Managing Data, Privacy, and Security

What you should consider from the start

Will Hellmuth, CIPP/US
Alex Reynolds , CIPP/US

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

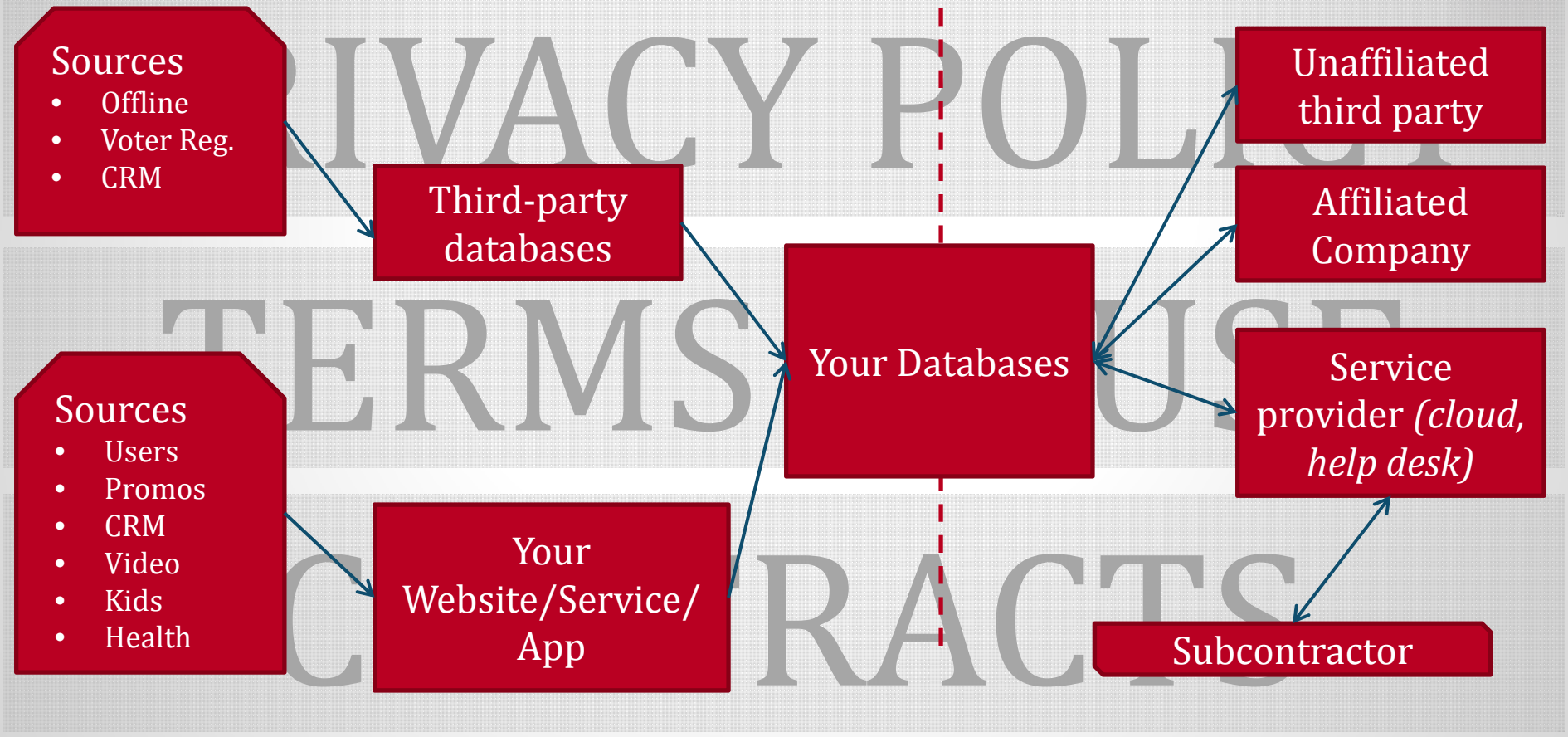
Agenda

Goal: Identify privacy and security compliance issues before they become problems.

