and their preferences
- Modify products, goods, and services for better user preference alignment



Resell data

- **Data broker** an entity that collects information about users and then sells the information for profit.
 - Selling the data
 - Creating customer profiles
- Example: Databroker creating diabetics profiles and reselling them to health insurance companies.



Targeting advertising

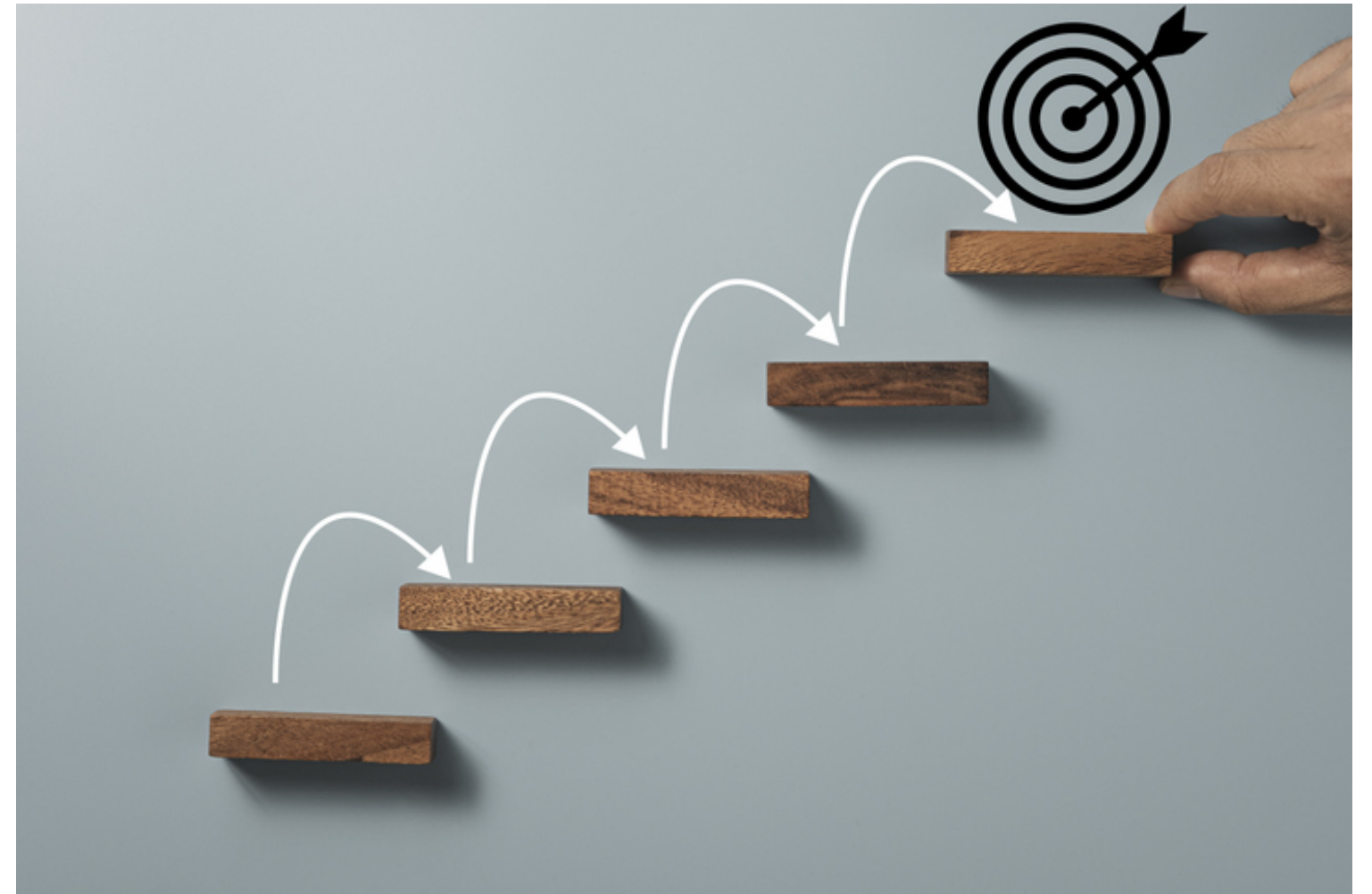
- Hundred billion(s) industry
- Nothing is free... even "free" services
- How it works
 - Sell advertising spots
 - Personalized ads based on profiles
- Example: Finding ads on different websites based on online product searches.






