SQUIRE
PATTON BOGGS

Automated Processing: Use Cases and Legal Guardrails

ANA Legal Webinar Series
October 11, 2022, 1:00 pm ET

Today's Presenters

Julia Jacobson
Partner, New York
Squire Patton Boggs
julia.jacobson@squirepb.com

David Naylor
Partner, London
Squire Patton Boggs
david.naylor@squirepb.com

Elizabeth Berthiaume
Associate, Dallas
Squire Patton Boggs
elizabeth.berthiaume@squirepb.com

Gicel Tomimbang
Associate, Los Angeles
Squire Patton Boggs
gicel.tomimbang @squirepb.com

Automated Processing Overview: Principles, Laws and Contracting

What do we mean by “automated processing”?

- “**Data Analytics**”: collection, categorization and analysis of data in order to make conclusions, predictions and other decisions – typically by automated means
- “**Artificial Intelligence**”: a catch-all term for a broad range of automated decision-making systems – *from* algorithms that process large amounts of data to achieve a specific outcome infinitely faster than a human could complete the same task *to* artificial general intelligence (AGI), a form of man-made intelligence that is indistinguishable from the human mind.
- **Machine Learning / Algorithmic Decision-Making**
    - “Profiling”: human involved, e.g., reviewing purchase profiles to determine whether to send opportunity for low-interest credit cards
    - “Automated Decision-Making”: no human involved, e.g., automatic refusal of retailer-branded credit card based on zip code

Automated Processing Principles

Underlying Principles

- Ethical Purpose
- Accountability
- Transparency and Explainability
- Fairness & Non-discrimination
- Privacy & Confidentiality
- Safety and Reliability

Key Laws and Guidance

SQUIRE PATTON BOGGS

- EU
  - AI Regulation
  - General Data Protection Regulation (*GDPR*) Article 22 and UK GDPR
- U.S.
  - FTC Notice of Proposed Rulemaking: Commercial Surveillance (Aug 2022)
  - White House's Blueprint for an AI Bill of Rights (Oct 2022)
  - American Data Privacy and Protection Act (*ADPPA*, proposed)
- Canada
  - Quebec Bill 64 – notice rules for decisions that are based *exclusively* on an automated processing and "a technological product or service having privacy settings must ensure that those settings provide the highest level of confidentiality by default"
  - Artificial Intelligence and Data Act (proposed June 2022)
- Brazilian Artificial Intelligence Act (proposed)

Key Laws and Guidance

U.S. State – Consumers

- California Consumer Privacy Act (*CCPA*), as amended by California Privacy Rights Act (*CPRA*)
  - *Profiling* is currently defined as "any form of automated processing of personal information … to evaluate certain personal aspects relating to a natural person …"
  - CPRA Regulations will address "access and opt-out rights with respect to businesses' use of automated decision-making technology, including profiling and requiring businesses' response to access requests to include meaningful information about the logic involved in such decisionmaking [sic] processes, as well as a description of the likely outcome of the process with respect to the consumer."
  - Also applies to employees and B2B personal information
- Colorado Privacy Act and Virginia Consumer Data Privacy Act
  - right to opt out when the profiling produces legal or similarly significant effects concerning the consumer
- Connecticut Act Concerning Personal Data Privacy and Online Monitoring
  - right to opt-out of profiling "in furtherance of **solely** automated decisions" when the profiling produces legal or similarly significant effects concerning the consumer

Key Laws and Guidance

U.S. Laws - Employees Context

- EEOC released guidance (May 2022) regarding employers' use of algorithmic decision-making to help ensure that employment tools do not disadvantage applicants or employees with disabilities in violation of the Americans with Disabilities Act
- New York City Council's Automated Employment Design Tools - municipal law that prohibits use of automated processing tools to screen candidates or employees for employment decisions unless the tool has a "bias audit". Effective January 1, 2023.
- Connecticut law requires employers to give prior written notice to all employees who may be affected by any type of electronic monitoring "in a conspicuous place which is readily available for viewing by its employees .. concerning the types of electronic monitoring which the employer may engage in. Such posting shall constitute such prior written notice."

Key Legal Considerations

- Notice
- Consent
- Right to opt out *vs*. opt in
- Solely automated decisions *vs*. partially automated decisions
  - Whether effect on individual is “significant”
- Privacy Impact Assessment
- Algorithm Assessment
- Data ownership
- Contracting

Risk of Non-Compliance

In the Matter of Everalbum, Inc.

