THE BRAVE NEW WORLD OF

PRIVACY

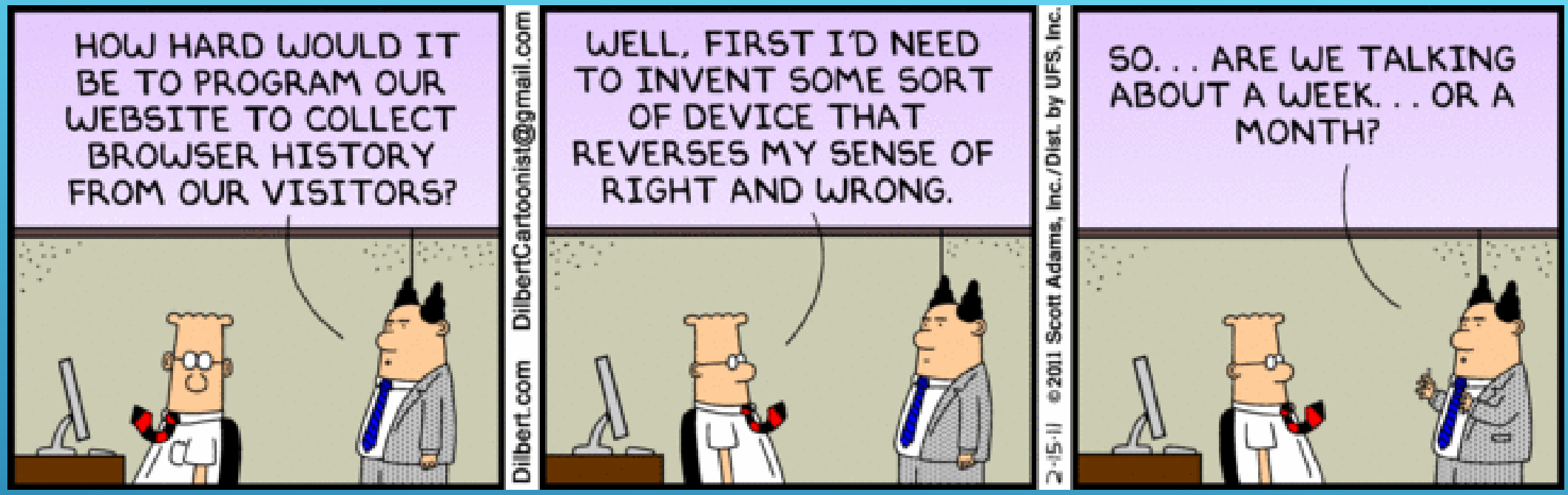
Understanding the intersection of regulated and unregulated data assets in a Privacy-focused world

SPEAKER: SABINO MARQUEZ

- Chief Information Security Officer and Privacy Director for Allocadia, Inc.
- Privacy Evangelist & Defender (capital-P and lowercase-P)
- Longtime Hacker, Penetration Tester, Social Engineer, Historian, Philosopher, & Fanatical Defender of Stakeholder Value
- Historian, Researcher, Author

