GTC

LAWYERS + STRATEGISTS

Mergers & Acquisitions
Data Privacy & Security - Panel

Jon Adams, *Senior Privacy Counsel, LinkedIn*

Rocco Grillo, *Executive Managing Director, Cyber Resilience Leader, Stroz Friedberg/Aon*

Sayoko Blodgett-Ford, *Member & Chief Privacy Officer, GTC Law Group (Moderator)*

Mergers & Acquisitions – Data Privacy & Security Panel

Jon Adams, Senior Privacy Counsel, LinkedIn. CIPP/US

- part of a team that oversees LinkedIn's privacy and data protection compliance program.
- Wilson Sonsini Goodrich & Rosati PC – privacy & technology transactions
- Sidley Austin LLP - product, transactional, and compliance counseling relating to privacy, data protection, cybersecurity, and IP matters
- FTC, Bureau of Consumer Protection – consumer protection & privacy law enforcement; policy

Rocco Grillo, Executive Managing Director/Cyber Resilience Leader
Stroz Friedberg/Aon

- serves on Stroz Friedberg's executive management team
- leads Cyber Resilience business - incident responders and security scientists
- Protiviti – Managing Director and Global Leader of Incident Response & Forensics
- RedSiren Technologies, Director
- Lucent Technologies

Sayoko Blodgett-Ford, Member & Chief Privacy Officer, GTC Law Group. CIPP/US

- extensive expertise in due diligence in connection with technology M&A transactions
- Boston College Law School – Adjunct Professor – Privacy Law & Mobile Apps
- Court Appointed Arbitrator
- Tetris Online, Inc. – General Counsel
- Nintendo of America Inc. – Senior Manager, Intellectual Property Group

DEALING IN DATA

Addressing Privacy in M&A Diligence and Agreements

THE PRIVACY MISSION

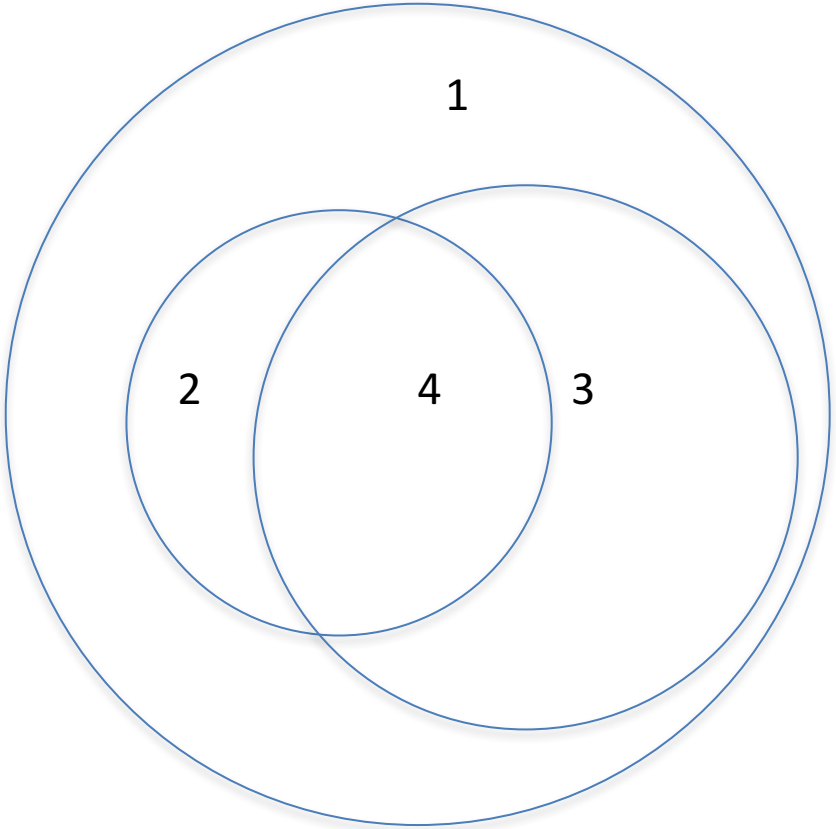
The goal is to balance privacy and security risks in pursuit of business objectives.

But how?

BUSINESS OBJECTIVES

- Deals happen for all kinds of reasons
- Data increasingly is key, but will not be central in all deals
- Privacy, security, and data concerns often do not drive business objectives (but could impede them)
- The importance of privacy and data security in a deal is hard to determine without investigating

BUSINESS OBJECTIVES



It’s hard to know how to approach privacy and security on a deal unless you dig in

1: All Deals
2: Data-Driven Deals
3: Deals with Large Privacy/Security Risk
4: Data-Driven + Large Privacy/Security Risk

**Not to scale*

DIGGING IN THROUGH DILIGENCE

- Potential Issue: Compliance Failures

Statutes and Regulations	*HIPAA, GLBA, GDPR, etc.*
Common Law Obligations	*Invasions of privacy, etc.*
Cross-Border Issues	*EU data transfers, data localization, etc.*
Self-Imposed Obligations	*Privacy policies, public statements, etc.*

DIGGING IN THROUGH DILIGENCE

- Contractual Breaches
  - Commercial contracts
  - Industry standards (*e.g.*, PCI-DSS)

DIGGING IN THROUGH DILIGENCE

- Data Breaches and Cyber Attacks
- Government Investigations
- Litigation and Pre-Litigation Activity
- Failure to meet “best” (or even “industry standard”) practices

LIMITS ON DIGGING IN THROUGH DILIGENCE

- Diligence efforts can fall short for various reasons, challenging risk assessment:
  - Desired documentation/info missing or not provided
  - Desired documentation/info does not exist
  - Shifting risk environment makes assessment difficult
- Need to shift risk appropriately as a result to avoid impacting business objectives

ADDRESSING RISK TO GET THE DEAL DONE

- Risk allocation should be addressed through the agreement between the parties
- Three key considerations:
  - Seller and acquiror deal objectives
  - Seller and acquiror negotiating power
  - Seller and acquiror risk tolerance

ADDRESSING RISK TO GET THE DEAL DONE

- Risk Shifting in Reps & Warranties
  - Do privacy and data security reps & warranties fall under IP reps & warranties?
  - What is “market” for the reps & warranties?
  - How can you find the balance through exclusions, materiality, and other terms of art?

ADDRESSING RISK TO GET THE DEAL DONE

- Several means to allocate risks/obligations in agreement (outside of the reps & warranties), such as:
  - Disclosure Schedules
  - Indemnification (and associated limitations)
  - Covenants
  - Closing Conditions
  - Purchase Price Adjustment

M&A INTEGRATION: GROWING PAINS

"*Now that we bought it, how do we use it?*"

- How do the parties integrate:
  - Product data?
  - Sales/customer data?
  - HR data?
  - IT systems?