Business Scenarios

- You want to:
  - **Market** across websites/apps?
  - **Import** personal information from another business? (BlueKai, LiveRamp, DoubleClick, Acxiom)?
  - Make a **child-friendly** website/online service?
  - Submit your app to the **app store**?
  - Conduct an **email marketing** campaign?
  - Process **credit card** payments?
  - Operate **internationally**?

Mapping the Data



Legal and Best Practice Requirements

(FTC, FCRA, COPPA, California, Google Analytics ToS, behavioral advertising, law enforcement access)

Why should you care?

The Right Thing To Do	▪ Good customer relations ▪ Best practices
Compliance	▪ FTC + State AGs: 212 cases in FTC database, hundreds more investigations ▪ Your statutory obligations; your business partners' statutory obligations
Part of Doing Business/Competitive	▪ Contracts ▪ M+A due diligence reviews
Security	▪ Protect your customers and business assets

What are your goals?

- **Provide users with**: transparency; choice; access; accountability
- **Comply** with federal, state, or international law
- **Ensure** data is protected at all levels (“clean in, clean out”)
- **Defend** against security threats

What is personal information?

Information that is **linked** or **reasonably linkable** to an individual.

NOMENCLATURE	EXAMPLES
Consumer Info	Linked (name, address) or reasonably linkable (could match cookie ID to a name)
Personal Info	U.S. statutory term; blanket term for linked or linkable info in the EU
Personally Identifiable Info (PII)	Name, telephone, address, email, etc. *Also found in statutes*
Sensitive	Child, payment card number, health
Non-PII	IP or MAC address *Non-PII can become PII*
De-identified	User X is a teen male who purchased a red shirt in June and a blue shirt in July
Aggregate	34% of our male subscribers like orange socks
Statutory terms	"Protected Health Information," "Nonpublic Personal Information"

Scenario: Website

Collection

- User-submitted info
- Automatically collected (purchases, page views, device IDs, referral URLs, location)
- Payment card
- Forums; public comments to blogs

Use

- Provide products/ services/content
- Perform analytics/optimize
- Advertising
- Investigate improper use

Disclosure

- Unaffiliated third party
- Affiliated company
- Service provider
- Subcontractors

Consider…

- One policy, or more?
- Knowing where the data comes from and goes to
- "Material" changes, if updating policy
- Online behavioral advertising (OBA)/interest-based ads