CAPITAL-P PRIVACY

Data Assets Specifically Regulated For Privacy

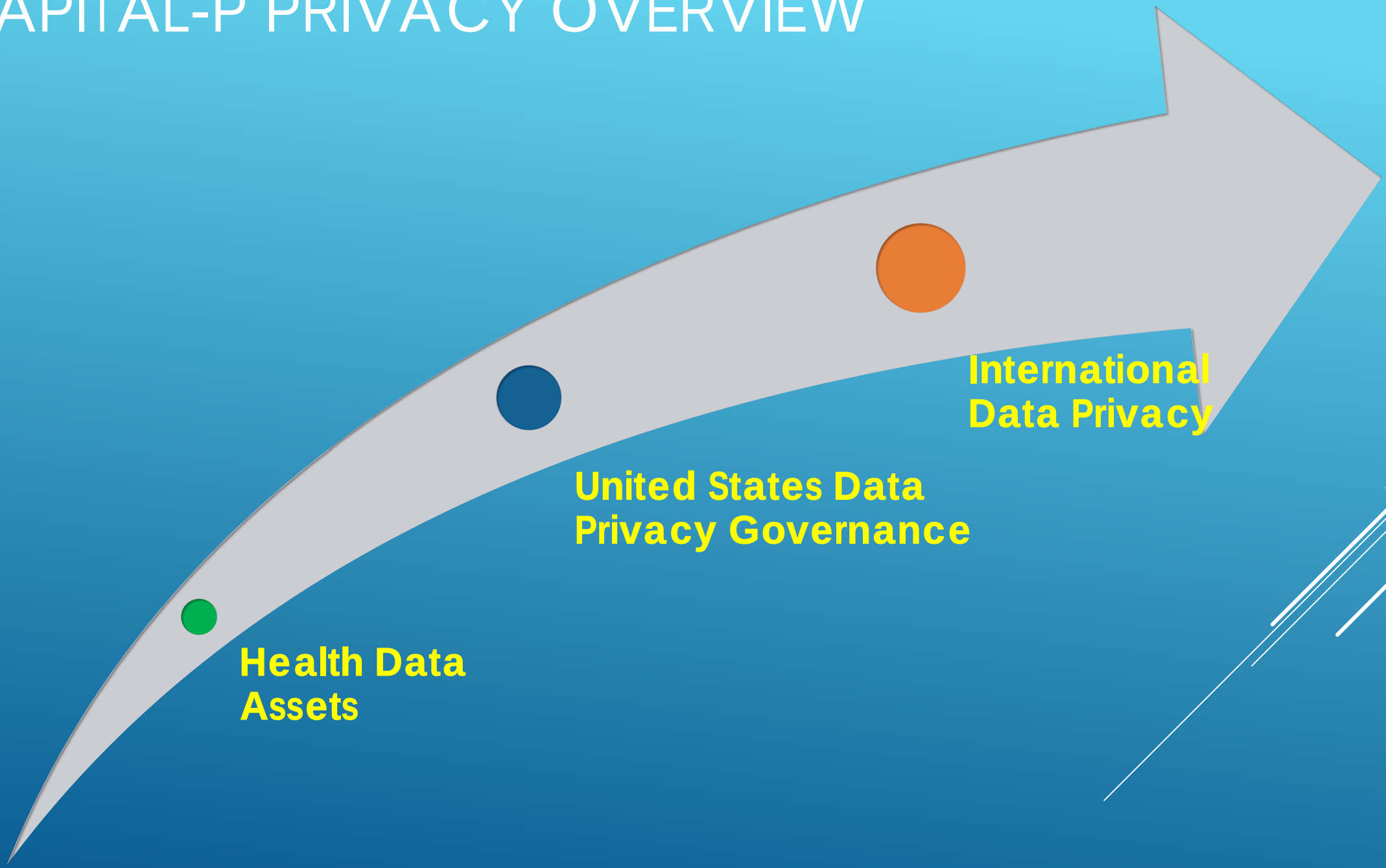


A BRIEF STROLL THROUGH THE HISTORY OF DATA PRIVACY PROTECTIONS

DEFINITIONS

- Privacy
- Information Privacy
- Capital-P Privacy
- Lowercase-P Privacy
- Surveillance
- Information Security

CAPITAL-P PRIVACY OVERVIEW



CAPITAL-P PRIVACY OVERVIEW

HEALTH DATA ASSETS

- Let's start with something near and dear: **HIPAA & HITECH**
  - Rationale for protected data asset class
  - The Security Rule and The Privacy Rule
  - HITECH expansion of the Rule to BA's
  - Breach Notification Rule (Omnibus)
  - HIPAA/EDI, Stringent Programming and Data Flow / Hygiene Requirements
  - Defined, Proscribed, Auditable, and Non-Compliance Consequences Severe Enough To Drive Strategy

