LEGITIMATE INTERESTS AND UNFAIR PRACTICES - EQUIVALENT PROCESSES

MARTIN ABRAMS & LYNN GOLDSTEIN
Posing the Key Questions

1. Does one need to think beyond small “p” privacy to the full range of interests?
2. Are legitimate interest assessments in Europe and elsewhere similar to unfairness assessments in the U.S.?
3. Will demonstrating that processes are fair when one thinks with data achieve the risk proofing necessary in 2017?

To answer those questions, one needs to look at the environment.
U.S. Competitive Business Advantage

• American businesses (with limited exceptions) are free to “think with data”
  – Almost everywhere else, “playing with data” requires establishing a legal basis to do so

• Most profiling (the fruit of thinking with data) is not regulated
  – Only “acting” with profiles in an inappropriate fashion is regulated

• Business observation norms are self regulatory in nature
  – FPF has played a leading role in this domain

• This competitive advantage is well known outside the U.S. by both non-U.S. business and policymakers
The Regulatory Environment

• Globally, we are in a privacy regulatory bear market
  – European Court of Justice – Independent regulators should empower individuals by investigating their complaints
  – 2018 - EU fines of up to 4% global turnover
  – Colombia, Canada, and other locations discussing granting of fining power directly to regulators or increasing fines
  – UN report: facilitate global data flows by harmonizing enforcement at a higher level
  – FCC pending privacy rule making
  – Standards associated with Privacy Shield
  – Courts everywhere becoming more activist

• Norming outside the U.S. has influence within the U.S.
Privacy Law Has Two Foundations

• Privacy law in the U.S. and most of the world encompasses privacy (individual information autonomy) and fair processing
  – So, privacy means both the full governance of data related to people as well as the assurance of values related to individual control
  – For purposes of clarity, the value will be referred to as small “p” privacy
• European law is more explicit
  – Privacy is a fundamental constitutional right to assure individual freedom, dignity, and protection of family life
  – Data protection, with the GDPR, is a constitutional and statutory right to fair processing to protect privacy but also assures the full range of “rights and freedoms”
    • This is a slight change from the past implementation of the Directive via local laws
  – How privacy as a value and fair processing as a statutory right go together is very much in play over the next two years
  – The data protection covers the full range of rights impacted by data, including health, education, and economics
• In the U.S., we speak about the values and act based on fair processing
• As professionals, it is useful to differentiate between small “p” privacy and fair processing
Technology Has Made Small “p” Privacy More Difficult

• First web browser - 1993
• Fixing Y2K problems with common processing modules – 2000
• RFID expanding automated observation beyond the Internet – 2004
• Precursors to Big Data - 2006
• iPhone released – 2007
• Internet of Things – 2010?
• Term big data coined by “Economist” - 2010
• Wearables becomes a thing - 2013
Understanding the Challenge of Data Migration

- Data may be classified into four categories
  - Individually provided
    - Governable by individuals
  - Observed
    - The sheer amount challenges autonomy
  - Derived
    - Depends on the underlying data
  - Inferred (also known as “created”)
    - The product of probability
    - Inferred data is data, and is used in further processing
Nature of Today’s Data Use Creates a Dilemma

• Privacy feels best when individuals have control
  – But even the best notices are long, complicated, layered
  – With created data how does one even inform?

• Advanced analytics is, if we are honest, a repurposing for “thinking with data”

• So even where the belt of consent (choice) creates a legal permission, the suspenders of the demonstration of fair processing is required to support that permission

• That is where concepts such as legitimate interests comes into play
European Law Requires Using the Right Legal Permission

(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for **compliance with a legal obligation** to which the controller is subject; or

(d) processing is necessary in order to **protect the vital interests** of the data subject; or

(e) processing is necessary for the performance of a **task carried out in the public interest** or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).
Legitimate Interest

• Processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by the third party or parties to whom the data are disclosed

• Except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject
Balancing Process

• Controller legitimate interests versus the full interests of the individual
  – WP29 paper reminds us it is a data protection issue, i.e., full range of fundamental rights

• End of the day, the issue is fairness as it relates:
  – To the full range of individual’s interests
  – The risks from not using the data as well as those that come from the processing