¹ <https://www.statista.com/statistics/261827/leading-media-companies-worldwide/>

Improve business strategy

- Tracking user footprint
 - Spending habits
 - Competitor platforms
 - User preferences
- Helps company make business and investment decisions



Frequent flyer program example

Scenario	Benefit	Privacy Tradeoff
<p>An airline is running a promo for customers who sign up for their frequent-flyer program.</p> 	<ul style="list-style-type: none">• Future exclusive discounts• Free perks• Free upgrades• Status points 	<ul style="list-style-type: none">• Potential third party compromise• Potential increase advertising and spam• Information resold 

Let's practice!

INTRODUCTION TO DATA PRIVACY

Privacy laws - when things go wrong

INTRODUCTION TO DATA PRIVACY



Tiffany Lewis

Security and Privacy Instructor

When things go wrong

- Impact to users when things go wrong:
 - Targeted selling
 - Information stolen
 - Identity stolen
 - Pricing discrimination



Data paradox

- Increased dependence on technology = Increased concern about privacy
- Correlation between user privacy and technology usage
- Data Privacy Paradox



¹ Chen, Long and Chen, Long and Huang, Yadong and Ouyang, Shumiao and Xiong, Wei, The Data Privacy Paradox and Digital Demand (May 2021). NBER Working Paper No. w28854, Available at SSRN:

Penalties for violating privacy policies

- Financial damages
- Business ban
- Miscellaneous penalties
 - Fines
 - Creation of mandated privacy programs
 - Incarceration
 - And more...



Privacy laws - compliance chart

Legislation
GDPR
CCPA
PIPL

Privacy laws and jurisdiction - compliance chart

Legislation	Jurisdiction*
GDPR	EU (applies to EU citizens)
CCPA	California (applies to CA residents)
PIPL	China (applies to Chinese citizens)

Compliance and privacy chart

Legislation	Jurisdiction*	Potential Penalty
GDPR	EU (applies to EU citizens)	Up to €10 million or up to 4% of the company's worldwide annual revenue. Whichever is highest
CCPA	California (applies to CA residents)	No cap fined per penalty. \$2500 for every unintentional violation and \$7,500 for intentional penalty after 30 days
PIPL	China (applies to Chinese citizens)	Up to \$7.8 million USD or up to 5% of a company's previous year's business revenue.

Real world privacy violations

Legislation	Company	Violation	Penalty
GDPR	Amazon	Targeted advertising carried out without user free consent	\$888M USD
CCPA	Sephora	Failed to notify customers that their data was being sold	\$1.2M USD
PIPL	Didi Int	Violated 16 different rules	\$1.2B*

Let's practice!