CAPITAL-P PRIVACY OVERVIEW

Statute	Data Asset Class
Fair Credit Reporting Act (FCRA) & Fair Debt Collection Practices Act (FBCPA)	*Limited privacy control over consumer credit data handling*
FTC Health Breach Notification Rule	*Privacy Breach Notification requirement for vendors of personal health records and related entities*
FTC Act	*Enforces commercial privacy commitments*
Children's Online Privacy Protection Act (COPPA)	*Internet Users 13 yrs & younger*
GLBA Privacy (15 U.S.C. §§ 6801–6809)	*Consumer Financial Data*
Family Educational Rights and Privacy Act (FERPA)	*Limited privacy defense for academic and student records*
Privacy Act of 1974	*PII in Federal Systems*

CAPITAL-P PRIVACY OVERVIEW

- What Do All These Statutes Have In Common?
  - Identifying Privacy-Impacted Data Asset Classes
  - Mandating Privacy Governance over those assets
  - Elevating Accountability to the Executive
  - Establish Corrective Procedures for non-compliance

CAPITAL-P PRIVACY OVERVIEW

The FTC Enforcement Bottleneck

- The FTC has brought a number of enforcement actions against mobile app developers and others in the industry for unfair or deceptive acts or practices in violation of the FTC Act, COPPA, and the FCRA.
- The FTC's Enforcement priorities are generally targeted:
  - Failing to adhere to privacy- or security-related representations
  - Collecting children's personal information without first notifying parents and obtaining their consent
  - Mobile device tracking without consent
- The regulatory climate is trending towards looseness in the short term. Caveat Emptor.
- **Hole in the system**: FTC only regulates commercial violations. You can sign privacy rights away in a contract, and if done right the FTC has no remedy.

CAPITAL-P PRIVACY OVERVIEW

FTC enforcement actions involving **privacy** misrepresentations

- **Path, Inc**. (**social networking app**—deceptive representations in user interface and privacy policy regarding the collection of personal information from users' mobile device contacts; also violated COPPA)
- **Goldenshores Techs., Inc.** (**flashlight app**—failed to adequately disclose that precise geolocation and persistent device identifiers were transmitted to various third parties, including advertising networks, when users ran the app, and misrepresented how much control users had over the collection and use of their data)
- **Snapchat, Inc.** (**photo messaging app**—deceptive representations about the disappearing nature of messages sent through the app, the amount of personal data collected, the collection of geolocation information, and security measures)

CAPITAL-P PRIVACY OVERVIEW

FTC enforcement actions involving **security** misrepresentations

- **Fandango, Inc.** (**movie ticketing app**—deceptive representations about security when, among other things, the developer overrode default SSL certificate validation settings without implementing other security measures)
- **Credit Karma** (**credit monitoring app**—same as above)
- **Equiliv Investments, LLC** (app developer **falsely marketed** an app as free from malicious software or viruses even though the purpose of the app was to load consumers' mobile phones with malicious software in order to mine virtual currencies)

CAPITAL-P PRIVACY OVERVIEW

Definition: The "Right To Privacy"

The Right to Privacy is our right to keep a domain around us, which includes all those things that are part of us, such as our body, home, property, thoughts, activities, feelings, secrets and identity.

The right to privacy gives us the ability to choose which parts in this domain can be accessed by others, and to control the extent, manner and timing of the use of those parts we choose to disclose.

