December 10, 2020

The Privacy Playbook: Protecting Deal Value Through a Targeted Privacy Due Diligence

FTI CONSULTING™

Introductions

Olivia Greer

Counsel

Weil, Gotshal & Manges LLP

Andrew Shaxted

Senior Director

FTI Consulting

John Stiffler

Senior Managing Director

FTI Consulting

Agenda

—**Introductions**

—**Cyber versus privacy** – *threats, targets and penalties*

—**Top data privacy landmines**

—**Best practices for mitigating risk**

—**Adapting your deal playbook**

—**Open Q&A**

What's the Difference Between Privacy & Cybersecurity?

Cybersecurity

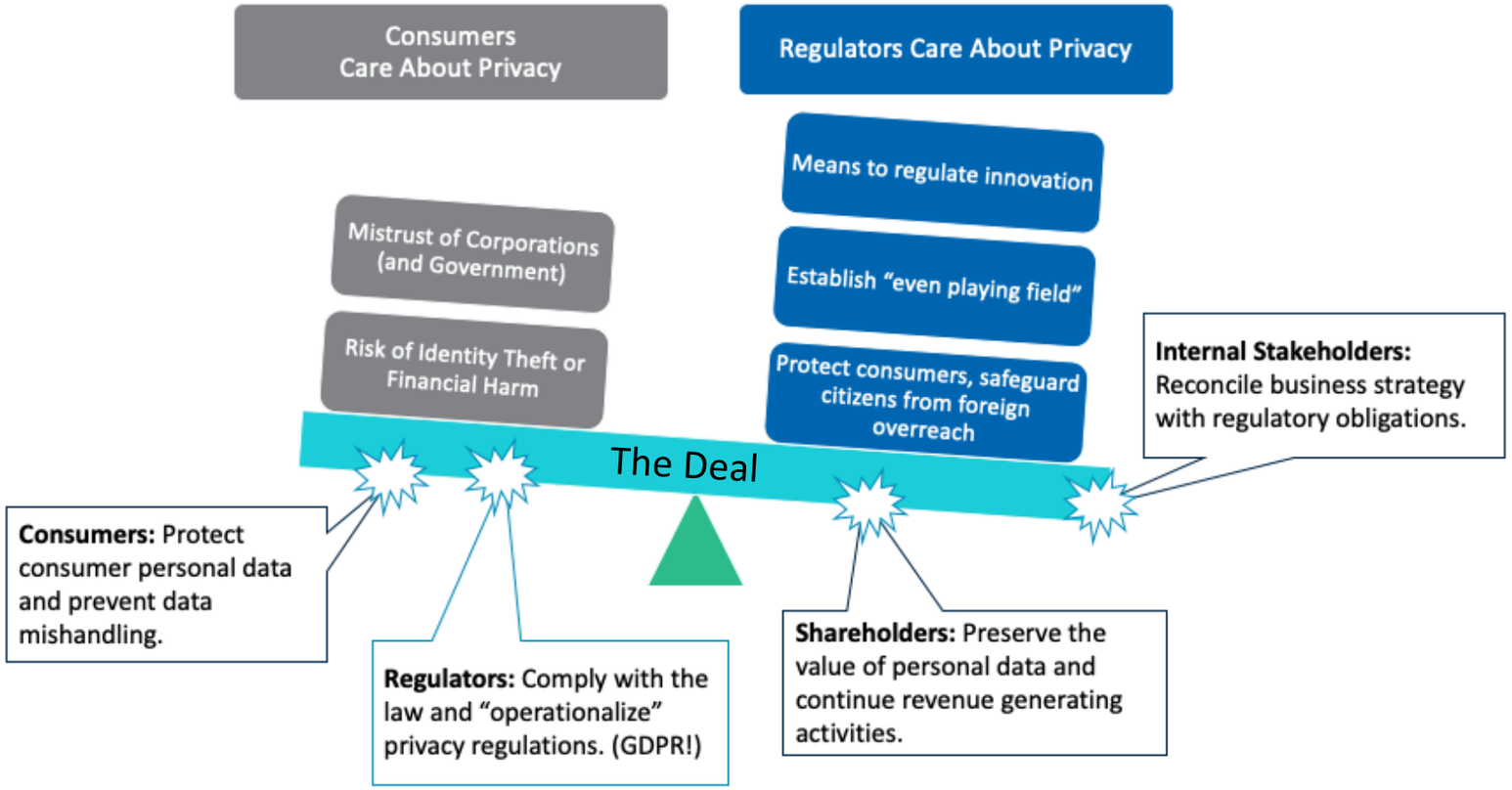
Focuses on protection of all information assets (personal information, but also trade secrets, confidential business information, employee information, etc.).