INTRODUCTION TO DATA PRIVACY

Spooky Privacy laws

INTRODUCTION TO DATA PRIVACY



Tiffany Lewis

Security and Privacy Instructor

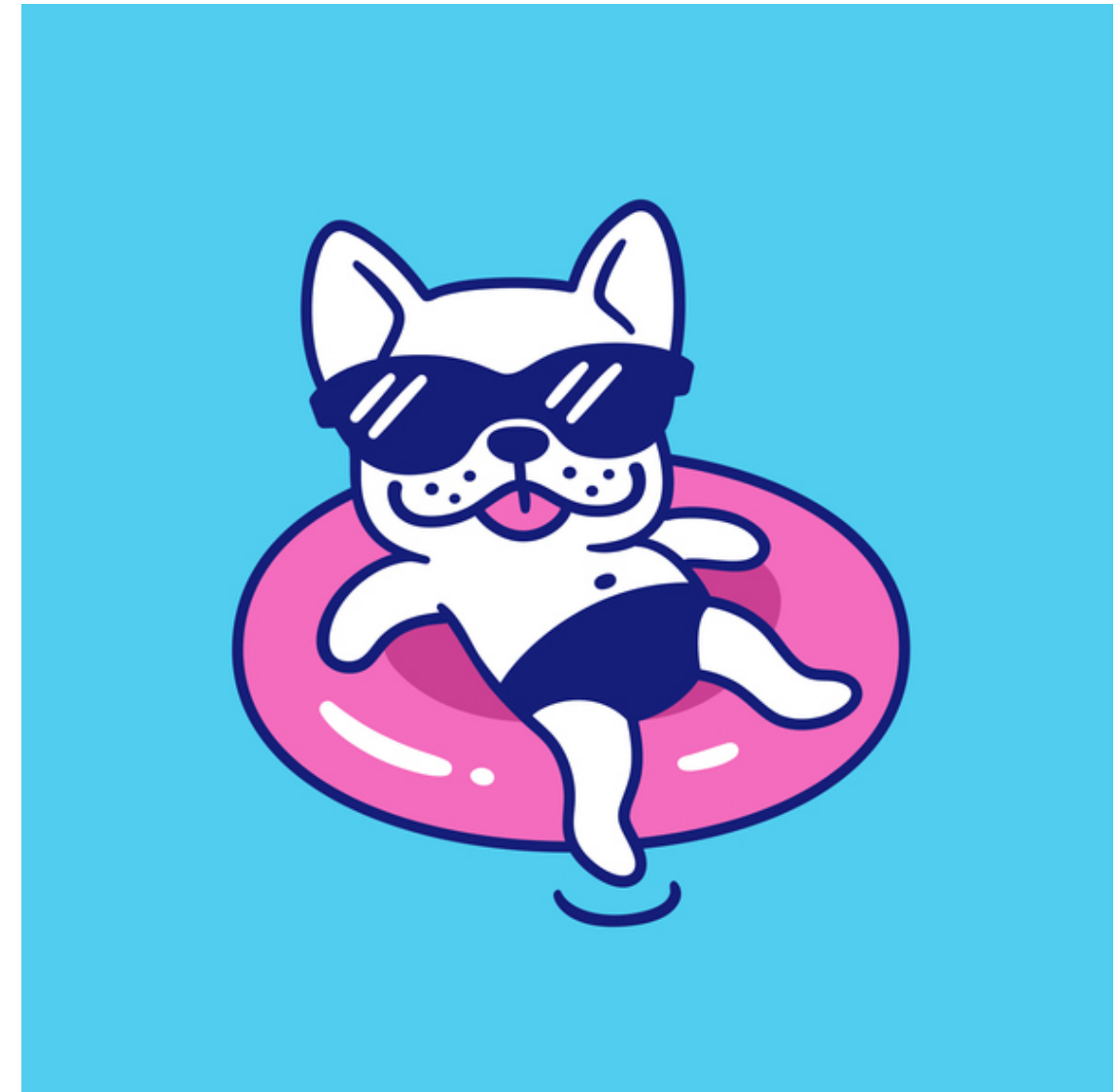
Sometimes rules are good

- Companies cannot go unchecked
- Need rules to protect consumers
- Standardization
- Legal protection



Trends

1. Data Sovereignty
2. Data Breach Notifications
3. User Data Requests
4. Increased Transparency
5. Accountability



¹ <https://www.gartner.com/en/newsroom/press-releases/2022-05-31-gartner-identifies-top-five-trends-in-privacy-through-2024>

Components of Privacy law (jAsper)

- (j)urisdiction
- (A)uthor and Aim
- (s)cope
- (p)enalty
- (e)nforcement
- (r)equirements



jAsper template

<Insert Regulation Name>	
Concept	Response
jurisdiction	
Author + Aim	
scope	
penalty	
enforcement	
requirements	

HIPAA	
Concept	Response
jurisdiction	USA
Author + Aim	Congress + Protecting sensitive patient healthcare information and prevent unauthorized disclosure
scope	Organizations that store, process, or transfer PHI
penalty	Criminal and Civil penalties
enforcement	Office of Civil Rights (OCR)
requirements	5 Rules

Privacy law challenges

- Moving target
- Subject matter expertise
- Lack of global privacy alliances
- Lack of standardization



Let's practice!

INTRODUCTION TO DATA PRIVACY

Bleeding edge Privacy topics

INTRODUCTION TO DATA PRIVACY



Tiffany Lewis

Security and Privacy Instructor

Shifting left

- Sooner better than later
- Not limited to privacy
- Privacy by Design
 - Encourages shifting left