- In 2017 online photo storage and organization app, Everalbum Inc. launched a new photo tagging feature that allowed users to tag faces in their photos to enable grouping photos. Initially, the photo tagging feature was turned on by default with no option to turn it off and was powered by publicly-available facial recognition technology
- Concurrently, Everalbum worked on developing its own facial recognition AI. Everalbum created four datasets to develop, train and test its facial recognition AI from a combination of publicly-available datasets and the photos of app users. After testing on the third data set, Everalbum submitted the facial recognition AI to the National Institute of Science and Technology for accuracy testing and comparison to competing technology.
- FTC alleged that Everalbum misrepresented how it used automated processing on users' photos and that users' photos would be deleted when they terminated their accounts.
- Everalbum required to "forfeit the fruits of its deception" by *deleting data* collected and retained without users' consent and *destroying algorithms* that Everalbum developed using users' photos and videos that were collected through deceptive means

Risk of Non-Compliance

FTC Enforcement Activity: ***Settlement with WW International, fka Weight Watchers, and Kurbo, Inc***

- Settlement over alleged violations of the Children’s Online Privacy Protection Act (COPPA)
- Requires WW to pay a $1.5 million penalty, delete personal information that was improperly collected from children and destroy models and algorithms developed with the use of that personal information.
- FTC prioritizing “meaningful ***disgorgement***” remedy in privacy and security enforcement.

Contracting Considerations

- Privacy
  - controller/business *vs*. processor/service provider *vs*. mixed role
  - applicable privacy policy and supplemental notices
  - information identifiably and sensitivity
- Confidentiality – personal data as confidential information
- Intellectual Property – data ownership and derivative works
- Limitations of Liability, Exclusions, Disclaimers
- Cybersecurity
- Governance – data deletion, supporting privacy rights requests (n.b., varies by applicable law)

Customer *vs.* Tech Provider

Customer (as controller/business) requirements include:

- Restrict vendors’ use of personal data to providing services
- Audit tech provider
- Ensure tech provider is subject to duty of confidentiality
- Algorithmic Impact Assessment – likely to cause potential harm to an individual?

Tech provider (as processor/service provider) obligations include:

- Securely process personal data
- Prompt data breach notifications
- Limit use of personal data to providing services (with limited exceptions)
- Assist with honoring consumer privacy requests
- Algorithmic Impact Assessment

SQUIRE
PATTON BOGGS

Automated Processing Hypothetical

Hypo Background

Happy Athletes (HA) is a sporting goods and active lifestyle retailer headquartered in New York with its flagship store in SoHo and other U.S. locations in Aspen, Austin, Boston, Los Angeles, Miami, San Francisco and Seattle; Toronto, Quebec City and Vancouver, Canada; London, U.K.; and Basel, Switzerland.

HA decides to deploy new technology that is a combination of hardware - heat sensors placed throughout its stores on walls, displays and/or ceilings – together with a SaaS dashboard.

The heat sensors collect information about in-store movement in order to optimize product placement, check out locations, staffing and similar variables to produce reports. The heat sensors can determine approximate size/height of the "marker" (or blob) and whether the heat blob appears to be alone or part of a group. The platform can be set to track individual heath markers throughout the in-store journey or to just general track patterns. The ceiling mounted sensors include a camera option that can be used for security or other purposes.

The algorithm uses various factors to create optimization maps both within individual stores and across locations. The optimization maps are customizable based on a variety of factors, such as time of day, weather, type of products (*e.g.,* grab-and-go, made to order, luxury, etc.), sales targets, characteristics of the location (*e.g.,* part of a mall or standalone location), and information about shoppers, such as whether they enter with someone else, the size of the shopper and companions, etc.

Sensitive Data

CCPA

- government identification number
- financial account, debit/credit card number in combination with any required access code, password or credentials
- precise geolocation
- racial or ethnic origin
- religious or philosophical beliefs, or union membership
- contents of a consumer’s mail, email, and text messages unless the business is the intended recipient of the communication
- “genetic data”
- health information,
- personal information collected and analyzed concerning a consumer’s sex life or sexual orientation
- processing of **biometric information** for the purpose of uniquely identifying a consumer

Biometric Information

Virginia

- “data generated by automatic measurements of an individual’s biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is ***used to identify a specific individual***”
- Excludes “a physical or digital photograph, a video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under HIPAA.”

Adding Sensors in Check-out Area

HA decides to add a new module for sensors in the check-out area that link a specific heat marker to the time spent in line and the purchase details.

- Are data collected by the sensors personal data?
- Are data collected by the sensors sensitive personal data?
- Are data collected by the sensors biometric data?

