Privacy Law & Digital Marketing for Business Lawyers

Dale Skivington, Chief Privacy Officer, Dell

Deborah Howitt, Director, Lewis Bess Williams & Weese

Privacy Law Framework

Numerous different laws and regulations govern the collection, use, and security of personally identifiable information ("PII")

- FTC
- State privacy & security laws
- Federal sectoral laws (HIPAA, GLBA, FERPA, etc.)
- International laws
- Marketing laws – spam, promotions, etc.
- Children (COPPA)
- TCPA and other FCC requirements
- FCRA and equal opportunity laws if using "big data"
- Self regulatory regimes

Federal Trade Commission

Authority from Sec. 5 of FTC Act "Unfair and deceptive trade practices" in commerce

- **Deceptive**: "material representation, omission or practice that is likely to **mislead** the consumer acting reasonably in the circumstances, to the consumer's **detriment**"
  - Use/dissemination of PII in violation of a privacy policy / broken promises
  - Insufficient notice
  - Poor security practices if promised otherwise
- **Unfair**: likely to cause substantial **injury** to consumers **without countervailing benefit** to consumers or competition, and is **not reasonably avoidable**
  - Retroactive changes, deceitful collection, improper use, unfair design/default settings, "unfair" data security practices, more

Federal Trade Commission (cont.)

FTC focus on marketing/advertising:

- Privacy policy disclosures (web and mobile):
  - Provide appropriate notice re: intended use of data
  - Obtain consent as appropriate based upon nature of the data/uses
  - Honor the consumer's choices re: use of the data
  - Say what you do/do what you say
  - Disclose material connections
- Examples of enforcement:
  - Failure to disclose material connection/incentive (Cole Haan)
  - Misrepresentation re: privacy of information (Facebook)
  - Deceptive tracking of location to deliver geotargeted ads (inMobi)
  - Insufficient disclosure of location advertising/tracking (Nomi)

FTC: CAN-SPAM

FTC enforcement

Applies to commercial emails “message /w primary purpose of which is commercial advertisement or promotion of commercial product or service”

- Compare with transactional/relationship message
- Need to evaluate if contains elements of both

Prohibits knowingly sending of commercial messages with intent to deceive or mislead recipients

If one company sending on behalf of another, both can be liable for violations

FTC: CAN-SPAM (cont.)

Basic requirements:

- Opt-out – must include unsubscribe link in every email, must process in 10 bus. Days
  - Opt-out means must be functional for 30 days
- No false or misleading header info (sender, of the message etc.)
- No deceptive subject lines
- Identify message as an ad
- Include physical address
- Additional requirements for sexually explicit content

FTC: COPPA

Children's Online Privacy Protection Act

Applies to sites/apps if:

- Directed at kids or
- Actual knowledge that collecting information from users under age 13
  - Doesn't apply to data re: kids if collected from adults

Primary requirements:

- Post notice on site re: what information is collected from children, how used, and disclosure practices for such information
- Obtain verifiable parental consent for the collection, use, or disclosure of personal information from children **before** collected
  - Parents have right to restrict access and use, and to obtain copy of info collected)
- Maintain confidentiality & security of information collected from kids
- Prohibit conditioning a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary

FTC: COPPA (cont.)

- Applies to active collection or **enabling** child to make PII available
- Site owner can be liable for third parties operating on their sites
  - e.g. ad network w/ actual knowledge collecting from under 13
- COPPA defines PII very broadly:
  - voice, audio, image
  - geolocation data revealing a street name plus city
  - online contact info (screen name etc.)
  - persistent identifier that recognizes users across time and sites (e.g. IP address)

State Data Privacy/Security Laws

Applicable based on location of the consumer

PII covered varies - typically name + SSN, drivers license, credit/debit or financial acct. w/ password

- Broader in some states (any online acct/pswd, biometric data, etc.)

Variations – some to watch include

- MA is the most stringent re: security
  - Requires written policies with specific elements, and includes computer security requirements, encryption requirements, and much more
  - Must oversee service providers (+ contracts)
- NV incorporates PCI and has encryption requirements

State Data Privacy/Security Laws (cont.)