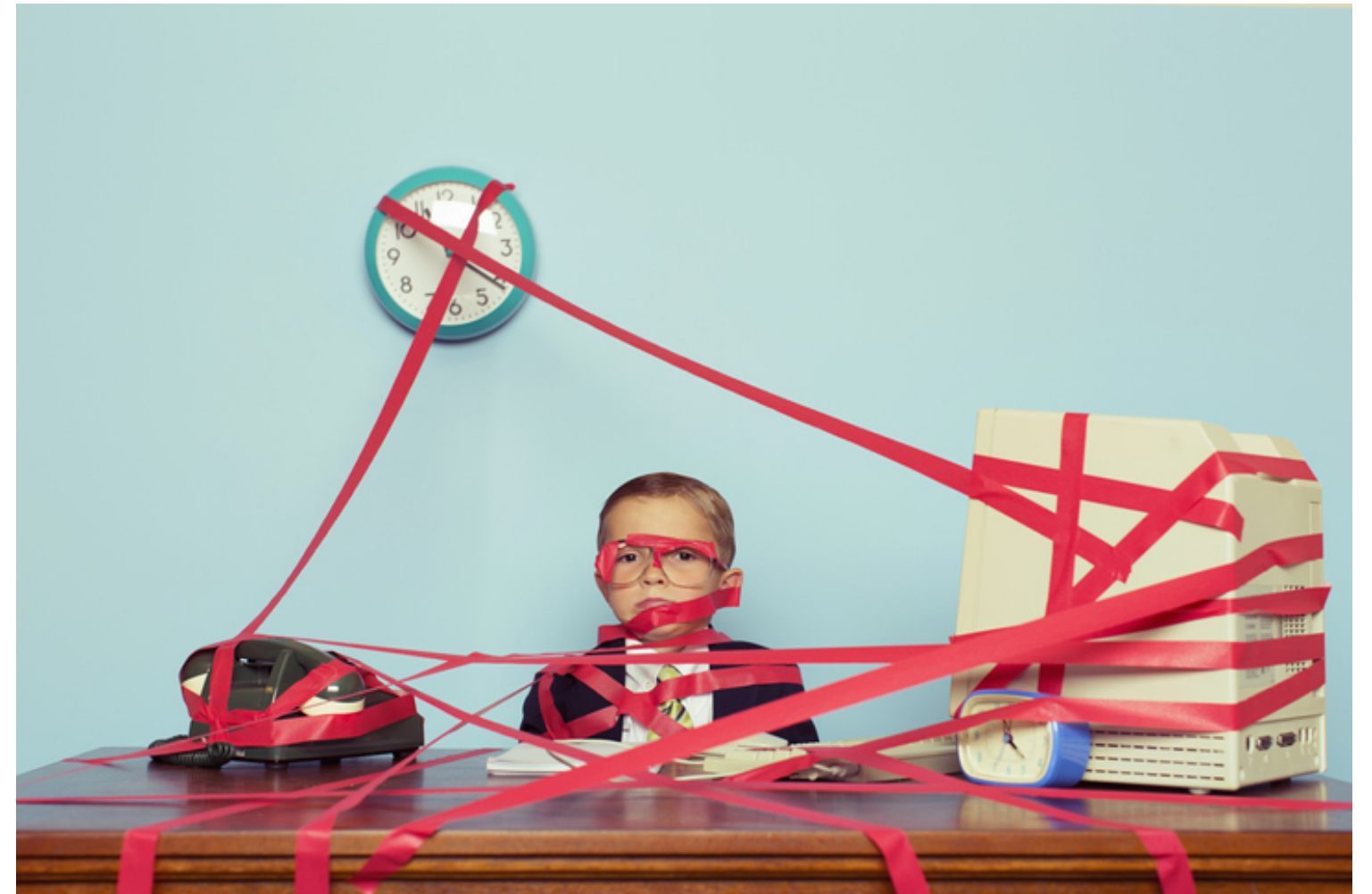
Bleeding edge

- Cutting edge technology
- Shiny and sharp
 - Possibility to innovate and improve
 - Lack of established best practices
- Example of bleeding edge technology: Ironman or Ironheart's suits



Bleeding edge challenges

- Only consistency is change
- Existing privacy and security controls may not sufficiently address risk
 - May need to create new controls and processes
- Lag between regulation and tech
 - Laws
 - Certifications



Bleeding edge technology - public cloud

- Public cloud over a decade old
- Consumable on demand infrastructure
- Shift from buying hardware to buying usage
- Cloud Service Providers (CSPs)
 - Google Cloud Platform (GCP)
 - Amazon Web Services (AWS)
 - Azure