When personal data are in scope …

1. Privacy Impact Assessment (“PIA”)
2. Questions retailer should ask tech provider during PIA:
   - Algorithmic Impact Assessment?
     - GDPR Article 35 Data Protection Impact Assessment
     - “IMPACT ASSESSMENT … [business that] uses an algorithm that may cause potential harm to an individual, and uses such algorithm solely or in part, to collect, process, or transfer covered data must conduct an impact assessment of such algorithm.” (ADPPA Section 207)
   - What data does technology ingest?
   - What does it do?
3. Operational Issues
   - Clear data retention periods
   - Data minimization, pseudonymization and anonymization
   - Cybersecurity

Heat Markers Become Identifiable

HA decides to add a module that enables the linkage of consumers' access to free in-store WiFi via an email address (required for WiFi access) or loyalty program registration through a mobile app that the user can download while in-store. Free WiFi users and loyalty program registrants agree to HA's privacy policy and terms of use before accessing the WiFi.

- Are data collected by the sensors personal data?
- Are data collected by the sensors sensitive personal data?
- Are data collected by the sensors biometric data?

Offline to Online Part 1

Tech provider develops an integration with an adtech provider. HA wants to combine data from heat sensors with other data collected by HA and made available by the adtech provider to create consumer profiles and then use the adtech to deliver cross-context ads to customers and loyalty program registrants. HA also will use the profiles for email marketing and push notifications in the HA loyalty app.

- What new issues must HA consider before deploying the adtech integration?

Offline to Online Part 2

The now-profiled heat marker person appears to be accompanied by two smaller heat markers. The technology uses that heat marker data to infer that the customer is a parent with two children. Since HA wants to expand its child-related product offerings, HA personnel add a tag to the CRM profile to enable the adtech provider to deliver parent-focused digital advertisements about HA on third-party websites.

HA personnel decide to review the inferred parent and child heat markers before tagging the customer as a parent.

Data Ethics and ESG Considerations

Data Ethics

Type of business ethics:

“a new branch of ethics that studies and evaluates moral problems related to data (including generation, recording, curation, processing, dissemination, sharing and use), algorithms (including artificial intelligence, artificial agents, machine learning and robots) and corresponding practices (including responsible innovation, programming, hacking and professional codes), in order to formulate and support morally good solutions (e.g. right conducts or right values)” *

* Floridi, L. and Taddeo, M. (2016). What is data ethics? Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 374 (2083)

Data Ethics Issues

- Perceived over-collection / overuse / misuse of personal information commonly associated with automated processing
  - Increased importance of clearly, accurately and meaningfully notifying individuals subject to automated processing and the intended use of the results of the automated processing
  - Consider view of ‘typical’ consumer and creepy factor
- Overpromising – like ESG commitments
- Vast data stores made possible by decreased cost and increased power of cloud computing
  - risk of re-identification
  - temptation for function creep
  - attractive to hackers
- Supply chain: vendor selection

SQUIRE
PATTON BOGGS

Key Takeaways

Key Takeaways

1. Know Legal Obligations
   - Identify personal data and other data in scope
   - Understand and address notice and transparency requirements
   - Ensure process to address complaints and inquiries about their personal information is keyed to automated processing issues
2. Manage Operational Risks Specific to Automated Processing
   - Use a top down and bottom up approach
   - Be aware of and monitor for function creep
   - Privacy Impact Assessments, Algorithm Assessments – assess harms and benefits
   - Data governance, *e.g.*, data retention; deletion or anonymization of data no longer needed for the specific notified purposes; avoid using results out of context

Key Takeaways

3. Contractual Considerations
    - Determine whether tech provider has regular quality assurance checks to identify erroneous, biased or unjustified results
    - Identify who owns what, *e.g.*, who “owns” the data and derivative works, who owns technology improvements and insights based on customer data sets
4. Consider Whether and What Data Ethics Commitments to Make
    - Be clear from the start about all actual (not speculative) business purposes for automated processing
    - Ensure automated processing is consistent with promises made to data subjects and other public statements

Questions? Thank you for joining us!

Julia Jacobson
Partner, New York
Squire Patton Boggs
julia.jacobson@squirepb.com

David Naylor
Partner, London
Squire Patton Boggs
david.naylor@squirepb.com

Elizabeth Berthiaume
Associate, Dallas
Squire Patton Boggs
elizabeth.berthiaume@squirepb.com

Gicel Tomimbang
Associate, Los Angeles
Squire Patton Boggs
gicel.tomimbang @squirepb.com