CAPITAL-P PRIVACY OVERVIEW

- The ”Right To Privacy” in the United States
  - The U. S. Constitution contains no express right to privacy.
    - Privacy Rights are implied in other amendments (subject to Supreme Court Interpretation), such as:
      - Privacy of beliefs (1st Amendment),
      - Privacy of the home against demands that it be used to house soldiers (3rd Amendment),
      - Privacy of the person and possessions as against unreasonable searches (4th Amendment), and
      - The 5th Amendment's privilege against self-incrimination, which provides protection for the privacy of personal information.
  - Some States grant Privacy Rights
    - Alaska, California, Florida, Montana, Washington
    - Laws tend to be reactionary. There are no Privacy Visionaries.
  - Exemptions
    - Law Enforcement
    - National Security
    - There is no incentive at any level to grant citizens Constitutional Privacy rights

CAPITAL-P PRIVACY OVERVIEW

- The "Right To Privacy" in other countries
  - **Europe**: UN Human Right, and The General Data Protection Regulation (GDPR)
    - Any state interference with a person's privacy is only acceptable if three conditions are fulfilled:
      - The interference is in accordance with the law
      - The interference pursues a legitimate goal
      - The interference is necessary in a democratic society
  - **Canada**: Privacy is a Human Right in the Charter, enforced through the Privacy Act, PIPA, and PIPEDA

Communications & Engagement	1. My organization is transparent about what it does with privacy-impacted data assets, and employee and customer information
	2. My organization is quick to respond to a privacy complaint, or from privacy questions from customers and regulators.
	3. My organization makes substantial effort to educate employees about data privacy, data security, and information risk management practices.
	4. Employees in my organization understand the importance of data privacy, both to the business and individually, and know how to protect sensitive and confidential data assets.
Business Operations	5. My organization considers privacy and the protection of personal information and privacy-impacted assets as a strategic corporate priority.
	6. A high-level executive leader is accountable for my organization's privacy program, works to remove obstacles to privacy program adoption, and is empowered to make decisions.
	7. My organization understands global Privacy cultural differences and has business plans to navigate them for the benefit of the stakeholder.
	8. My organization strictly enforces all levels of non-compliance with laws and regulations.
Data Protection	9. My organizations' leadership believes that a data breach event would adversely and materially affect our reputation and financial position.
	10. My organization has ample resources to protect employee and customer data, and can prove assurance outside of audit periods.
	11. My organization is able to quickly detect and prevent the theft or misuse of privacy-impacted data assets.
	12. My organization has the expertise and technology to protect privacy-impacted assets.

3 MINUTE BREAK

Next Up: Lowercase-P Privacy

Stretch

Drink

Chat

LOWERCASE-P PRIVACY

Everything changed when no one was looking, and now there’s no going back.

A BRIEF HISTORY OF LOWERCASE-P PRIVACY

LOWERCASE-P PRIVACY OVERVIEW

1. The History of LCPP
2. The Business of Data Analytics
3. The Technology of Data Analytics
4. The Privacy Risks of Mobile Apps
5. The Compromised Web Browser
6. Social Networks: Surveillance as a Service
7. Smart Homes, Appliances, and Wearables
8. AI, Perfect Pricing, & The Self-Perfecting Data Model

LOWERCASE-P PRIVACY OVERVIEW

The History of LCPP

1. Gaps in Regulation despite abuses.
2. Creation of new Platforms/Markets (Mobile, Internet)
3. Technology to digest, analyze, and provide insight on unimaginably huge and unstructured data sets at cloud scale.
4. A Culture that forces it all along.