California – leader in data privacy

- Security requirements for PII
  - Reasonable measures, also must contractually require for service providers
- Online privacy policies
  - Policy must be conspicuous
  - Websites must disclose
    - how they respond to Do Not Track (DNT) signals from browsers and other mechanism
    - whether third parties use or may use the site to track (*i.e.*, collect personally identifiable information about) individual California residents "over time and across third party websites."
- "Online eraser" law for minors
  - Sites and apps "*directed*" to minors, *or that have actual knowledge* that a user is a minor, must allow registered users under 18 to remove (or ask the provider to remove or anonymize) publicly posted content
- Restricts online advertising of certain categories to kids under 18

State Data Privacy/Security Laws (cont.)

Data breach notification laws

Typical elements in state statutes

- Who is covered by the statute
  - Typically any entity that owns or licenses (or has possession) of PII of the state's resident
  - Sometimes "does business in the state"
  - Sometimes different for state government agencies
- Trigger for notification
  - Access, misuse, etc.
  - PII covered (varies)
  - Encryption safe harbor – several states

State Data Privacy/Security Laws (cont.)

Breach notification laws (cont.)

- Timing of notification
  - Typically as soon as possible (subject to law enforcement)
  - Some specific requirements e.g. stated # of days (for consumers or AG)
- What the notice must contain (or not contain)
- How notice may be delivered
- Other parties to be notified
  - AG, credit bureaus, etc.
  - Sometimes based on number of state residents impacted
- Enforcement – AG only, private right of action

“Little FTC Acts” – State Laws

Focus on unfair/deceptive trade practices

State law elements vary

- Typically private right of action
- Some include punitive damages
- Some include minimum damages

CO Consumer Protection Act:

- Private citizen must prove five elements:

  (1) unfair or deceptive trade practice;

  (2) in the course of the defendant’s business;

  (3) significantly impacted actual or potential customers;

  (4) the plaintiff suffered an injury to a legally protected interest;

  (5) the deceptive trade practice caused the plaintiff’s injury

Telephone Consumer Protection Act - TCPA

FCC enforcement

- Prior **express** consent required for autodialed calls/pre-recorded messages (includes texting)
  - Burden on company to show proof of the consent (track in CRM)
    - Best practice: maintain each consumer's written consent for at least four (4) years (federal statute of limitations to bring an action under the TCPA)
  - Limited exceptions for established business relationship, nonprofits, other
  - Consent may not a condition of purchase
- Do not call list – must check against this before making calls
- Timing requirements for certain calls
- Private right of action

Federal Sectoral Laws

Several federal sectoral privacy laws have provisions limiting sharing and/or use of data and will impact marketing

- Gramm-Leach Bliley Act – disclosure notices, sharing provisions, opt-out
- HIPAA - limitations on use of protected health information for marketing
- Family Education Rights & Privacy Act – limits use/disclosure of student records
- Video Privacy Protection Act – limitations on certain disclosures (including for marketing)

Sweepstakes and Contests

- Sweepstakes = game of chance
  - Must not have element of consideration (illegal lottery)
  - Eliminate consideration by free alternate method of entry
- Contest = skill or measurable achievement
  - Include criteria by which entries are judged
  - Ok to have consideration
- Be aware of the following:
  - Requirements to register/post bond in certain states if prize value exceeds stated amount
  - Canadian requirements
  - If joint promotion, be sure data rights, use, sharing are clearly disclosed

Self Regulation

Leading marketing and advertising industry associations collaborated to form the Digital Advertising Alliance (DAA)

- Initiated a comprehensive, self-regulatory effort and enforcement standards for online behavioral advertising (OBA)
- Goal of answering the FTC's calls to foster transparency, knowledge and choice for consumers re: online behavioral advertising w/ 7 principles:
  - Education – of consumers re: OBA
  - Transparency – deployment of multiple mechanisms for clearly disclosing and informing consumers about data collection and use associated with online behavioral advertising
  - Data Security - reasonable security for, and limited retention of, data collected in OBA
  - Material Changes - obtain consent before applying any change to OBA policies
  - Sensitive Data - certain data collected and used for OBA merits different treatment (kids, financial, health)
  - Accountability - develop and implement policies and programs to further adherence to Principles.

Guidance re: ads on websites, mobile, cross device, online video, etc.