Laws/BP

- FTC
- COPPA
- DAA/NAI
- PCI-DSS
- CA and DE statutes

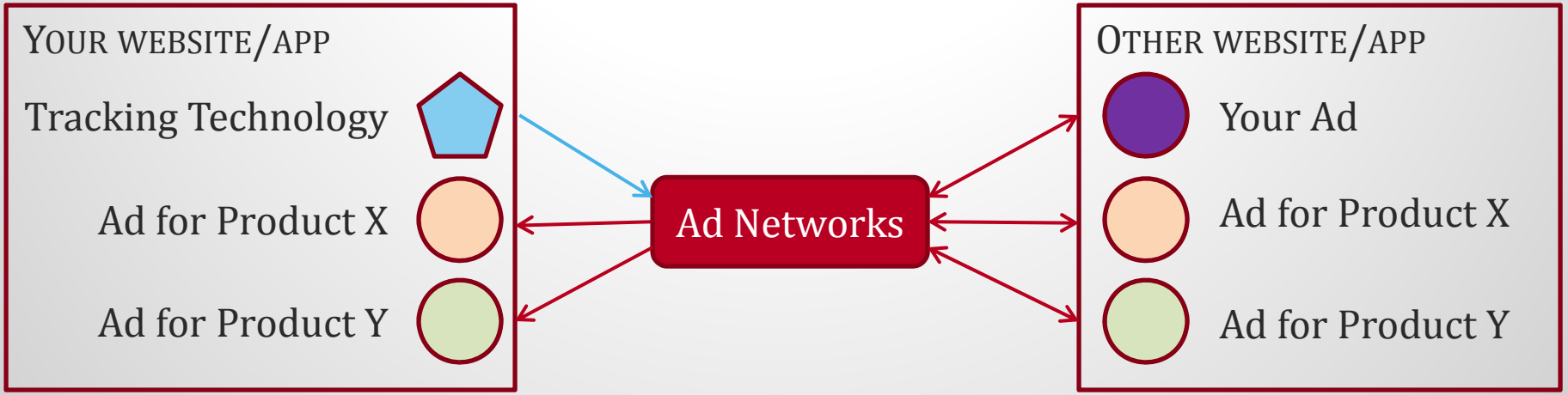
Behavioral Advertising

Contextual Ads (not OBA)

Key Scenarios

- You permit third parties to place ads and/or trackers on your website
- You engage third parties to place your ads based on data they collect from your users
- You collect data across websites/apps for OBA

Ads served based on data gathered from users across websites/apps

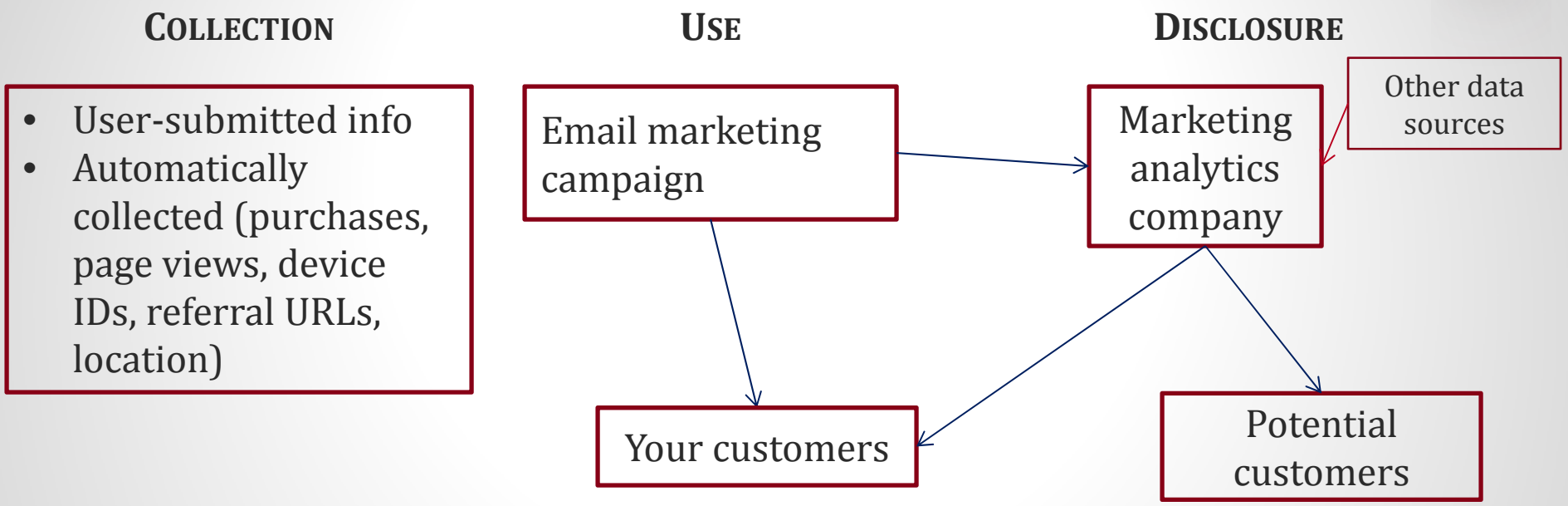


Scenario: App Developer

Collection	Use	Disclosure
• Registration info • Precise location (GPS) • Usage data • Data from other apps	• Provide products/ services/content • Perform analytics/optimize • Advertising • Investigate improper use	Service provider (cloud host, analytics for OBA/direct marketing) Other apps

