Consumer Protection & Privacy in AI Applications

January 15, 2020

Daniel J. Weitzner weitzner@mit.edu, MIT IPRI Founding Director
AI Regulation is Data Regulation
Data Regulation is Privacy Regulation

AI Regulation is Privacy Regulation?
Overview: Privacy & fairness in data intensive environments

1. Views of privacy in tension -- always
2. Modern privacy practice -- Privacy as Fairness
   a. Fair Credit Reporting Act
   b. Equal Credit Opportunity Act
3. Internet-era Privacy
4. GDPR Revolution
5. Data analytics for fair analytics
Privacy: An essentially-contested concept

W.B. Gallie: “that in certain kinds of talk there is a variety of meanings employed for key terms in an argument, and there is a feeling that
• dogmatism (“My answer is right and all others are wrong”),
• skepticism (“All answers are equally true (or false); everyone has a right to his own truth”), and
• eclecticism (“Each meaning gives a partial view so the more meanings the better”) are none of them the appropriate attitude towards that variety of meanings.”

See also: Democracy, Art, Religion
Does privacy mean being alone?

“The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness….They conferred, as against the government, the right to be let alone - the most comprehensive of rights and the right most valued by civilized men.”

Or, working together?

This Court has recognized the vital relationship between freedom to associate and privacy in one's associations. Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs.

NAACP v. Patterson - 357 U.S. 449 (1958)
No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Article 12 Universal Declaration of Human Rights
Detour: traditional computer science view of privacy

Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.

Alan Westin, Privacy and Freedom (1967)
Jerry Saltzer/Mike Schroeder (CACM 1974)
Modern privacy begins in the mainframe era

Fair Information Practice Principles: (FIPPs)
1. Collection Limitation
2. Data Quality
3. Purpose Specification
4. Use Limitation
5. Security Safeguards
6. Openness
7. Individual Participation
8. Accountability
Fair Credit Reporting Act (1970):

- You must be told if information in your file has been used against you.
- You can find out what is in your file.
- You are entitled to free reports if a person has taken adverse action against you because of information in a report;
- You have a right to know your credit score.
- You can dispute inaccurate information with the consumer reporting agency.
- Your consent is required for reports that are provided to employers.
- You may choose to remove your name from consumer reporting agency lists for unsolicited credit and insurance offers.
- You may opt-out at the major credit bureaus
- You may seek damages from violators.
Equal Credit Opportunity Act (ECOA)

**Activities constituting discrimination:** It shall be unlawful for any creditor to discriminate against any applicant, with respect to any aspect of a credit transaction—

1. on the basis of race, color, religion, national origin, sex or marital status, or age (provided the applicant has the capacity to contract);
2. because all or part of the applicant’s income derives from any public assistance program; or
3. because the applicant has in good faith exercised any right under this chapter.

-- 15 USC 1601
Equal Credit Opportunity Act (ECOA) - Regulation B

Disparate Treatment

Example: A lender offers a credit card with a limit of up to $750 for applicants age 21–30 and $1,500 for applicants over 30. This policy violates the ECOA’s prohibition on discrimination on the basis of age.

Disparate Impact

A lender’s policy is to deny loan applications for single-family residences for less than $60,000. This minimum loan amount policy is shown to disproportionately exclude potential minority applicants from consideration because of their income levels or the value of the houses in the areas in which they live.
US Federal Privacy Laws

1. Cable Communications Policy Act of 1984
2. Children's Internet Protection Act of 2001 (CIPA)
3. Children's Online Privacy Protection Act of 1998 (COPPA)
5. Computer Fraud and Abuse Act of 1986 (CFAA)
6. Consumer Credit Reporting Reform Act of 1996 (CCRRA)
7. Electronic Funds Transfer Act (EFTA)
8. Fair and Accurate Credit Transactions Act (FACTA) of 2003
9. Fair Credit Reporting Act (Full Text).
10. Federal Information Security Management Act (FISMA)
11. Federal Trade Commission Act (FTCA)
12. Driver's Privacy Protection Act of 1994
13. Electronic Communications Privacy Act of 1986 (ECPA)
15. Family Education Rights and Privacy Act of 1974 (FERPA)
17. Privacy Act of 1974
18. Privacy Protection Act of 1980 (PPA)
20. Telecommunications Act of 1996
22. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)
23. USA Freedom Act
24. Video Privacy Protection Act of 1988
Internet arrives: US and Europe diverge

US – privacy on the ground

- FTC and White House ‘bully pulpit’
- FIPS lite: notice, choice, access, security
- FTC enforcement through ‘unfair and deceptive practices’ (FTC Act §5)
- Little legislation
- Kids privacy

EU – privacy on the books

- Omnibus law: DPD then GDPR
- Growth of EU member-state DPAs
- ‘Adequacy principle’: Viral propagation of data protection rules around the globe
- Enforcement gets more serious
Implementing Privacy: policy and tech challenges

**GDPR**

**Lawful basis - Consent, etc.**

legitimate interest, etc.