LOWERCASE-P PRIVACY OVERVIEW

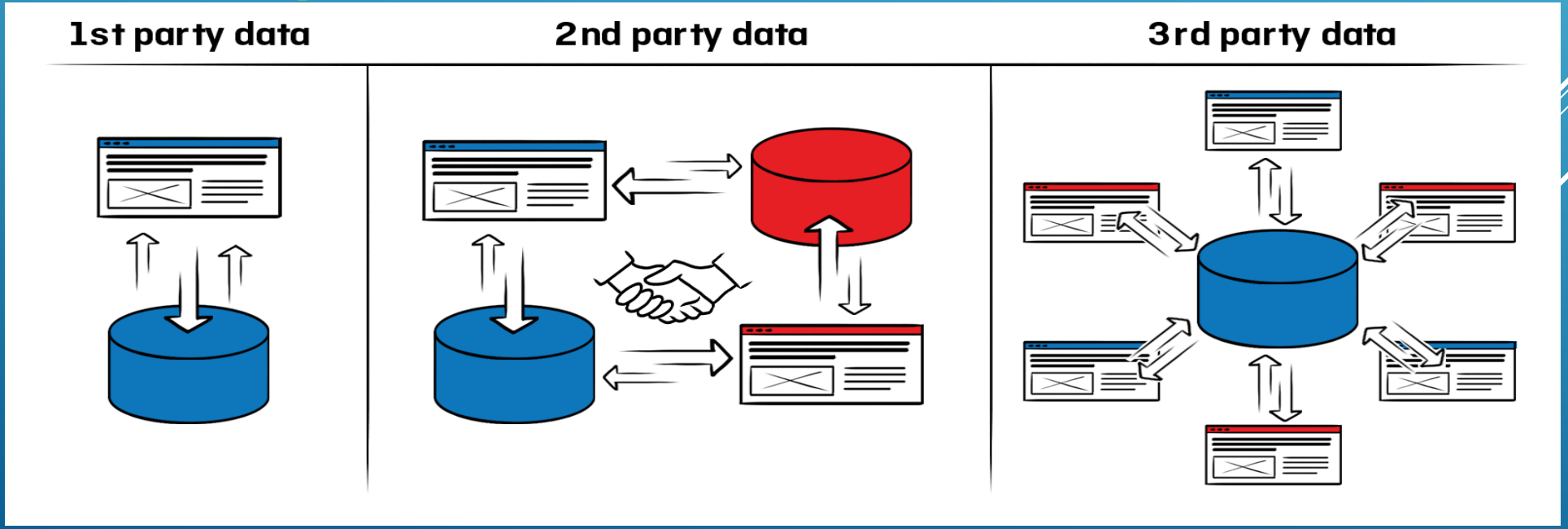
The Business of Unregulated Data Analytics

1. **1st Party Data** is collected by firms with which the user has a direct relationship.
2. **3rd Party Data** is collected by thousands of specialist firms across the web with little-to-no oversight
3. **Data Brokers**: Help actors manage 1st party data collection, as well as sell 3rd party data and 'completing' data.
    1. **eXelate, a data broker, sells "men in trouble".**
    2. **IXI sells "burdened by debt: small-town singles".**
    3. **Forbes, sells data about readers who visit its site.**
    4. **BlueKai aggregates and sells access to an average of 100 points of data for 1 billion people and devices.**
    5. **OkCupid used to sell information about users' alcohol consumption and drug use.**