In the deal context, cybersecurity due diligence seeks to:

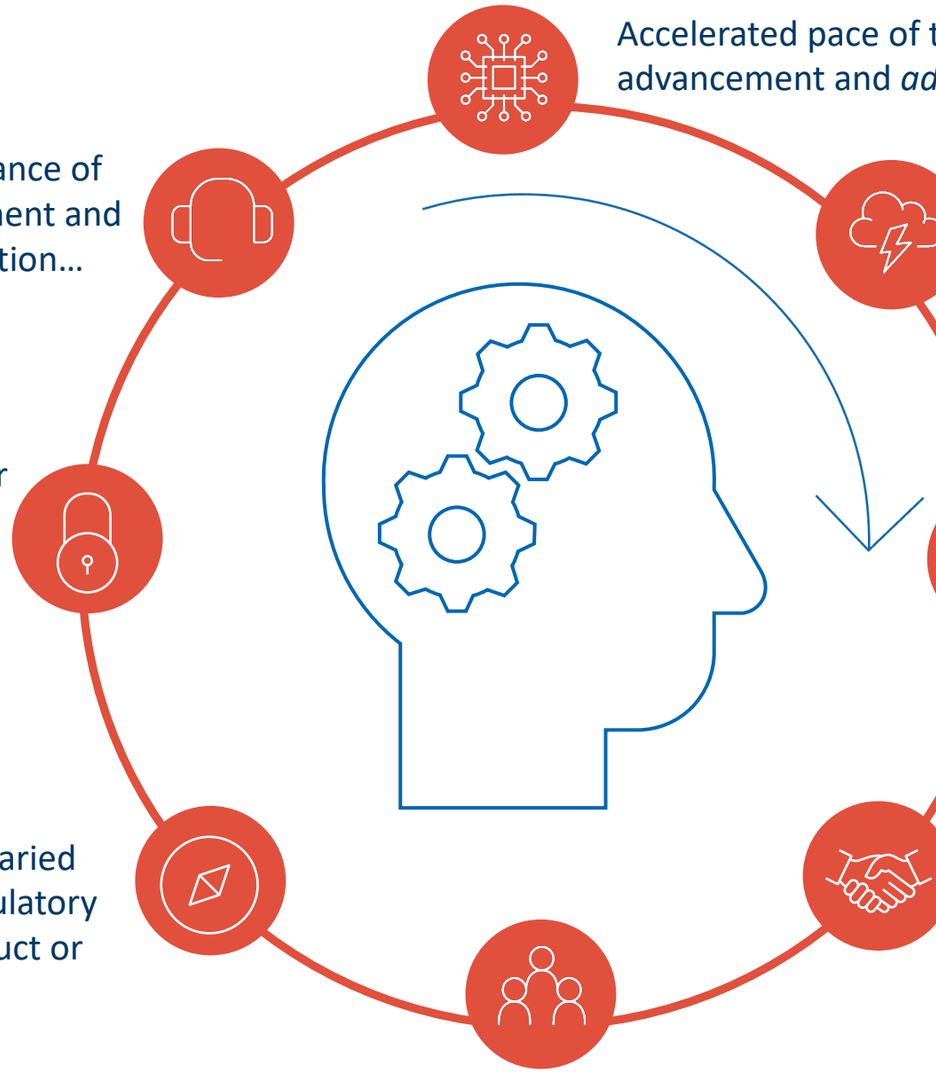
- Ensure adequate technical controls exist across products/systems,
- Review past exposure to breach events, and
- Assess future exposure to breach events.

Privacy

"Privacy" due diligence focuses specifically on Personally Identifiable Information (PII). Protection is a piece of the Privacy due diligence effort, but steps further to puzzle address questions regarding collection, use, and disclosure of that PII.