• “Unified Ethical Frame for Big Data Analysis” established the concept of using the full range of interests for assessments

• “Enforcing an Ethical Big Data Assessment” established that ethical assessments are a legitimate interest process
Accountability Essential Elements

1. Corporate commitment to internal policies (maybe codes of conduct) that link to external criteria – data protection law
2. Mechanisms to put those policies into effect, including identifying risk to individuals and mitigating those risks (privacy-by-design)
3. Internal monitoring to assure mechanisms work
4. Individual participation (transparency and consent where appropriate)
5. Standing ready to demonstrate to a regulator on request, and remediation where necessary
IAF Work

• 2013 – Two-phase (discovery and application) approach by Abrams, Bruening, and Leta

• 2014 – Challenge to develop an assessment process that would be implementable, could be demonstrated, and could lead to trust

• 2014 – Unified Ethical Frame for Big Data Analysis

• 2015 – Enforcement Study

• 2016 – Legitimate interests

• 2016 – Effective Data Protection Governance
Assessments Begin with Flexibility in the White Space between the Lines in Legislation

• EU law includes legitimate interests based on balancing process
  – It requires a trusted balancing process
• FTC consent orders include requirements for accountability based in part on privacy by design
  – Include information impact assessments
  – Guidance hasn’t defined a balancing process
• Canadian law includes concepts of implied consent and legitimacy
• All require comprehensive information impact assessments (“CIIA”)
CIIAs Purpose is to Assure Processing is Legal, Fair, and Just

**Civil law data protection**
- All processing must have a legal basis
  - Where consent is ineffective one must demonstrate:
    - Fair
    - Just

**U.S. common law**
- Processing must not be illegal
  - But absence of legal prohibition is not enough, must be:
    - Not unfair
    - Just
Key Governance Concepts

- Data protection assures the full range of individual interests, not just a narrow definition of privacy
- Reticence risk is meaningful, real, and creates harms
- A fair and just assessment is necessary – what is the cost of not processing?
- This takes us beyond compliance to ethics
VALUES FOR AN ETHICAL FRAME

**Beneficial**
- Sense of purpose
- Define the benefits
- Parties who gain benefit
- Risk-Benefit balance

**Progressive**
- Materially better
- Measures
- Support innovation
- Consider risks

**Sustainable**
- Legal basis/permissions
- Influence of model(s)
- Longevity of insights
- Ability to refine/correct

**Respectful**
- Data origination/restrictions
- Context/Purpose
- Interests of all parties
- Expectations/Rights

**Fair**
- Insights/Applications
- Inferences/Discrimination
- Labeling/Predestination
- Compatibility/Legal Basis
CIIA Framework

- Full project description with clear intents
- Questions to identify issues related to processing and accountability
- Clear description of stakeholders
- A description of intended benefits and possible risks
- A final assessment of fairness based on facts
When Should CIIAs Take Place

• “Thinking with data” (discovery)
  – Project scoping
  – Discovery processing

• “Acting with data” (application)
  – Using insights to predict behavior
  – Reviewing for effectiveness
CIIA Process

• Step one: is a full assessment necessary?

• Step two: characterizing the Project
  – Accountability – Who owns it? Who is responsible? Who answers for it?
  – Purpose
  – Sources
  – Preparation
  – Contractual and Legal Conditions
  – Accuracy
  – Insights
  – Outcomes
  – Stakeholders
CIIA Process cont.

• Step 3: What are the benefits? Risks? Who is impacted?
  – Benefits
  – Risks/Mitigations
  – Risk/Benefit Analysis

• Step 4: Decision - It is legal, fair, and just because
  – These are the stakeholders!
  – These are the benefits that justify processing and mitigations that justify processing!
  – These are the residual risks that the organization is comfortable with
Standing Ready to demonstrate

- As part of an internal accountability process
- To an external regulator on request
- Externally when useful to drive trust
If Not Required in the U.S., Why Do It?

• In a regulatory bear market, the best defense is evidence of a sound assessment process
• Interoperability is useful in hostile global environments
• The suspenders of demonstrable add to the belt of individual choice
• Reticence risk is costly in an aggressive marketplace
• Similarities between FTC unfairness assessment and EU legitimate interests assessment facilitate encourage interoperability amongst global legal systems