M&A INTEGRATION: GROWING PAINS

- What does the seller privacy policy permit?
  - Free transfer of data (*i.e.*, no *Toysmart*)?
  - Restrictions on use?
  - Is notice/choice required?
- How does this align with the deal objectives?
  - Impact of legal restrictions on deal objectives

M&A INTEGRATION: GROWING PAINS

- Integration of data in transactions where seller or its successor continues to operate:
  - Data sharing frameworks?
  - Contracts?
  - Internal/External APIs?
  - How to handle HR/benefits data?
  - What about data-related service providers?

M&A INTEGRATION: GROWING PAINS

- Many deals result in the two parties continuing to negotiate data use, transfers, and sharing long after the deal concludes
- Thorough diligence and planning (without gun-jumping) are the keys to efficiently realizing business objectives

APPENDIX: SAMPLE REPS

Facebook/WhatsApp Reps & Warranties

SAMPLE REPS

(i) The Company's data, privacy and security practices conform, and at all times have conformed, to all of the Company Privacy Commitments, Privacy Laws and Company Data Agreements. The Company has at all times: (i) provided adequate notice and obtained any necessary consents from data subjects required for the Processing of Personal Data as conducted by or for the Company and (ii) abided by any privacy choices (including opt-out preferences) of data subjects relating to Personal Data (such obligations along with those contained in Company Privacy Policies, collectively, "***Company Privacy Commitments***"). Neither the execution, delivery and performance of this Agreement nor the taking over by Acquirer of all of the Company Databases, Company Data and other information relating to the Company's customers will cause, constitute, or result in a breach or violation of any Privacy Laws or Company Privacy Commitments, any Company Data Agreements or standard terms of service entered into by users of the Company Products. Copies of all current and prior Company Privacy Policies have been made available to Acquirer and such copies are true, correct and complete.

SAMPLE REPS

(ii) The Company has established and maintains appropriate technical, physical and organizational measures and security systems and technologies in compliance with all data security requirements under Privacy Laws and Company Privacy Commitments that are designed to protect Company Data against accidental or unlawful Processing in a manner appropriate to the risks represented by the Processing of such data by the Company and its data processors. The Company and its data processors have taken commercially reasonable steps to ensure the reliability of its employees that have access to Company Data, to train such employees on all applicable aspects of Privacy Laws and Company Privacy Commitments and to ensure that all employees with the right to access such data are under written obligations of confidentiality with respect to such data.

SAMPLE REPS

(iii) No breach, security incident or violation of any data security policy in relation to Company Data has occurred or is threatened, and there has been no unauthorized or illegal Processing of any Company Data. No circumstance has arisen in which: (i) Privacy Laws would require the Company to notify a Governmental Entity of a data security breach or security incident or (ii) applicable guidance or codes of practice promulgated under Privacy Laws would recommend the Company to notify a Governmental Entity of a data security breach.

SAMPLE REPS

(iv) The Company has not received or experienced and, to the knowledge of the Company, there is no circumstance (including any circumstance arising as the result of an audit or inspection carried out by any Governmental Entity) that would reasonably be expected to give rise to, any Legal Proceeding, Order, notice, communication, warrant, regulatory opinion, audit result or allegation from a Governmental Entity or any other Person (including a data subject): (A) alleging or confirming non-compliance with a relevant requirement of Privacy Laws or Company Privacy Commitments, (B) requiring or requesting the Company to amend, rectify, cease Processing, de-combine, permanently anonymize, block or delete any Company Data, (C) permitting or mandating relevant Governmental Entities to investigate, requisition information from, or enter the premises of, the Company or (D) claiming compensation from the Company. The Company has not been involved in any Legal Proceedings involving a breach or alleged breach of Privacy Laws or Company Privacy Commitments.

SAMPLE REPS

(v) Schedule 2.9(jj)(v) of the Company Disclosure Letter contains the complete list of notifications and registrations made by the Company under Privacy Laws with relevant Governmental Entities in connection with the Company's Processing of Personal Data. All such notifications and registrations (including the Company's certification under the U.S.-EU/Switzerland Safe Harbor) are valid, accurate, complete and fully paid up and, to the knowledge of the Company, the consummation of the Transactions will not invalidate such notification or registration or require such notification or registration to be amended. To the Company's knowledge, other than the notifications and registrations set forth on Schedule 2.9(jj)(v) of the Company Disclosure Letter, no other registrations or notifications are required in connection with the Processing of Personal Data by Company.

SAMPLE REPS

(vi) Where the Company uses a data processor to Process Personal Data, the processor has provided guarantees, warranties or covenants in relation to Processing of Personal Data, confidentiality, security measures and compliance with those obligations that are sufficient for the Company's compliance with Privacy Laws and Company Privacy Commitments, and there is in existence a written Contract between the Company and each such data processor that complies with the requirements of all Privacy Laws and Company Privacy Commitments. The Company has made available to Acquirer true, correct and complete copies of all such Contracts. To the knowledge of the Company, such data processors have not breached any such Contracts pertaining to Personal Data Processed by such Persons on behalf of Company.

SAMPLE REPS

(vii) The Company has not transferred or permitted the transfer of Personal Data originating in the EEA outside the EEA, except where such transfers have complied with the requirements of Privacy Laws and Company Privacy Commitments, including the Company's certification under the U.S.-EU/Switzerland Safe Harbor.

SAMPLE REPS

(viii) The Company has valid and subsisting contractual rights to Process or to have Processed all third-party-owned data howsoever obtained or collected by or for the Company in the manner that it is Processed by or for the Company (all such data, "***Company-Licensed Data***"). The Company has all rights, and all permissions or authorizations required under Privacy Laws and relevant Contracts (including Company-Data Agreements), to retain, produce copies, prepare derivative works, disclose, combine with other data, and grant third parties rights, as the case may be, to each of the Company-Licensed Data as necessary for the operation of the Business as presently conducted. The Company has been and is in compliance with all Contracts pursuant to which the Company Processes or has Processed Company-Licensed Data, and the consummation of the Transactions will not conflict with, or result in any violation or breach of, or default under, any such Contract. Schedule 2.9(t)(ix) of the Company Disclosure Letter identifies each Contract governing any Company-Licensed Data to which the Company is a party or is bound by, except the standard terms of use entered into by users of the Company Products (copies of which have been Made Available to Acquirer).

SAMPLE REPS

(ix) The Company is the owner of all right, title and interest in and to each element of Company Data that (i) is used or held for use in the Business that is not Personal Data or Company-Licensed Data or (ii) the Company purports to own (collectively, "***Company-Owned Data***"). The Company has the right to Process all Company-Owned Data without obtaining any permission or authorization of any Person. Other than as set forth on Schedule 2.9(t)(x) of the Company Disclosure Letter, the Company has not entered into any Contract governing any Company-Owned Data or to which the Company is a party or bound by, except the standard terms of use entered into by users of the Company Products (copies of which have been Made Available to Acquirer).