Self Regulation

DAA Enhanced Notice Requirements - on every web page where data is being collected or used for OBA

- NOTE: "or used" includes ads on third party sites being targeted based on data collected elsewhere
  - The link should:
    - indicate that OBA is taking place on the page (can display DAA's Icon)
    - link directly to the place in the website's privacy policy that describes the site's OBA practices and points to an "industry-developed Website," such as aboutads.info, where consumers can opt-out of behaviorally targeted ads
    - Websites should state that they adhere to the DAA Principles.
  - DAA indicates that if sites fail to comply, they may face a formal compliance review by the DAA (which may result in referral to the FTC for enforcement)

International Laws - Canada

PIPEDA - Personal Information Protection and Electronic Documents Act

- Applies to all personal data - information ‘about’ identifiable individuals
- Applies unless a provincial analogue is substantially similar
  - BC, Alberta and Quebec have own laws
- “Adequate” for purposes of EU

International Laws - Canada

PIPEDA requires adherence to 10 principles

- **Accountability** – Organization responsible for personal information under its control, must designate individual
- **Identifying Purposes –** at time of collection, state purpose of collection
- **Consent –** typically required collection, use, or disclosure of personal information
- **Limiting Collection** – only collect what is necessary for purposes identified; use fair & lawful means.
- **Limiting Use, Disclosure, and Retention** – only use for purpose collected or consented, dispose when no longer needed for the purpose
- **Accuracy** – ensure accurate, complete and up to date
- **Safeguards –** use reasonable security measures to protect, appropriate to sensitivity
- **Openness** – make information about policies/practices re: information readily available
- **Individual Access** – individuals have the right to their information, and to challenge accuracy/have it amended
- **Challenging Compliance** – right to address compliance issues w/ the organization's responsible individual

International Laws - Canada

The Canada Anti Spam Law (CASL)

"Commercial Electronic Messages"

- Encourages commercial activity
- Not messages re: existing biz, e.g. invoice
- Includes SMS

Must ID sender

Consent required

- Must opt-in (e.g. checkbox)
- Must allow opt-out
- Can transfer consent, but complex
- Implied consent if inquiry (6 mo. ONLY)

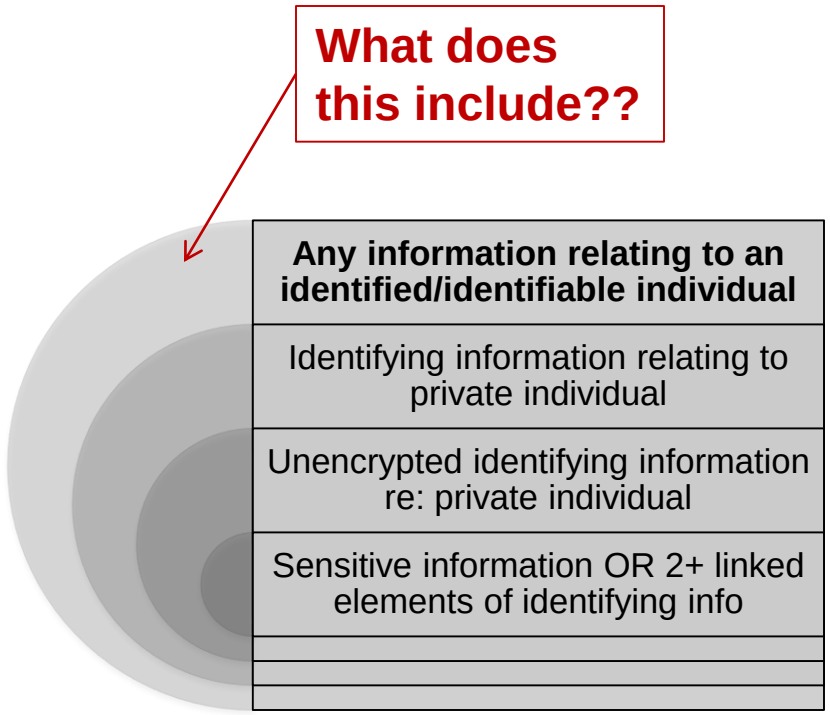
Exceptions for family/personal relations