Data Privacy Risk



Accelerated pace of technological advancement and *adoption*…

Recurring bouts of economic and geo-political uncertainty…

Increasingly onerous regulatory enforcement environments…

Unprecedented profitability and consolidation within key industries…

Growing and changing customer base…

New markets, new competition, varied customer cultures, additional regulatory requirements, and potential product or service modifications…

Constantly-changing cyber attack vectors, assailant typology, and defense methods…

Growing importance of customer sentiment and company reputation…

KEY TYPES OF DATA

- Personal Health Information (PHI)
- Personal Credit Information
- Personally Identifiable Information (PII)
- Customer and price lists
- Salary and compensation information
- Client or customer account information
- Trade secrets and intellectual property
- Data stored in a prohibited jurisdiction (*i.e. data subject to European Union data protection laws stored in the United States*)
- Content subject to legal hold obligations
- Content subject to regulatory retention obligations
- Data leaving restricted jurisdictions
- Contractually limited information, including government data

Repercussions for Privacy Issues Include:

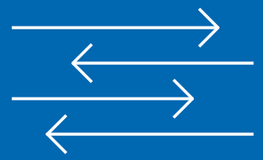
Loss of customers and goodwill

Government investigations, fines and settlements

Class action litigation

Adverse changes in business practices

Bad press



Collateral impact on partners and customers

What is Personal Information?

Personal Information / Personally Identifiable Information (PII): *No single definition*

May include:
• Name • Gender • Age/DOB • Telephone number • Email address • IP address • Geolocation information • Device identifiers • Browsing history

“Sensitive Information”
• Medical, health or insurance information • Financial/payment card information • Social security number • Driver’s license number • Passport number • Information from children under 13

Collection of Information

But I don't think this applies to me because:

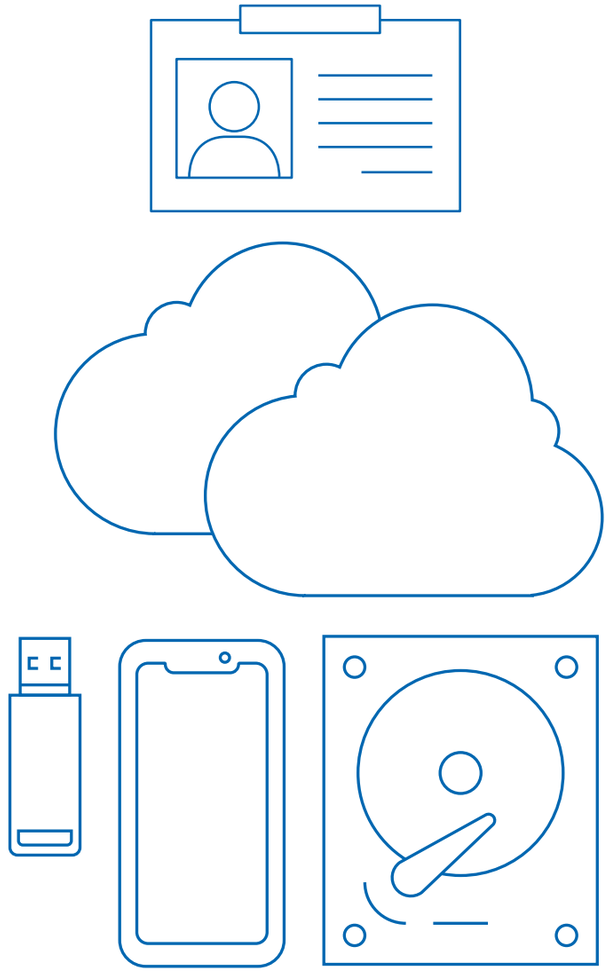
My data aren't "personal information" because I got them from a public source / public records / by scraping a website / etc…

My information is anonymous….