LOWERCASE-P PRIVACY OVERVIEW

The Technology of Unregulated Data Analytics

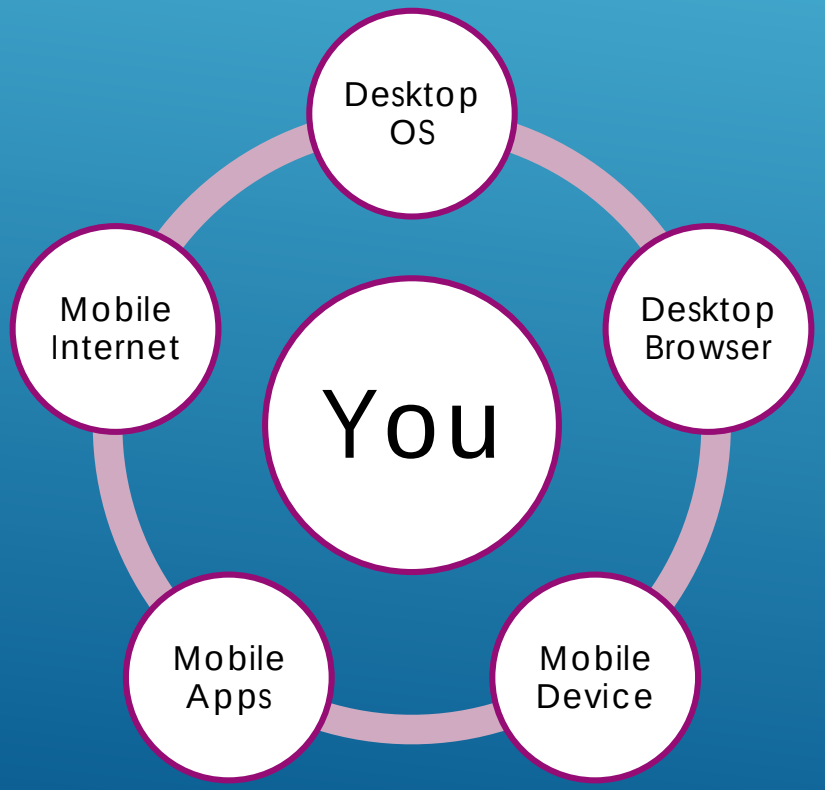
1. **Trackers**: Cookies, beacons, evercookies, social buttons, e-tags, ad trackers, analytics trackers, geolocators, device ID's, chip serial numbers, etc.
2. **Relationships To The Data Asset**:

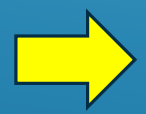


LOWERCASE-P PRIVACY OVERVIEW

The Technology of Unregulated Data Analytics, cont.

1. **Collection Points**:





LOWERCASE-P PRIVACY OVERVIEW

The Privacy Risks of Mobile Apps

- If it's Free, You're the Product.
- AI-as-a-Service increases analytics capacity for smaller players
- Many apps that collect health data aren't regulated
  - Diet trackers, Weight trackers,
  - Medical reference apps, Illness or disease apps
  - Health Trackers, Exercise and Workout trackers, Step counters
- Free Chat, Voice, Video, or Social features is a privacy trap
- 3rd Party SDK's & Surveillance OS's
- Geotracking is typically opt-out

LOWERCASE-P PRIVACY OVERVIEW

The Compromised Web Browser: Desktop & Mobile

- The web browser is place on your computer where you let the Internet in.
- Browsing without privacy defenses is not advised
  - Script Blockers
  - Tracker Blockers
  - Reverse Firewalls
  - Ad Blockers
  - Forced-Encryption
  - Password Vaults
  - Social Blockers

LOWERCASE-P PRIVACY OVERVIEW

Social Networks: Surveillance As A Service

- The business model of social networks is viral surveillance.
- The users are the assets sold to 3rd parties.
- Or, the users are the raw material for the AI insights that are then sold or strategically used.
- Users share up their level of comfort, and every bit of data goes to feeding the model.
- Profile are self-building, as users are self-surveilling.
- AI provides insight on emotion, brand loyalties, health indicators, near-term risk events, life events, etc.

LOWERCASE-P PRIVACY OVERVIEW

Smart Homes, Appliances, and Wearables

- Completely unregulated
- Internet of Things Security and Privacy is terrible. No incentive to invest.
- Razor blade model for smart devices: the money is in the long tail
- The economics of IoT don't support privacy or security up front
- Stay clear of this market until meaningful regulation

LOWERCASE-P PRIVACY OVERVIEW

AI, Perfect Pricing, & The Self-Perfecting Data Model

- Data is forever and only grows in value with aggregation.
- A culture of loose regulation and commercial incentives align against privacy progress
- AI will only grow more accessible. Computers don't get slower.
- Case Study: Uber and Perfect Pricing

3 MINUTE BREAK

Next Up: Privacy Self-Defense

Stretch

Drink

Chat

LOWERCASE-P PRIVACY SELF-DEFENSE

Defending yourself and your company from Privacy incidents.