International Laws – EU/UK

- EU Data Protection Directive
  - Notice (about collection + use of PII)
  - Choice (re: how data is used, express consent sometimes required)
  - Data Security (must take reasonable precautions to secure data)
  - Data Integrity (data collection limited by intended use, current, accurate)
  - Access (data subject allowed access to view, correct, modify, delete data)
  - Enforcement (recourse mechanism, remedies)
  - Onward Transfer (limitations on transfers to third parties and internationally)
- EU Cookie Consent Banner/Policy
  - Advance notice/consent for non-essential cookies
- Opt-in required for marketing in EU (double opt in for Germany)
- May only transfer to countries w/ “adequate” protections for PII (U.S. not adequate)
  - Privacy Shield
  - Model Clause Agreements
  - Binding Corporate Rules

International Laws – EU/UK

- Personal Data
  - “any information relating to an identified/identifiable individual”
- Sensitive Data
  - “data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union memberships, health, and sex life (+ orientation)”



International Laws – EU/UK

- GDPR – coming soon!

Current Data Protection Directive 95/46/EC	Changes created by GDPR
European reach only	Global reach
Local law divergence across 28 EU states	Regulation: uniform across EU
Multiple Data Protection Authority ("**DPA**") exposure	"One stop shop"
Limited accountability	Accountability key!
Controllers only	Controllers and Processors
Small fines, differ between countries	Huge fines
No obligation to report breaches	Obliged to report breaches without delay
No obligation to have DPO	DPO required for larger organisations

International Laws – EU/UK

- Privacy Shield
- Means of transferring EU PII to U.S. even though U.S. not “adequate”
- Companies self-certify
- Privacy Shield Framework consists of several components:
  - 7 ‘core’ Data Protection Principles
  - 16 ‘supplemental’ Data Protection Principles
  - Oversight and enforcement standards
  - Government access/redress matters
- Annual Recertification
- Enforcement by FTC and Dept. of Commerce

Privacy Governance at Dell

Audit Committee of Board

Chief Ethics and Compliance Officer

Chief Privacy Officer

Privacy Managers | **Privacy Attorneys** | **Privacy Operations**

Sample Privacy Maturity Model

	1 Ad hoc	2 Initial	3 Formal	4 Validated	5 Monitored
Policy	None written	Limited distribution & understanding	**Formal but may be inconsistent**	Globally consistent & enforceable	Regularly reviewed & updated
Governance	None established	Discrete, informal, & limited	**Corporate oversight & exec level**	Management involvement at all levels	Scorecard reporting
Risk management	Incomplete & inconsistent	**Risk assessment, not management**	**Risk assessment & management**	Cross-functional, executive validation	Component of ERM
Procedures & controls	None written	**Limited coverage**	Consistent & global	Subject to self-assessment & audit	Exception reporting & resolution
3rd party management	No standards	Some standards May be inconsistent	**Consistent, cross-functional coordination**	Proactive monitoring & self-assessment	Independent external audits
Compliance & monitoring	None established	Informal & limited	**Audit-driven, remedial actions endorsed**	Analytics technology; cross-functional	Accountability-driven, extends beyond enterprise
Incident management	Ad hoc & inconsistent	Some consistency Little analysis	Root cause analysis, global standards	**Issue tracking Technology in place**	Effectiveness & efficiency metrics
Training & awareness	None	General, infrequent, single media	**Custom-tailored, recurring, multi-media**	Role-specific awareness; 3rd parties	Ongoing awareness

*Comprehensive Privacy assessments done in Commercial, Marketing, Software. Services assessment is ongoing.

Sample Privacy Risk Categories Modeled After GAPP

1. Management
2. Notice
3. Choice and Consent
4. Collection
5. Use, Retention, and Disposal
6. Access Disclosure to Third-Parties
7. Security for Privacy
8. Quality
9. Monitoring and Enforcement

Source: CEB analysis.