Public cloud benefits and challenges

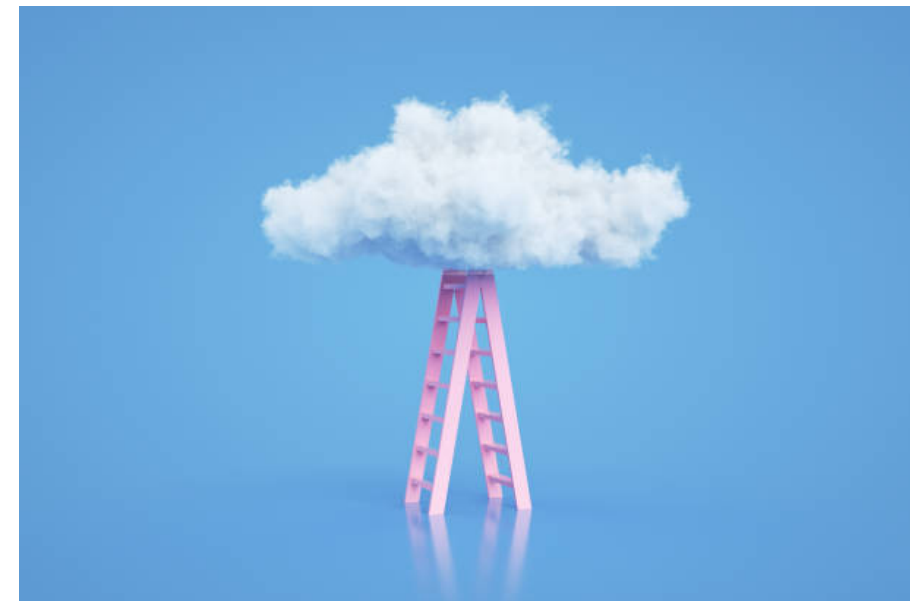
Benefits:

- Scale resources to meet demand
- Decrease hardware investment
- Faster innovation