SAMPLE REPS

(x) The Company does not Process the Personal Data of any natural Person under the age of 16.

(xi) The Company has never directly stated or indirectly implied that Company Products enhance the security of data (including Personal Data) accessed, provided or sent by end users.

Cybersecurity Industry Challenges

The cyber threats **evolve rapidly** and can quickly endanger a company that can't keep pace.

Organizations are under persistent pressure to **refine** their **defenses** against **attackers** who are **constantly advancing** their techniques.

Regulators are also trying to **keep pace** further complicating an organization's risk management approach.

Organizations must commit to a **continuous process** of **evaluation** and **improvement.**

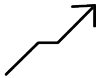
Regular assessments, testing, refinement, and responsiveness are essential to **keeping critical assets protected** and **ensuring strong governance** and compliance.

Organizations need to be constantly focused on **limiting** the **economic** and **reputational damage** from incidents.

Cyber Threat Landscape

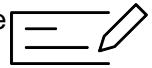
COST

Average cost of a data breach
increased from
$3.9 to $4M

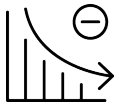


2016 Ponemon Cost of Data Breach Study: Global Analysis

$2.5B
in insurance
premiums



Global loss
$445B



CSIS Center for Strategic and International Studies

THREAT

430M

Pieces of unique
malware **(up 36%)**

Symantec Internet
Security Threat Report
(April 2016)

35%
increase
in rasomware

Symantec Internet
Security Threat Report
(April 2016)

554M
records
compromised

First 6 months of 2016
Germalto Breach level
Index 1H

CONNECTIVITY

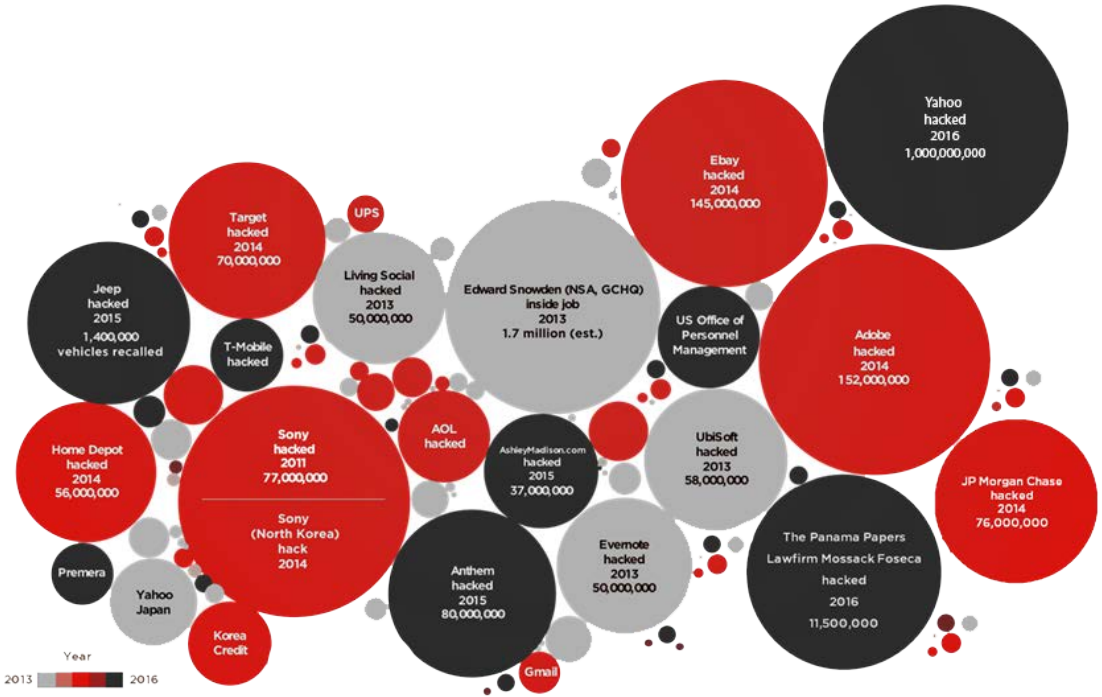
By 2020 there will be
20.8B
connected
devices

Gartner Report

Average companies connect to
1,555
Individual
partners

Skyhigh Networks

Cyber Incidents



Why is Good Cyber Hygiene Important?

Were you ready for Wannacry/Not Petya?

Improve cyber resiliency maturity by assessing, establishing and improving:

- IT controls
- External and internal malware vulnerability
- Corporate governance controls
- Technical vulnerability
- Penetration test assessments
- Benchmarks against peers
- Breach assessments

M&A Areas to Assess & Remediate

Compliance & Data Architecture

Understand the process/procedures by which the company obtains data, including the locations in which data originates

- Understand the type of data received by the company and the internal controls in place regarding PII
- Evaluate compliance with PII standards by executing targeted PII searches against sampling of workstations and network shares
- Execute automated tests against standard books and records to identify conflicts of interest, suspicious activity patterns, and transactions requiring additional review
- Evaluate governance, policies and verify procedures for compliance requirements: FCPA, Safe Harbor, etc.

M&A Areas to Assess & Remediate

Cyber Readiness & Resilience

Understand the current security posture of the organization from a people, policy, governance and operations perspective

- Assess the current incident response plan, review critical personnel needed, review communications plan, create effective triage, and rehearse flow of tasks and communication. Update plan as required
- Threat Analysis of key applications, web, cloud and infrastructure for vulnerabilities
- Contract with an incident response provider prior to an incident
- Assess vendor contracts requirements and access to corporate systems, infrastructure and assets
- Proactively review for current threats against up to date attack vectors, strategies and known bad actors
- Evaluate insider risk activity proactively- identify any potential risks

Cyber Resilience M&A Approach

- Implement a holistic approach to minimize exposures to cyber risks and threats aligned with industry leading best practices.

- Include a framework approach to achieve objectives for cybersecurity transformation, starting with a foundational Cybersecurity Risk Assessment:

By performing an accelerated baseline Cybersecurity Risk Assessment, starting the organization's specific business and cyber threat profile, organizations can develop and implement a security strategy and prioritized plan to transform and optimize its Cybersecurity, while enhancing value from existing and future cybersecurity investments.

Cyber M&A Due Diligence Checklist

Assess the maturity of the overall security program including governance, employee awareness, resistance to cyber fraud, and incident response preparedness.

- ❑ Review oversight and reporting of security program, decision making, and reporting to senior leadership
- ❑ Review documented incident response plan and security incident reports and procedures
- ❑ Review history of prior data security breaches and incidents and responses
- ❑ Review documented security awareness program
- ❑ Perform phishing testing of users to determine susceptibility to email-based threats

Determine how well the IT infrastructure aligns with the best security practices. Assess resistance to internal and external hackers.