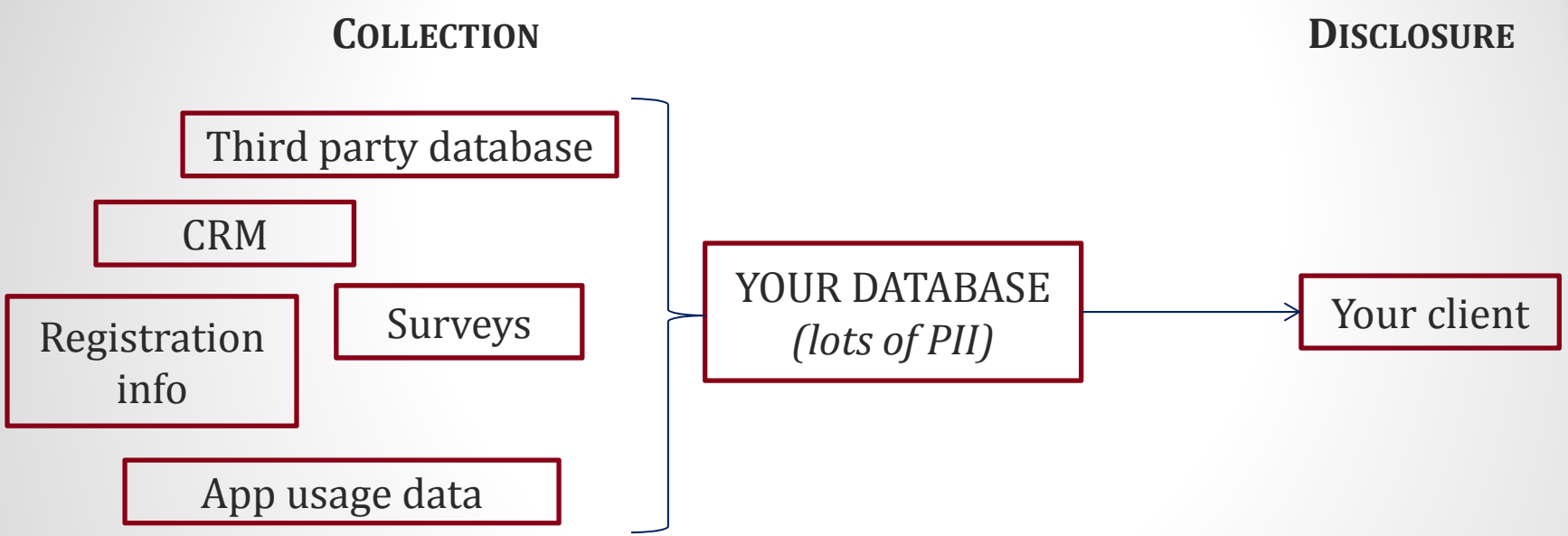
Consider…	Laws/BP
• If you want to sell through an app store, your collection, use, and disclosure (and security) must be consistent with app store Terms of Use	• FTC and State guidance • Same as for websites, plus: store Terms of Use

Scenario: Email Marketing



CONSIDER…	LAWS/BP
• Anti-spam laws • Ensuring third parties acting on your behalf comply with law and respect your customer relationships	• CAN-SPAM • CASL