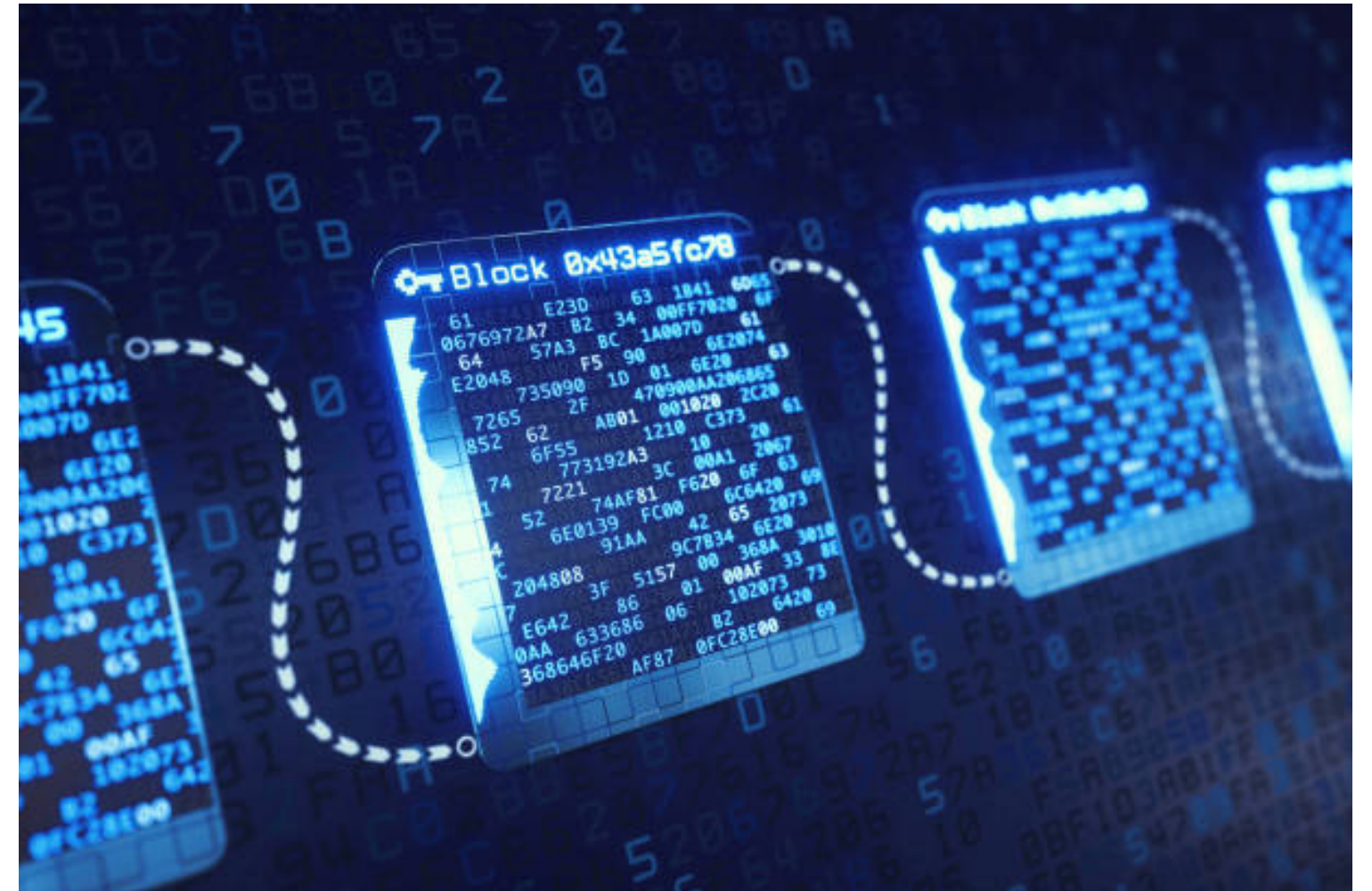
Challenges

- Creating new privacy and security controls
- Training



Bleeding edge technology - blockchain

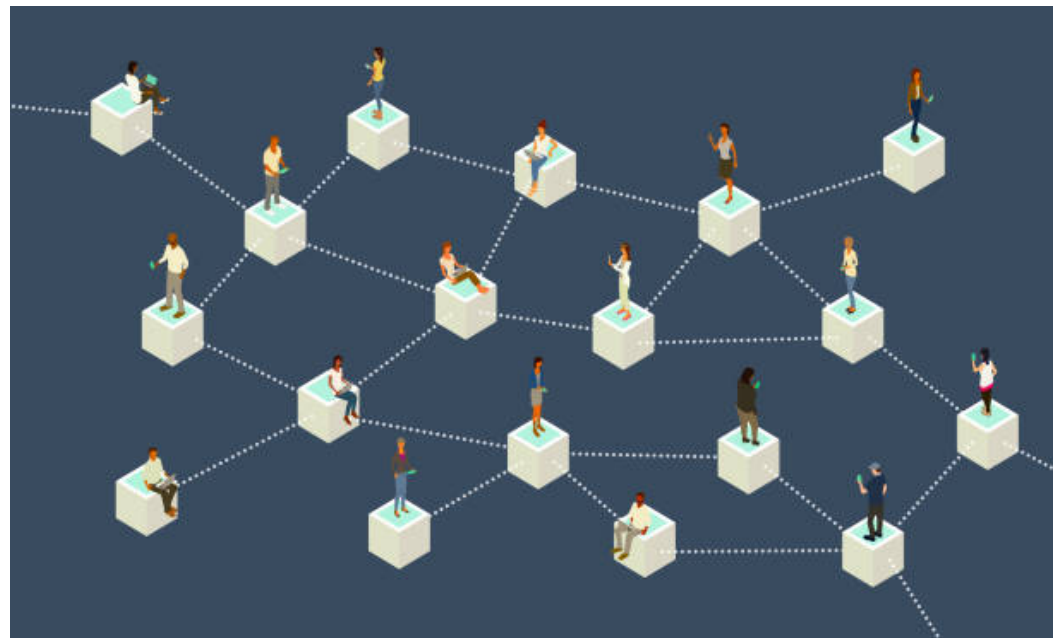
- Shared ledger that records transactions and assets
- Built across distributed systems
- "block" and block chains
 - Data groupings chained to one another
- Examples:
 - Cryptographic currency
 - Next wave of the Internet (web3, web5)



Blockchain benefits and challenges

Benefits

- Immutability
- Transparency and speed
- Security



Challenges

- User deletion requests
- Mapping to pre-existing to privacy laws



Let's Practice

INTRODUCTION TO DATA PRIVACY

Congratulations!

INTRODUCTION TO DATA PRIVACY



Tiffany Lewis

Security and Privacy Instructor

Recap

Congrats!

Should have a strong understanding of:

- Privacy and Security basics
- Privacy by Design
- Overlap between Privacy and Security
- Foundational components of Privacy laws
- Bleeding Edge Technology and Privacy
- Why companies collect data
- Why privacy matters



Congratulations!

INTRODUCTION TO DATA PRIVACY