- ❑ Perform technical security assessment of IT infrastructure
- ❑ Review inventory of business critical assets and physical, operational and technical security controls currently in place to protect them
- ❑ Review insider threat prevention and detection program, including pre-employment screening procedures and ongoing monitoring, as well as measures protecting IP theft by departing employees
- ❑ Review third party risk management program, including pre-engagement and periodic assessments
- ❑ Perform penetration testing and application security assessments to identify vulnerabilities

If subject to security-related regulations or government guidelines (e.g. HIPAA, SEC, etc.) determine how well the security program adheres to them.

- ❑ Review historical compliance audits and whether recommended changes have been scheduled or already implemented

Contact

Rocco Grillo
Executive Managing Director
Global Leader, Cyber Resilience Services
Stroz Friedberg
rgrillo@strozfriedberg.com
+1 212.981.2674

STROZ FRIEDBERG
an Aon company

AON
Empower Results®

GTC

LAWYERS + STRATEGISTS

Special Issues in M&A

1. Meeting the challenge of the “Rush” deal

2. Web scraping

3. GDPR impacts

Sayoko Blodgett-Ford
GTC Law Group PC
Member & Chief Privacy Officer

1. THE "RUSH" DEAL

- "We are in a competitive bid situation."
- "We have to move fast. Our CEO/founder plans to announce this deal at our trade show in a week.'"
- "This is a major public deal. Material risks are reflected in the market already. Every extra day increases risk of a leak that could affect the stock prices and kill the deal."

And, everyone's favorite thing to hear on a Friday ...

- "We plan to announce publicly early Monday morning before the market opens, so we have to sign Sunday night."

THE "RUSH" DEAL – CRISES MODE

a *buy-side, tactical, legal** perspective

STEP 0.1 Know the buyer as well as possible.

- How do they handle data privacy & security in their core business model and in their growth areas?
- What do they already feel comfortable they can handle?
- What is their level of data privacy & security sophistication/risk tolerance?
- Are they skilled at integration?
- Do they have relevant past/pending lawsuits?
- Do they have active lobbying positions on certain issues?

THE "RUSH" DEAL
DATA PRIVACY DILIGENCE IN CRISES MODE

STEP 1 DO YOUR HOMEWORK – *FAST!*

- Company and competitor websites and news
- White papers/demos available online
- Google search
- Litigation search
- SEC filings (if applicable) EDGAR | Company Filings
- Corporate records check
  - to find prior names and acquisitions/divestitures
- Internet Archive
- And of course anything relevant in the data room
  - (if you are lucky and it has more than their lease)

THE "RUSH" DEAL
DATA PRIVACY DILIGENCE IN CRISES MODE

STEP 2 USE A DATA OVERVIEW REQUEST SHEET

- Prioritize & highlight key requests based on Steps 0.1 and 1
- Ask the seller to fill it out as best they can quickly before a diligence call (and schedule that call).
- Tell the seller they can update or mark "in progress" or "to be confirmed" for items that would take additional time to verify.
- Make sure that the Data Overview is not just filled out by Legal. Dev/Engineering/Product team needs to be involved.

DATA OVERVIEW REQUEST SHEET (EXAMPLE)

PROJECT [NAME]
CONFIDENTIAL
DATA/PRIVACY OVERVIEW QUESTIONS
NOTE: The purpose of these questions is to provide a comprehensive initial overview re Data/Privacy, including data collection, storage, use and transmission.
This overview is not a substitute for the detailed responses that will be required in specific areas of diligence, including third party data provider review, inbound software review, data security, commercial contracts etc.
Unless otherwise noted, please answer the questions below for each current and planned Company product or service.
If there was a substantial difference for past products or services, please note and provide a brief explanation.
If a question is not applicable, please note "N/A" and provide a brief explanation of the reason it does not apply.
If you are not sure of an answer or need to review further - just put "UNDER REVIEW" or "IN PROCESS" in the response so we can get this back quickly.

DO NOT LEAD WITH GENERIC "ONE SIZE FITS MOST" QUESTIONS

HIGHEST PRIORITY QUESTIONS
In providing products and services, does the Company collect, use, process, share or store any personal information of anyone (other than personal information of employees for HR purposes or contact information for business customers)?
Please provide a diagram or other illustration (or multiple diagrams and illustrations, if necessary) that shows a high-level overview of the Company's collection/sources, use/processing, and subsequent transmission/sharing of data for each of the Company's product/service offerings, including **[NAME PRODUCT/SERVICE LINES]**, and any other products/services. If different entities play multiple roles in this data flow, please so indicate. Please indicate whether consumer/individual consents are tracked for each step in the flow of the data, and whether such consent is "opt-in" or "opt-out". Please also use arrows to indicate directional flow, one-way, two-way, etc.
Who is the designated privacy compliance individual at the Company? Who is the Company's privacy compliance outside counsel? Does the Company have a Chief Information Security Officer, Chief Privacy Officer, Data Protection Officer (or equivalent thereof)? If so, please provide their name and title and note whether or not they have been disclosed on this deal.
Please provide a list of all of the types of data collected by the Company. Please indicate which items of data on the list are NOT shared with customers, partners or other third parties.
Please describe the cross-border data flows handled by the Company.
Has the Company self-certified under the EU-US Privacy Shield? If not, why not?
Does the Company comply with the EU General Data Protection Regulation ("GDPR")? Please describe.

PRIORITIZE & FOCUS ...

HIGHEST PRIORITY QUESTIONS (NOTE: THESE ARE FICTIONAL FOR THIS TRAINING!)
Your enterprise BYOD security product "**MOBI-SAFE**" uses biometric validation - e.g., thumbprint or an image of a photo ID. You have announced plans to use the Apple iPhone X FaceID technology for the same purpose. Have you taken any steps to comply with the new Illinois biometric identification law? How do you plan to comply with GDPR?
What is the status of your investigation into the May 2017 security incident involving your outside payments vendor for your "**MOBI-PAY**" product?
Several of your top customers have child-directed websites and products. What data do you collect and store for such customers?
In your "**MOBI-TRACK**" product, do you use "zombie" cookies, re-identification, persistent IDs or any methods that are similar to those involved in the FTC enforcement action against Turn/Verizon (see, https://www.ftc.gov/news-events/press-releases/2016/12/digital-advertising-company-settles-ftc-charges-it-deceptively)
How do you obtain customer permission to use their data in the aggregate for your "**MOBI-THREAT**" analysis product?

THE “RUSH” DEAL

STEP 3 COMMUNICATE

- Loop in key team members in relevant diligence streams.
  - Get input on data overview questions
  - Share seller’s responses
  - Invite all relevant diligence groups to attend the data overview call
  - Coordinate follow-up requests
  - Minimize duplicate requests
- If the data privacy team is separate from the commercial contracts team (HR team etc.), tell the other team(s) what to keep an eye out for to avoid duplication of effort.
- Connect regularly to make sure everyone agrees on priorities – and that key information is shared.