Choice and Consent

Risk	Risk Description
Privacy Policy Choice and Consent Risk	The risk that the company's privacy policies do not address the choices available to individuals and the consent to be obtained.
Choice and Consent Communication Risk	The risk that the company's privacy notice does not inform individuals about the choices available to them with respect to the collection, use, and disclosure of personal information and that implicit or explicit consent is required to collect, use, and disclose personal information, unless otherwise permitted.
Denying or Withdrawing Consent Risk	The risk that when personal information is collected, individuals are not adequately informed of the consequences of refusing to provide personal information or of denying or withdrawing consent to use personal information.
Implicit or Explicit Consent Risk	The risk that implicit or explicit consent is not obtained from the individual at or before the time personal information is collected or soon after.

Key Privacy Process Controls Supporting Marketing

- Incident Response Process
- Preference Management Process
- Third Party Privacy Management Process
- International Transfer Process
- Privacy Impact Assessment Process
- Online Behavioral Marketing/Cookie Management Process
- Data Subject Access Controls
- Training

Big Data and Profiling

1

White House: *Seizing Opportunities, Preserving Values-2014, 2015*

- report calling for national data breach legislation and privacy rights extended to non-U.S. citizens, among other recommendations, and warned of discrimination via Big Data.

2

Big Data: A Technological Perspective-2014

- President's Council of Advisors on Science and Technology (PCAST) released a report examining the current and likely future capabilities of key technologies, both those associated with the collection, analysis, and use of big data and those that can help to preserve privacy.

3

FTC workshop and report on Internet of Things

- In January 2015, the FTC issued a report and made recommendations regarding security, data minimization, notice, and choice

4

EU Article 29 Committee

- Issued guidelines on the Internet of Things, including PIA's, deleting data, consent, and data subject access.

5

Data Protection Commissioners Mauritius Convention

- October 2014 Declaration on the Internet of Things recommended that data be considered PII, notice and choice, and end to end encryption.

6

Consumer Bill Of Rights – March 2015

- President Obama released a discussion draft for omnibus privacy legislation including section on "respect for context" which would permit uses not previously envisioned if the organization performs PIAs and provides certain additional protections or submits to FTC Review Board.

7

EU General Data Protection Regulation- Effective May 2018

- Includes requirement for explicit consent for certain types of profiling

Potential for Big Data to do good is enormous

Ethical issues do arise and as a result…having a framework to consider and mitigate is a best practice and an emerging Legal requirement.

Ethical issues include

Privacy Concerns
Using data in a way your employees or customers would not have expected