Collection of Information

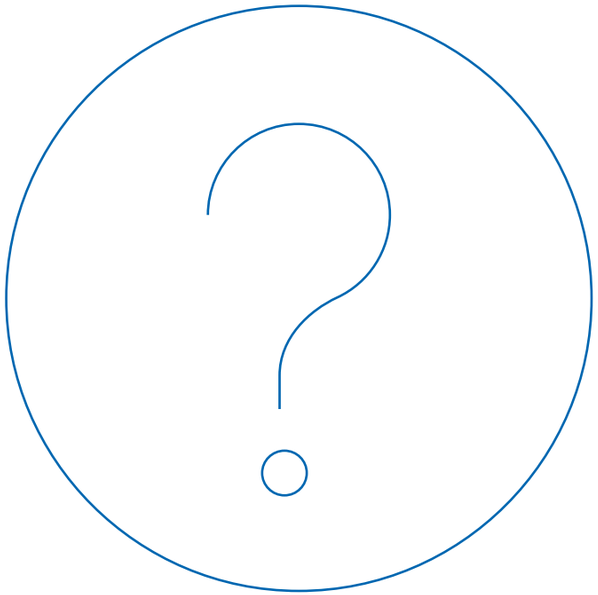
- **Purchased data sets.**
- **Employee or customer data.**
  - HR Data
  - Includes information in third-party applications (*i.e., Slack, Salesforce, etc.*)
- **Information provided by user.**

  For example, if your services require individuals to sign up for accounts using name, email address, etc.
- **Information collected automatically.**
  - Device-specific information (*hardware model, operating system version, unique device identifiers, and mobile network information including phone number*)
  - Device event information (*crashes, system activity, hardware settings, browser type, browser language, the date and time of your request and referral URL*)



Use of Personal Information

- Is personal information shared, sold or transferred with/to third parties?
- Are there agreements with vendors or other third parties that govern the protection of shared information?
- Do customer agreements address practices with respect to collection of information?
- Where and how is personal information stored?
- How long is personal information retained?
- How is personal information disposed of?
- Is there a privacy or data security policy?
- How is personal information used for marketing (especially texting or calling)?
- Who is tasked with responsibility for privacy?



Sharing Personal Information with Third Parties

"We do not share, sell, rent or lease your personal information to third parties."

REALLY??

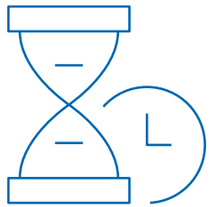
What about:

- Vendors who help provide services
- Subcontractors of vendors who help provide services
- Hosting companies / Cloud Service Providers
- Advertisers
- Analytics

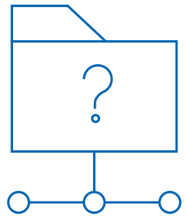
Transfer of personal information in connection with a transaction

Retention of Personal Information

Only store personal information for as long as it is needed for a legitimate legal or business need (*e.g., reporting obligations, operations, etc.*)



Storing personal information, particularly sensitive information, for extended periods of time may expose a company to increased risks



How are you going to explain what you stored?

Federal Trade Commission Act § 5

- **Section 5 broadly prohibits "unfair or deceptive acts or practices in or affecting commerce."**
  - **Deception:** a material representation or omission that is likely to mislead consumers acting reasonably under the circumstances
  - **Unfairness:** practices that cause or are likely to cause substantial injury to consumers that are not outweighed by countervailing benefits to consumers or competition and are not reasonably avoidable by consumers.
- **Flexible law that can be applied to many different situations, entities, and technologies**

U.S. Federal Privacy Sector-Specific Laws

Healthcare	Financial	Telecommunications	Education	Workplace/ Employment
—Health Insurance Portability and Accountability Act (HIPAA) —HITECH / GINA	—Fair Credit Reporting Act (FCRA)/Fair and Accurate Credit Transactions Act of 2003 (FACTA) —Gramm-Leach-Bliley Act (GLBA) —Dodd-Frank —Bank Secrecy Act	—Telemarketing Sales Rule/Telephone Consumer Protection Act —CAN-SPAM —Junk Fax Prevention Act —Wireless Domain Registry —Telecommunications Act —Video Privacy Protection Act / Cable Communications Privacy Act	—Family Educational Rights and Privacy Act (FERPA) —Protection of Pupil Rights Amendment —No Child Left Behind	—Anti-discrimination laws —Background screening —Employee monitoring —Investigation of employee misconduct —Termination of employment

Adapting Your Deal Playbook

FTI CONSULTING™

Open Q&A

Thank you!

OLIVIA GREER
Counsel
Weil, Gotshal & Manges LLP
+1 (212) 310-8815
olivia.greer@weil.com

ANDREW SHAXTED
Senior Director
FTI Consulting
+1 (773) 658-0241
andrew.shaxted@fticonsulting.com

JOHN STIFFLER
Senior Managing Director
FTI Consulting
+1 (415) 283-4262
john.stiffler@fticonsulting.com

FTI CONSULTING™