THE “RUSH” DEAL

STEP 4 LOOK FOR SOLUTIONS

- Keep your eyes on the finish line.
- Goal is to assess and mitigate risk/exposure, not kill the deal.
  - Is any clean-up remediation needed?
  - Pre-sign, pre-close, post-close?
- Specific indemnity (if a private deal)?
- Keep placeholders in the deal docs as long as possible.
- Expect “surprises” in diligence and on the Disclosure Schedules.

2. WEB SCRAPING

"It's publicly available on the Internet.
We can use it like anyone else."

"It's 'indexing', not 'scraping.'"

"We're just like Google."

"Everyone does it."

2. WEB SCRAPING (Facebook v. Power Ventures)

https://www.youtube.com/watch?v=4QUai3OmkdA

21:53 to 23:30

Computer Fraud and Abuse Act ("CFAA")
18 U.S. Code Sec. 1030(a)(2)

Whoever intentionally accesses a computer **without authorization or exceeds authorized access**, and thereby obtains — … (C) **information** from **any protected computer** …. [violates the statute].

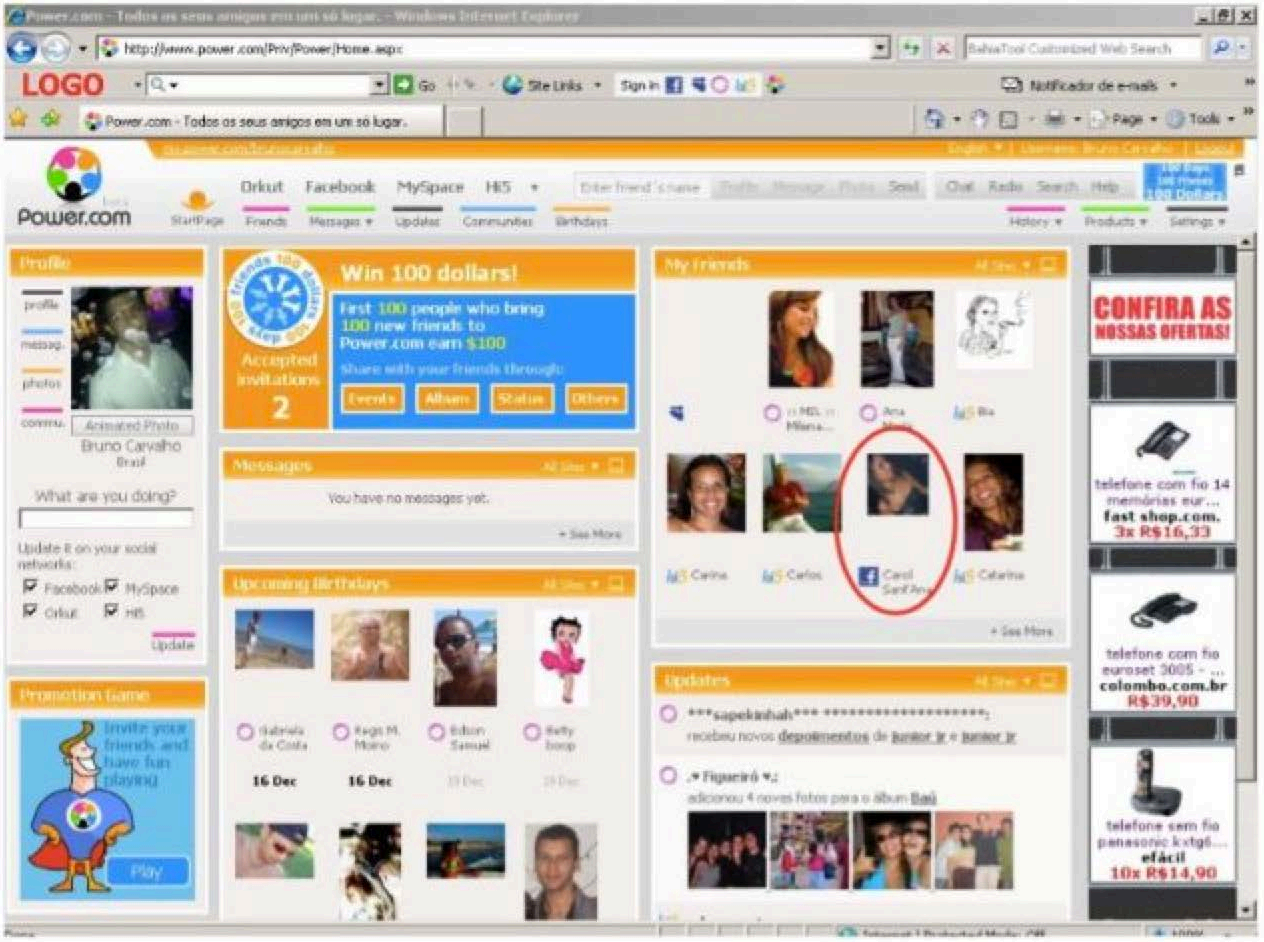


Figure 1: Power.com Screenshot including a Facebook friend

3. **Safety**

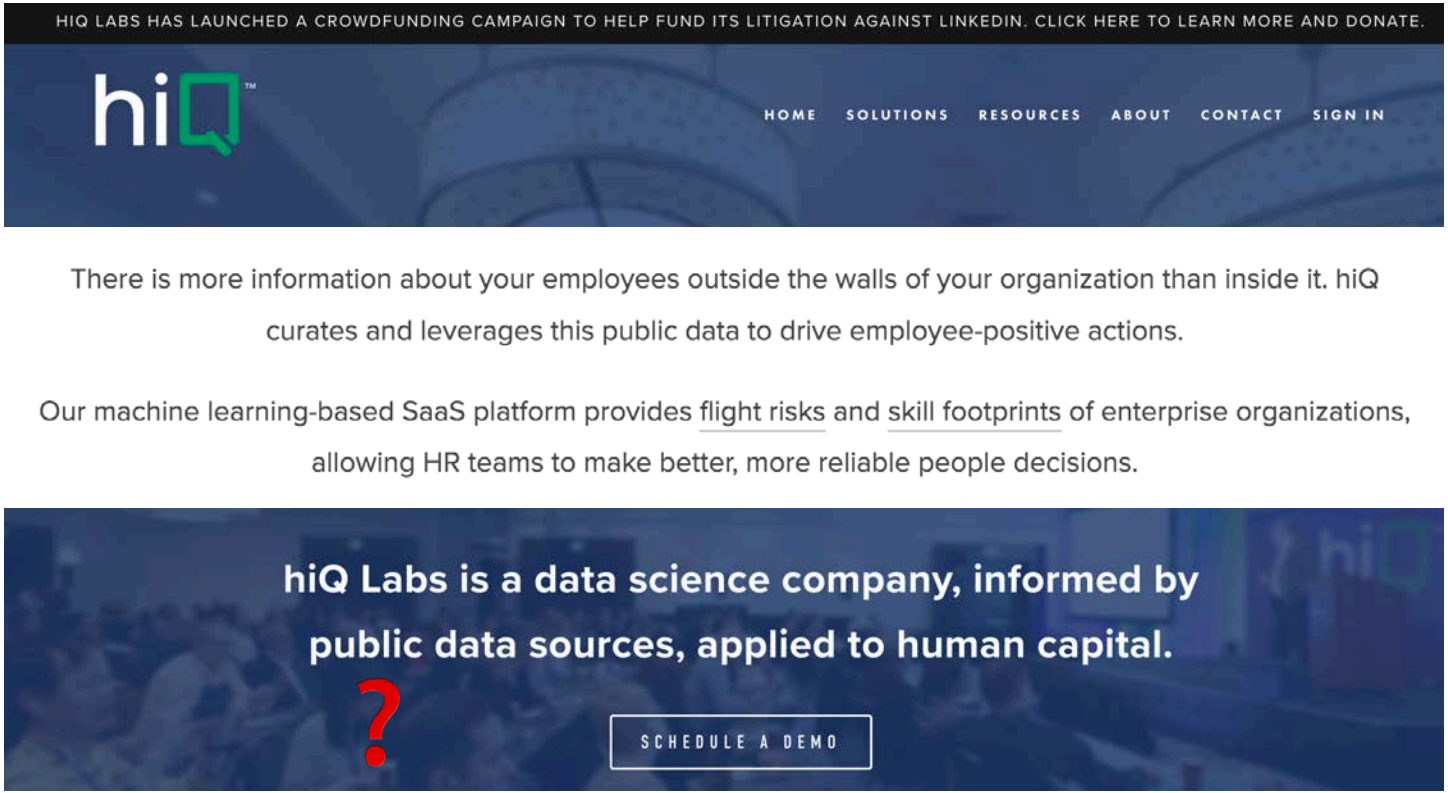
We do our best to keep Facebook safe, but we cannot guarantee it. We need your help to keep Facebook safe, which includes the following commitments by you:

1. You will not post unauthorized commercial communications (such as spam) on Facebook.
2. You will not collect users' content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without our prior permission.
3. You will not engage in unlawful multi-level marketing, such as a pyramid scheme, on Facebook.

"You will not collect users' content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without our prior permission."

https://www.facebook.com/legal/terms

2. WEB SCRAPING (hiQ v. LinkedIn)



AUGUST 14, 2017

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

HIQ LABS, INC., Plaintiff, v. LINKEDIN CORPORATION, Defendant.	Case No. 17-cv-03301-EMC **ORDER GRANTING PLAINTIFF'S MOTION FOR PRELIMINARY INJUNCTION** Docket No. 23

I. INTRODUCTION

Plaintiff hiQ initiated this action after Defendant LinkedIn issued a cease and desist letter and attempted to terminate hiQ's ability to access otherwise publicly available information on profiles of LinkedIn users. The letter threatens action under the Computer Fraud and Abuse Act (CFAA). LinkedIn also employed various blocking techniques designed to prevent hiQ's