+

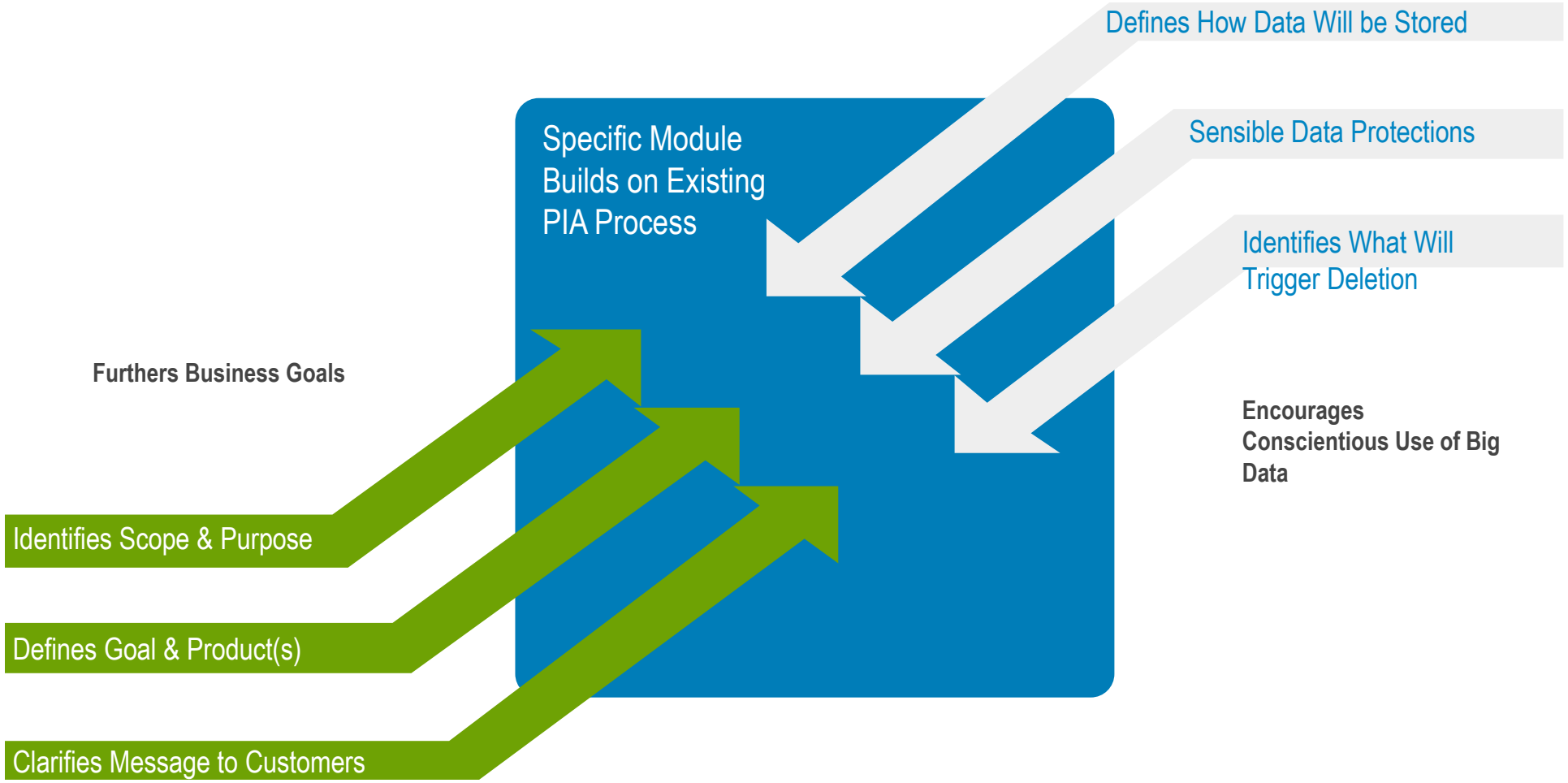
Discrimination Concerns
Using data in a way that adversely impacts a segment of stakeholders

Develop a Governance and Accountability Framework

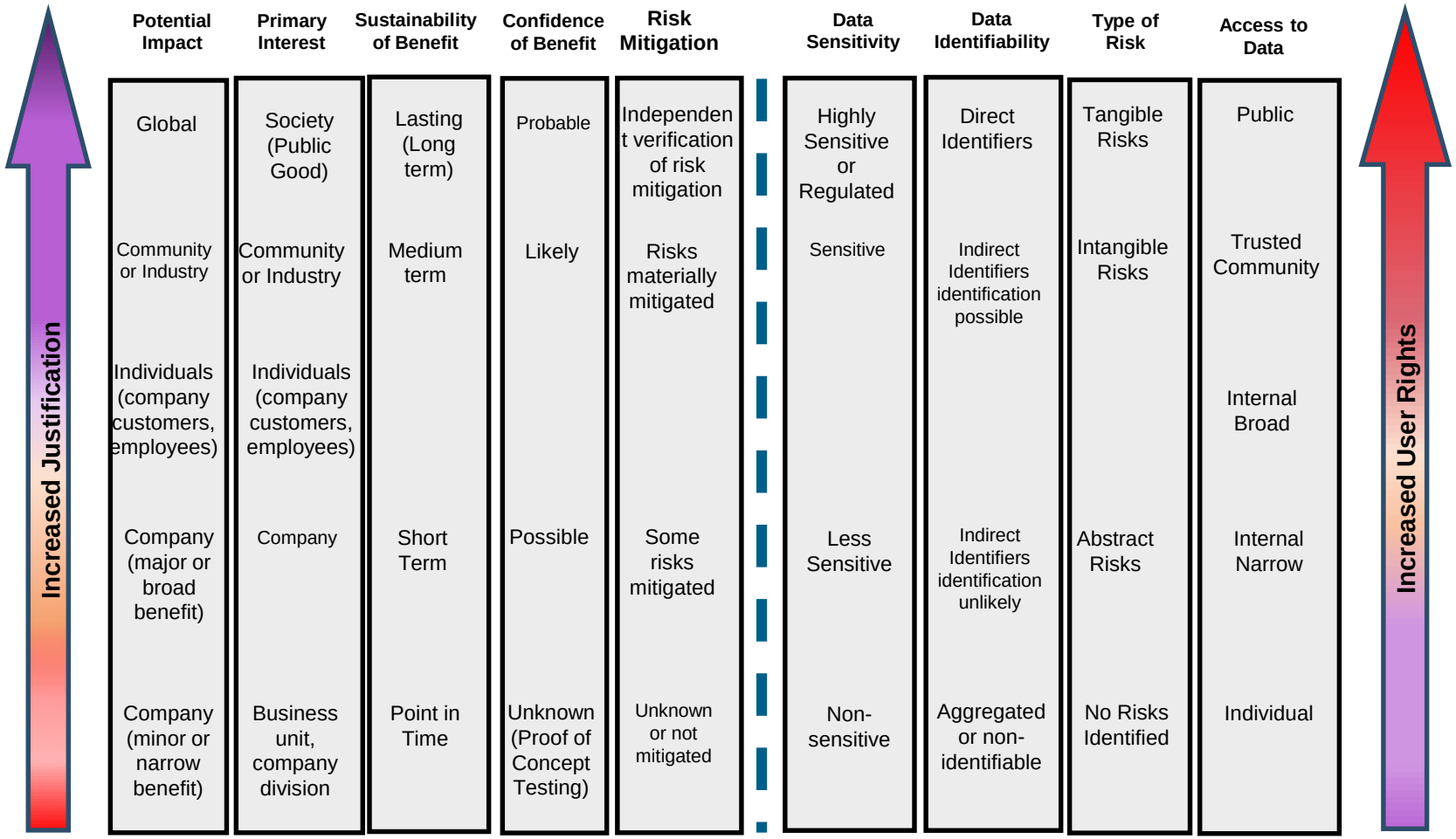
Framework Key Components:

- Include a Security and Privacy Impact Assessment
- Include a playbook on when, how and by whom these initiatives should be reviewed and approved
- Use tools which assist in balancing the company and your stakeholders interests to make the best ethical decisions

Privacy Impact Assessment for Big Data Projects



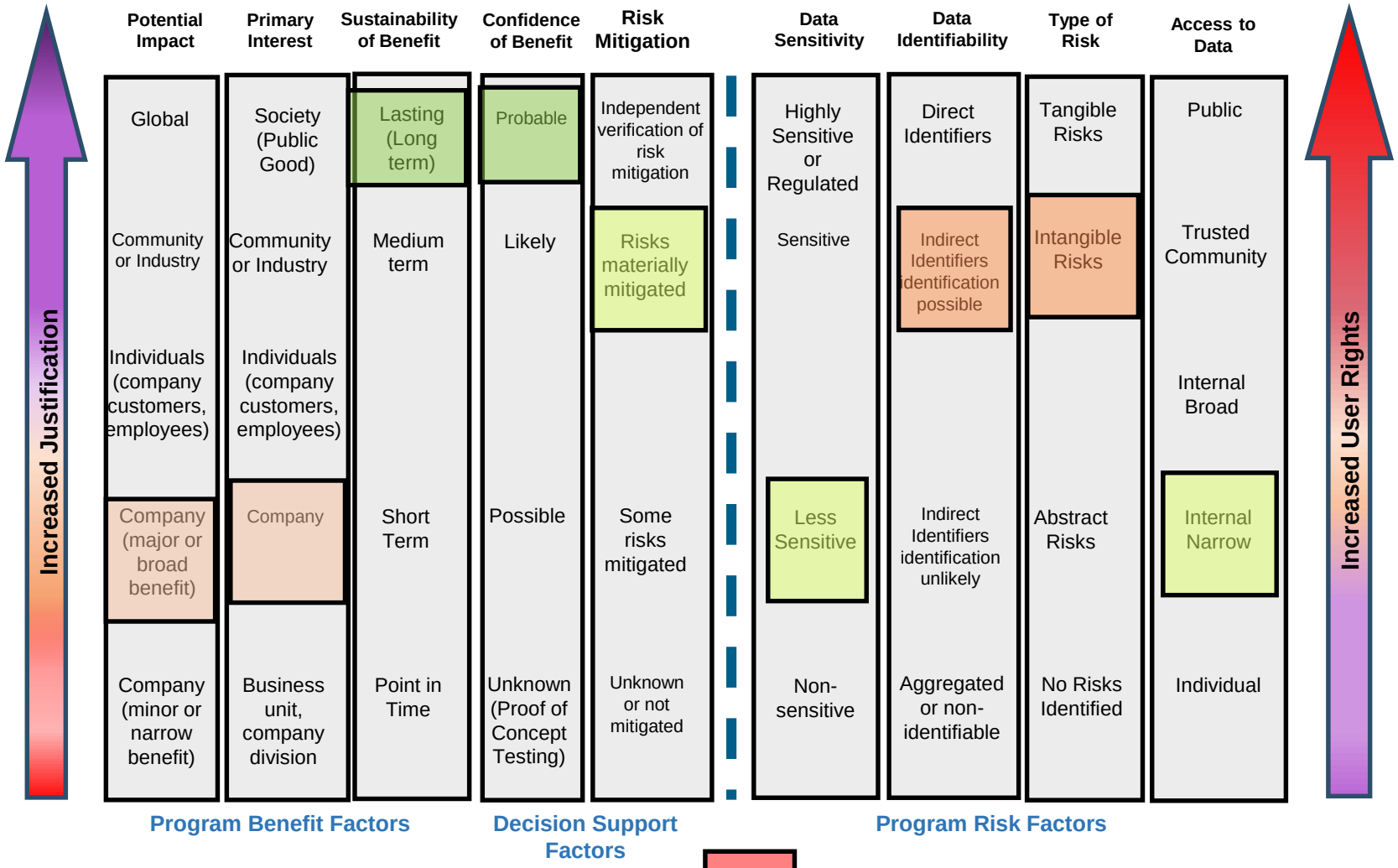
Proposed Risk-Benefits Analysis Tool for Analytics and Big Data Initiatives