Right to be informed

Right of access

Right to rectification

Right to erasure

Right to restrict processing

Right to portability

Right to object

Right to avoid automated decisionmaking & explanation

Data Breach Notification

Accountability

**Fines < 4% annual revenue**

**Art. 5 GDPR**

**Principles relating to processing of personal data**

Processing shall be lawful only if and to the extent that at least one of the following applies:

1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
2. 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;
3. processing is necessary for compliance with a legal obligation to which the controller is subject;
4. processing is necessary in order to protect the vital interests of the data subject or of another natural person;
5. 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;
6. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
# Implementing Privacy: policy and tech challenges - unsolved problems

<table>
<thead>
<tr>
<th>GDPR</th>
<th>Consumer Privacy Bill of Rights</th>
<th>Cal. Consumer Privacy Act</th>
<th>Apple proposal</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Lawful basis - Consent, etc.</strong></td>
<td>Right individual control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>legitimate interest, etc</td>
<td>Right to respect for context</td>
<td>Right to opt out of sale</td>
<td></td>
</tr>
<tr>
<td>Right to be informed</td>
<td>Right to transparency</td>
<td>Right to know</td>
<td>Right to know</td>
</tr>
<tr>
<td>Right of access</td>
<td>Right to access</td>
<td></td>
<td>Right to access</td>
</tr>
<tr>
<td>Right to rectification</td>
<td>Right to accuracy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Right to erasure</td>
<td></td>
<td>Right to have data deleted</td>
<td></td>
</tr>
<tr>
<td>Right to restrict processing</td>
<td></td>
<td>No discrimination for exercise</td>
<td>Right to minimization</td>
</tr>
<tr>
<td>Right to portability</td>
<td>Machine-readable formats</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Right to object</td>
<td>Right to correction</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Right to avoid automated decisionmaking &amp; explanation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Breach Notification</td>
<td>Security &amp; Breach Notification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accountability</td>
<td>Accountability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fines &lt; 4% annual revenue</td>
<td>Fines</td>
<td>$7500/incident, 30 day cure</td>
<td></td>
</tr>
<tr>
<td>GDPR</td>
<td>Consumer Privacy Bill of Rights</td>
<td>Cal. Consumer Privacy Act</td>
<td>Apple proposal</td>
</tr>
<tr>
<td>------</td>
<td>---------------------------------</td>
<td>--------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td><strong>Lawful basis</strong> - Consent, etc.</td>
<td>Right individual control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>legitimate interest, etc</td>
<td>Right to respect for context</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Right to be informed</td>
<td>Right to transparency</td>
<td>Right to know</td>
<td></td>
</tr>
<tr>
<td>Right of access</td>
<td>Right to access</td>
<td>Right to know</td>
<td></td>
</tr>
<tr>
<td>Right to rectification</td>
<td>Right to accuracy</td>
<td>Right to know</td>
<td></td>
</tr>
<tr>
<td>Right to erasure</td>
<td>Right to accurate</td>
<td>Right to know</td>
<td></td>
</tr>
<tr>
<td>Right to restrict processing</td>
<td>No discrimination for exercise</td>
<td>Right to minimization</td>
<td></td>
</tr>
<tr>
<td>Right to portability</td>
<td>Machine-readable formats</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Right to object</td>
<td>Right to challenge decisions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Right to avoid automated decisionmaking &amp; explanation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Breach Notification</td>
<td>Security &amp; Breach Notification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accountability</td>
<td>Accountability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fines &lt; 4% annual revenue</td>
<td>Fines</td>
<td>$7500/incident, 30 day cure</td>
<td></td>
</tr>
</tbody>
</table>
Disparate Impact Analysis - Data Challenges

Burden Shifting:

1. Plaintiff’s prima facie demonstration of a policy’s disparate impact
2. Defendant’s job-related business necessity defense
3. Plaintiff’s demonstration of an alternative policy without the same discriminatory impact.
GDPR foray into ‘automated decision making’

Art 4: “automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person:
● it has to be an automated form of processing;
● it has to be carried out on personal data;
● the objective of the profiling must be to evaluate personal aspects about a natural person.

Art 22: “Automated decision-making is the ability to make decisions by technological means without human involvement.
● data provided directly by the individuals concerned (such as responses to a questionnaire);
● data observed about the individuals (such as location data collected via an application);
● derived or inferred data such as a profile of the individual that has already been created (e.g. a credit score).
Automated decision-making & Right of Explanation

GDPR requires:

- Fairness
- Transparency
- Lawful basis for processing: consent, contract, legal obligation, legitimate interest!

Other Protections:

- Minimization
- Purpose limitation
- Retention limitation

Solely automated processing with legal effect

- Right to avoid decision-making solely based on automatic processing
- Must have legal or other similar effects: legal rights, financial capacity, employment, benefits
- Significant decisions must have a human in the loop
- Exceptions
  - Necessary to deal with large volume of data
  - Legal authorization
  - Explicit consent - ‘freely given, informed’
Upstart: CFPB vs GDPR

CFPB on Upstart:

“Underwriting models that use innovative underwriting techniques may enable people with limited credit history, among others, to obtain credit or obtain credit on better terms. Under the terms of our no-action letter, Upstart has agreed to a number of conditions designed to mitigate risk to consumers. We hope this will create an important opportunity to further our own understanding of the use of alternative data and modeling techniques in lending decision-making...”

GDPR guidance:

“Hypothetically, a credit card company might reduce a customer’s card limit, based not on that customer’s own repayment history, but on non-traditional credit criteria, such as an analysis of other customers living in the same area who shop at the same stores. This could mean that someone is deprived of opportunities based on the actions of others. In a different context using these types of characteristics might have the advantage of extending credit to those without a conventional credit history, who would otherwise have been denied.”