2. WEB SCRAPING
Key Take-Aways

If scraped data is a key asset and essential to the business model, it is important to understand the details of the scraping and assess (& allocate) risks, remediation options, and short and long term strategies.

Keep an eye on the key active lawsuits because the law is evolving.

hiQ v. LinkedIn
Sandvig v. Sessions (ACLU case)

https://www.aclu.org/cases/sandvig-v-sessions-challenge-cfaa-prohibition-uncovering-racial-discrimination-online

3. GDPR IMPACTS

1. **Does GDPR throttle the business model?**
   - For example, targeted online behavioral advertising in certain areas (health, financial, educational, race, gender etc.) may be in trouble.
   - Surprising and “creepy” uses of consumer data are also at risk.
   - The combination of the seller data with the buyer data may not be permitted by EU DPAs. What is the plan for handling this issue?

2. **Are there business-significant special aspects of GDPR** that differ from US law in non-intuitive ways (for example: children under 16 versus under 13, opt-in versus opt-out consent, etc. ...).

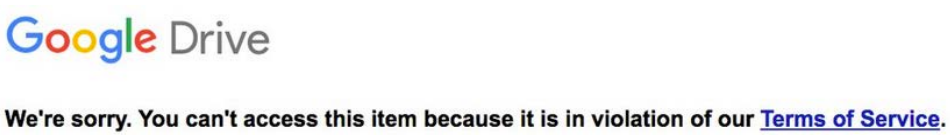
3. **Can you share personal data of European residents during diligence?**

4. **If there has been a breach, who will bear the risk of a GDPR fine?**

5. **TAG ALL EUROPEAN DATA BEFORE IT IS INTEGRATED INTO ANY OTHER DATABASE.**

Surprising use of data? GDPR Problem?

Google Docs Glitch That Locked Out Users Underscores Privacy Concerns



The New York Times

By MAYA SALAM OCT. 31, 2017

Google Docs threw some users for a loop on Tuesday when the service suddenly locked them out of their documents for violating Google's terms of service. The weird part? The documents were innocuous. The alerts were caused by a glitch, but they served as a stark reminder that not much is truly private in the cloud.

"This shows that Google is using advanced machine learning and other A.I. technologies to examine vast amounts of information in near real time," Dana Gardner, a leading cloud expert and a principal analyst at Interarbor Solutions, said on Tuesday.