Analytics Balancing Variant v4
June 2015
The Conference Board Council of Chief Privacy Officers

Proposed Risk-Benefits Analysis Tool for Analytics and Big Data Initiatives

Hypothetical Use: Evaluation of Consumer Customer Churn Initiative



Factor weighs against the project

Neutral factor

Factor weighs in favor of the project

Analytics Balancing Variant v4
June 2015
The Conference Board Council of Chief Privacy Officers

Ethical Obligations: MRPC

1. MRPC Rule 1.6: Duty of confidentiality
    - Must not reveal client information unless received informed consent from the client
    - Must take reasonable steps to guard against inadvertent, unauthorized disclosure of or access to client information
        - ensure that when transmitting information (email or otherwise) that security is in place to prevent disclosure
    - Comments to this rule indicate factors used in determining whether the attorney took reasonable steps to protect against inadvertent disclosure include, but are not limited to:
        - Type of information;
        - Safety of the information without additional security measures;
        - Cost of the additional security measures, and
        - Whether those safeguards impede the attorney's ability to represent the client and others

Ethical Obligations: MRPC (cont.)

2. MRPC Rule 1.1: Duty to provide competent representation

- Comments to Rule 1.1 require that attorneys must "keep abreast of changes in the law and its practice *including the benefits and risks associated with relevant technology*"
  - Lawyers should know the safeguards in place and the limitations of those safeguards when storing or transmitting information
  - OK to rely on third party technology experts per ABA Cybersecurity Handbook

3. MRPC Rule 5.1: Must also supervise junior lawyers and non-lawyers to ensure their conduct "is compatible with the professional obligations of the lawyer" (e.g. make sure they also use required security measures)

Ethical Obligations: MRPC (cont.)

Additional security protections apply to all information relating to clients and client matters

- Don’t store client information on personal devices or accounts, send to personal email, or leave accessible to unauthorized parties
- Information and documents relating to client representations should be stored securely in accordance with your firm’s policies
- Try not to use public or insecure networks to handle client information unless:
  - you use VPN (to encrypt traffic) and
  - you do not tell the computer to “remember” the connection (e.g. no auto-reconnect next time you are at that location)
- Don’t use public computers for client work

Remember that many privacy laws/regulations also contain data security requirements

- State laws, FTC, federal sectoral laws