LOWERCASE-P PRIVACY SELF-DEFENSE

1. **Two Battlefields**: The Individual & The Organization
2. Current State of Defense
3. Defense Against Mobile Devices
4. Defense Against Web Browsers
5. Defense Against Apps
6. Defense Against Social Networks
7. Privacy Program Action

LOWERCASE-P PRIVACY SELF-DEFENSE

Two Privacy Battlefields: The Individual & The Organization

INDIVIDUALS	ORGANIZATIONS

LOWERCASE-P PRIVACY SELF-DEFENSE

Current State of Defense

INDIVIDUALS	ORGANIZATIONS
• If you're not actively defending your privacy, you're defenseless • The law is not on your side, Caveat Emptor. • Almost all Net-connected consumer technology has a Privacy Economy component. 	- If your organization isn't subject to Privacy compliance, you've likely spent $0 on Privacy Defense - For Compliance-impacted orgs, Privacy Defense is a Tag Team between an Executive Owner, General Counsel, the CISO, and the CIO. - Very few enterprise-class tools to defend LCPP. Lumped under DLP (but that's not exactly right) - Technical Defenses are still local to the endpoint. Edge lockdown is still most effective.

LOWERCASE-P PRIVACY SELF-DEFENSE

Defense Against Mobile Devices

INDIVIDUALS	ORGANIZATIONS

• Android: There's nothing that can be done.
• iPhone:
  • Content Blockers for Safari
  • Privacy Mode
  • Auto-VPN (HMA, Nord)
• Don't understand the business model of the App? Don't install it.
  • "I Just Love To Click 'I Agree' and 'OK' every time I see a box. I can't help myself!"
	- Add LCPP components to your mobile device management policy, and use your MDM technology to control apps that expose your environment to LCPP risk.
	- For Privacy sensitive areas, policy to forbid photographs, video calls, or other tech that captures an environment. No one scrubs room THAT clean.
	- VPN to push all external mobile traffic through company-controlled portals (OpenVPN in AWS, e.g.)

LOWERCASE-P PRIVACY SELF-DEFENSE

Defense Against Web Browsers

INDIVIDUALS	ORGANIZATIONS

• Business models matter: Edge v. Safari v. Chrome v. Firefox/Open Source
• Use Extensions
  • Script & Social blockers
  • Tracker/Beacon Blockers
  • Ad Blockers
  • Flash Blockers
• Every link is potential surveilled bait. Think before clicking
	- Tune the browser in OS images for Privacy as well as security & process compatibility.
	- Adjust your border defenses to stop Privacy Attacks in the browser
	- Provide Social Risk Management Training for users to push risk detection and mitigation to the human endpoint.

LOWERCASE-P PRIVACY SELF-DEFENSE

Defense Against Apps

INDIVIDUALS	ORGANIZATIONS
• If it's free, you're the product being sold. • If it's paid, read the Privacy Policy and understand how the company makes money. • If it offers chat, it's most likely surveilled. • **EXCEPTION: Signal** • Avoid the Facebook and Google ecosystems, if feasible	- Tune the browser in OS images for Privacy as well as security & process compatibility. - Adjust your border defenses to stop Privacy Attacks in the browser - Provide Social Risk Management Training for users to push risk detection and mitigation to the human endpoint. - All apps require legal and CISO review

LOWERCASE-P PRIVACY SELF-DEFENSE

Defense Against Social Networks

INDIVIDUALS	ORGANIZATIONS

• You're trading your Privacy for blinking lights, cat videos, and pictures of babies.
• Set up your own private social blog or social network. You need pay with money instead of privacy.
  • Social Engine
  • Elgg
• If you can't set one up yourself, get it hosted.
• NEVER USE SOCIAL LOGINS, DEAR GOD
	- Limit use to the Marketing department and only for approved campaigns.
	- Block Social at the edge. No need to let it in.
	- There are commercial social solutions that only provide the service-for-fee. No Privacy violations.
	- Any social apps or networks require due diligence privacy reviews by Privacy Ops

Q&A THERAPY

That was a lot.