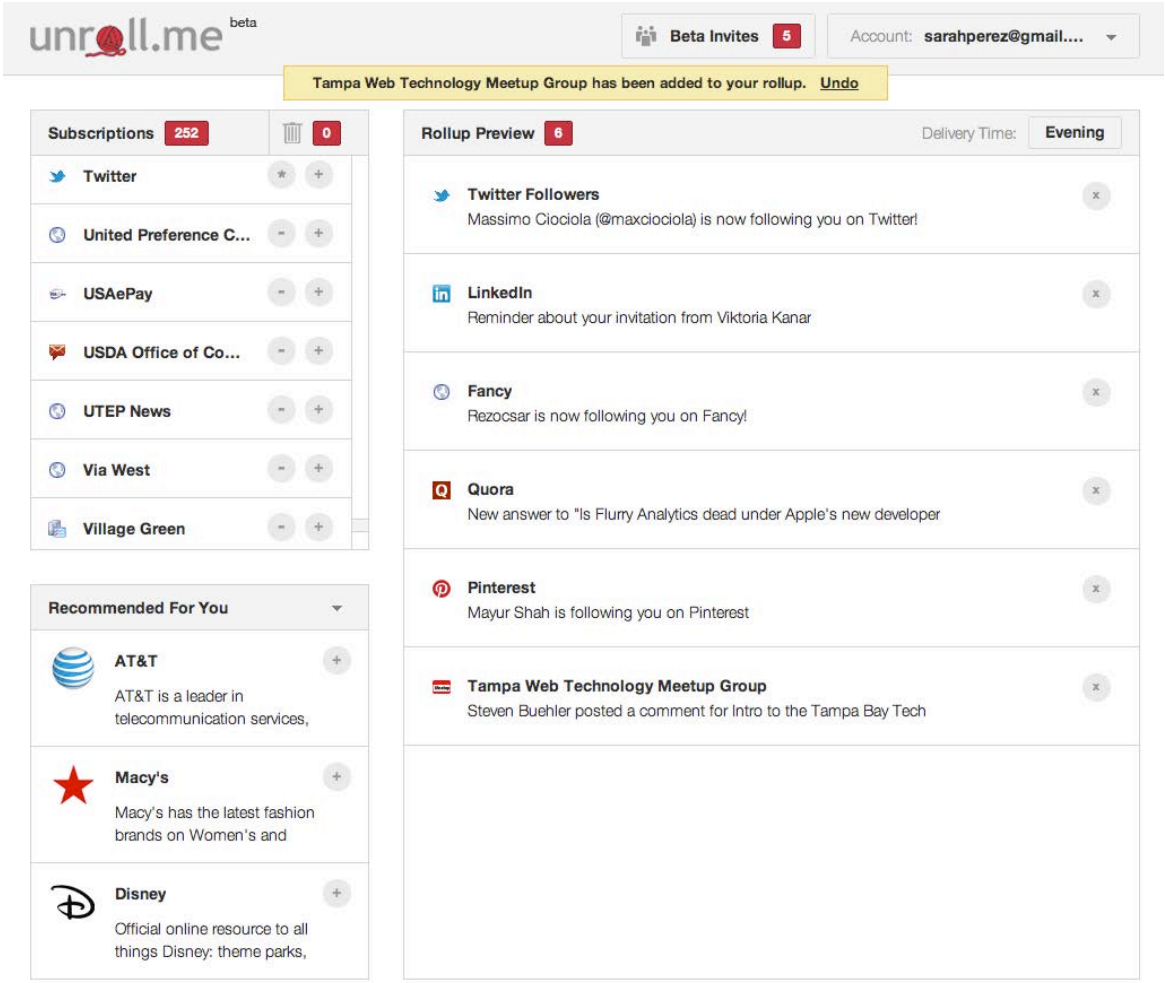
Surprising use of data? GDPR Problem?

Unroll.me hit with privacy suit over alleged sale of user data

The inbox cleanup service has been accused of violating federal privacy laws by allegedly harvesting user data.

Cnet April 26, 2017

Unroll.me offers a free service that promises to organize your inbox by sorting subscription emails and letting you unsubscribe from the ones you don't want. But according to reports, Unroll.me also tracked emailed receipts sent by the ride-sharing company Lyft, and **sold them to Uber**, Lyft's biggest competitor.

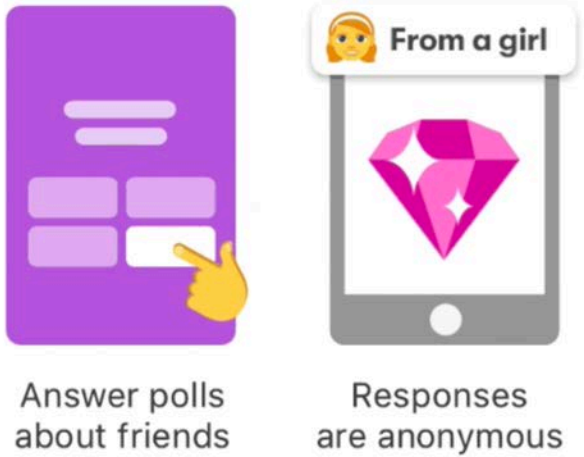

unroll.me beta
Beta Invites 5
Account: sarahperez@gmail....
Tampa Web Technology Meetup Group has been added to your rollup. Undo
Subscriptions 252
0
Twitter
United Preference C...
USAePay
USDA Office of Co...
UTEP News
Via West
Village Green
Recommended For You
AT&T
AT&T is a leader in telecommunication services,
Macy's
Macy's has the latest fashion brands on Women's and
Disney
Official online resource to all things Disney: theme parks,
Rollup Preview 6
Delivery Time: Evening
Twitter Followers
Massimo Ciociola (@maxciociola) is now following you on Twitter!
LinkedIn
Reminder about your invitation from Viktoria Kanar
Fancy
Rezocsar is now following you on Fancy!
Quora
New answer to "Is Flurry Analytics dead under Apple's new developer
Pinterest
Mayur Shah is following you on Pinterest
Tampa Web Technology Meetup Group
Steven Buehler posted a comment for Intro to the Tampa Bay Tech

Under 16 versus under 13? GDPR Problem?

What is TBH, Facebook's newly acquired anonymous teen compliment app?

The Washington Post

By Hamza Shaban October 17



Anyone older than 13 can use the app, but TBH targets teens and their social networks, asking first-time users to select their high school grade and to identify their school or college.

Data combination not OK under GDPR?

E.U. Fines Facebook $122 Million Over Disclosures in WhatsApp Deal

New York Times May 18, 2017

The European Union's antitrust chief, Margrethe Vestager, said that Facebook had told the European Commission, the executive arm of the European Union, that the social network would not combine the company's data with that of WhatsApp, which has more than one billion users.

Yet last August, Facebook announced that it would begin sharing WhatsApp data with the rest of the company. That could allow it to gain an unfair advantage over rivals, by giving it access to greater amounts of data to help support its online advertising business.

Data combination not OK under GDPR?

CVS reportedly offers over $66B to acquire Aetna

By Reuters

October 27, 2017 | 1:23am | Updated

GDPR: Sharing data during M&A negotiations?

Home » Privacy Policy

PRIVACY POLICY

Effective Date: April 24, 2017.

Amazon to buy Whole Foods Market in deal valued at $13.7 billion

Washington Post June 16, 2017

Sharing of Information

...

we may share Personal Information/Personal Data about you as follows:

In connection with, **or during negotiations of, any proposed or actual** merger, purchase, sale (including a liquidation, realization, foreclosure or repossession), lease, amalgamation or any other type of acquisition of all or any portion of Whole Foods Market assets, financing, disposal, conveyance or transfer of all or a portion of our business to another company;

COMPARE TO 2013 PRIVACY POLICY

Sharing of Information

We will not sell or otherwise share personally identifying information with other people or nonaffiliated companies except for those purposes described above, or as required by law. However, we will share this information with certain business partners to provide requested service that we do not provide directly, but we will only share personal information with these business **partners if they agree not to disclose the information to other parties and agree not to use this information to solicit business from you**.

https://www.wholefoodsmarket.com/20131104privacy-policy-archived

GDPR: How to handle risk of fine in data breach?