Scenario: Data Aggregator



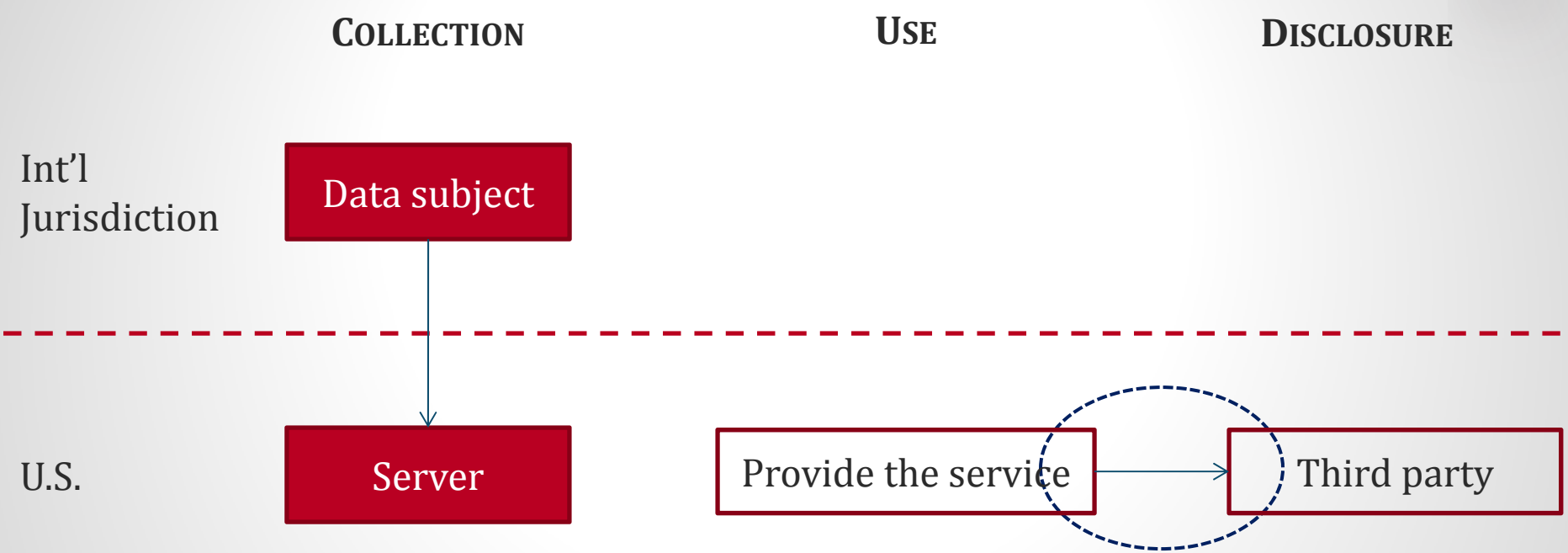
CONSIDER…

- "Clean in, clean out" (i.e., avoid liability by making sure data is collected and disclosed with appropriate consent)
- Client uses of data (e.g., OBA, fraud)

LAWS/BP

- FTC scrutiny
- Fair Credit Reporting Act
- DAA/NAI
- Privacy policies, terms of service, contracts of data sources

Scenario: International



CONSIDER…

- Broader definitions of personal information than U.S.
- EU General Data Protection Regulation in 2018
- EU ePrivacy Regulation (regulation of OTT services)

LAWS/BP

- GDPR
- Country-specific laws
- Constraints local laws may place on your business partners

Other potential issues

- Governmental access to your customers' info (i.e., you were served with a subpoena, what do you do?)

  Electronic Communications Privacy Act, regulatory disclosures

- Providing service in highly-regulated industries

  "Financial Institutions," HIPAA "covered entities," telecommunications sector, energy sector

- Selling your business

  Due diligence process

Security

Risks

- Unauthorized Access
- Hacking
- Theft
- Insider threat
- Nation state
- Ransomware

Controls

- Written information security program
- Access controls (e.g., good password, separate admin accounts, “clean desk” policy)
- Encryption
- Physical safeguards

TRAINING

Remember…

- Privacy and Security are not one-off considerations

- Re-evaluate when:
  - Adding new services
  - Contracting with third parties
  - Changing the use of previously collected information
  - Remediating a security incident

Questions?

Will Hellmuth

202-973-4270

williamhellmuth@dwt.com

Alex Reynolds

202-973-4251

alexreynolds@dwt.com