Tesco would face fines of up to £1.9bn under GDPR for Tesco Bank breach

Entire Tesco group would be in the firing line - with demands for more payouts on top from class-action lawsuits

computing

08 November 2016

GDPR: How to handle risk of fine in data breach?

TalkTalk gets record £400,000 fine for failing to prevent October 2015 attack

(PRE-GDPR) **05 October 2016**

ICO investigators found that the cyber attack between 15 and 21 October 2015 took advantage of technical weaknesses in TalkTalk's systems. The attacker accessed the personal data of 156,959 customers including their names, addresses, dates of birth, phone numbers and email addresses. In 15,656 cases, the attacker also had access to bank account details and sort codes.

The data was taken from an underlying customer database that was part of TalkTalk's acquisition of Tiscali's UK operations in 2009. The data was accessed through an attack on three vulnerable webpages within the inherited infrastructure. TalkTalk failed to properly scan this infrastructure for possible threats and so was unaware the vulnerable pages existed or that they enabled access to a database that held customer information.

QUESTIONS?


Ages 6 and Up
MAGIC 8 BALL
8
Ask a Question...
Turn over for the Answer!
TRY ME!

Thanks to our expert panelists ...

Jon Adams, Senior Privacy Counsel, LinkedIn. CIPP/US

- part of a team that oversees LinkedIn's privacy and data protection compliance program.
- Wilson Sonsini Goodrich & Rosati PC – privacy & technology transactions
- Sidley Austin LLP - product, transactional, and compliance counseling relating to privacy, data protection, cybersecurity, and IP matters
- FTC, Bureau of Consumer Protection – consumer protection & privacy law enforcement; policy

Rocco Grillo, Executive Managing Director/Cyber Resilience Leader
Stroz Friedberg/Aon

- serves on Stroz Friedberg's executive management team
- leads Cyber Resilience business - incident responders and security scientists
- Protiviti – Managing Director and Global Leader of Incident Response & Forensics
- RedSiren Technologies, Director
- Lucent Technologies

STROZ FRIEDBERG
an Aon company

AGENDA

9:15am - 10:15am Mergers & Acquisitions – Data Privacy & Security
Jon Adams, Senior Privacy Counsel, LinkedIn
Rocco Grillo, Executive Managing Director, Cyber Resilience Leader, Stroz Friedberg/Aon
Sayoko Blodgett-Ford, Member & Chief Privacy Officer, GTC Law Group

10:15am - 11am Beyond the Basics: Recent Developments in Global Data Privacy & Security
David Bender, Special Counsel, Data Privacy, GTC Law Group and Distinguished Fellow, Ponemon Institute

11am - 11:10am *BREAK*

11:10am - 12:10pm Vendor Risk Management – Data Privacy & Security
Sherry Ryan, CISO, Juniper
Tanya O'Connor, Director, Information Security, Arcadia Healthcare Solutions
Gary Roboff, Senior Advisor, Santa Fe Group - Shared Assessments
Rick Olin, Shareholder, CIPP/US, GTC Law Group

12:10pm - 12:30pm Closing

DAVID BENDER
Special Counsel - Data Privacy

GTC
LAWYERS + STRATEGISTS

Ponemon Institute Distinguished Fellow

WHITE & CASE

- Co-founded the Privacy practice, and founded the IP practice, at White & Case, and headed that firm's Privacy practice. Work included privacy audits to bring corporations into global compliance, vetting proposed conduct of multinationals to ascertain compliance with pertinent privacy laws, advising on cross-border data transfer, and counseling clients regarding various other privacy matters.

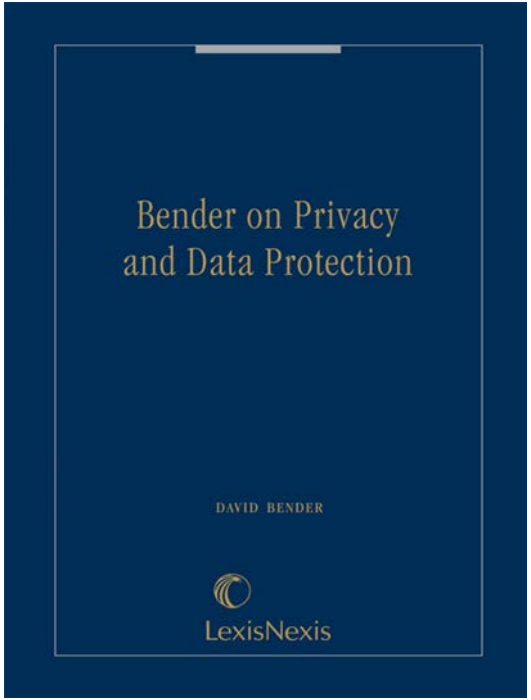
AT&T

- Served in-house at AT&T for 10 years, during the latter half of which he was responsible for all IP litigation brought by or against any Bell System company.

PACE UNIVERSITY

- Teaches Privacy Law at the University of Houston and Pace University.

LexisNexis



Bender on Privacy and Data Protection

by David Bender (Author)

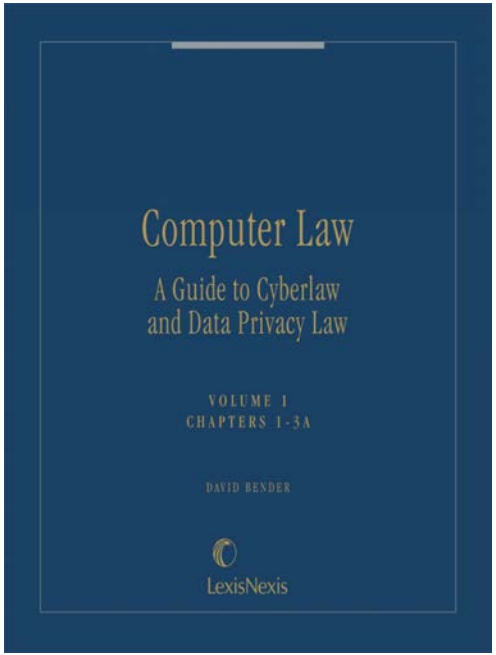
Publisher: LexisNexis

Select a format

eBook :mobi ISBN: 9780769890630 Published: October 09, 2014 IN STOCK	Price $268.00	QTY - 1 +
eBook :epub ISBN: 9780769890630 Published: October 09, 2014 IN STOCK	Price $268.00	QTY - 1 +

https://store.lexisnexis.com

LexisNexis



Computer Law: A Guide to Cyberlaw and Data Privacy Law

by David Bender (Author)
Publisher: Matthew Bender
Frequency: (2 issues)

Print Book :6 Volumes; Looseleaf updated twice annually
ISBN: 9780820510682
IN STOCK

eBook :epub
ISBN: 9781579113940
IN STOCK

eBook :mobi
ISBN: 9781579113940
IN STOCK

https://store.lexisnexis.com