SQUIRE PATTON BOGGS

Practical Privacy: Anonymization

April 25, 2023, 11:00 - 11:30 am ET

Speakers

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

Dr. Annette Demmel
Partner
Squire Patton Boggs, Berlin
annette.demmel@squirepb.com

SQUIRE PATTON BOGGS

Agenda

- Key Terminology
- Legal Requirements for Anonymization
- Anonymization in Practice
- Questions (if any)

Terminology

- Personal Information – direct and indirect identifiers
  - under some laws, publicly available information (but not necessarily the inferences based on the publicly-available information)
- Aggregated Information – may or may not be personal
- Pseudonymized Information – process applied to personal information that replaces identifying information with an alias (*still personal*)

Terminology

SQUIRE PATTON BOGGS

- Deidentified Information – In the U.S. federal Health Insurance Portability and Accountability Act (HIPAA): information that is not individually identifiable by following the de-identification standard and implementation specifications in §164.514(a)-(b) [of the HIPAA Privacy Rule]
- Anonymized Information – data that has been *produced as the output* of a personal information anonymization *process* (*see below*)

Industry Standards

ISO's Definition of Anonymization: process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party

NIST Definition of Deidentification: process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party

SQUIRE PATTON BOGGS

California Consumer Privacy Act

1798.140 (b) "Aggregate consumer information" means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device.

1798.140 (m) "Deidentified" means information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer provided that the business that possesses the information:

(1) Takes *reasonable* measures to ensure that the information cannot be associated with a consumer or household. **(2)** *Publicly commits* to maintain and use the information in deidentified form and not to attempt to reidentify the information, except that the business may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this subdivision. **(3)** *Contractually* obligates any recipients of the information to comply with all provisions of this subdivision.

SQUIRE PATTON BOGGS

Virginia Consumer Data Protection Act

§ 59.1-575

"De-identified data" means data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to such person.

"Pseudonymous data" means personal data that cannot be attributed to a specific natural person without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

§ 59.1-581 (D) No consumer rights apply to "pseudonymous data in cases where the controller is able to demonstrate any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing such information."

SQUIRE PATTON BOGGS

Virginia Consumer Data Protection Act

§ 59.1-581 Processing de-identified data; exemptions

(A) The controller in possession of de-identified data shall:

1. Take reasonable measures to ensure that the data cannot be associated with a natural person; 2. Publicly commit to maintaining and using de-identified data without attempting to re-identify the data; and 3. Contractually obligate any recipients of the de-identified data to comply with all provisions of this chapter.

(D) " … A controller that discloses pseudonymous data or de-identified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or de-identified data is subject and shall take appropriate steps to address any breaches of those contractual commitments."

Defining Data Anonymization under the GDPR

SQUIRE PATTON BOGGS

Recital 26 GDPR:

4 To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.

5 The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

10 Misunderstandings about Anonymization

SQUIRE PATTON BOGGS

According to the European Data Protection Supervisor:

1. "Pseudonymization is the same as anonymization"
2. "Encryption is anonymization"
3. "Anonymization of data is always possible"
4. "Anonymization is forever"
5. "Anonymization always reduces the probability of re-identification of a dataset to zero"
6. "Anonymization is a binary concept that cannot be measured"
7. "Anonymization can be fully automated"
8. "Anonymization makes the data useless"
9. "Following an anonymization process that others used successfully will lead our organization to equivalent results"
10. "There is no risk and no interest in finding out to whom this data refers to"

Anonymization Errors

SQUIRE PATTON BOGGS

- In 2006, a movie-streaming service, published a dataset with 10 million movie rankings made by 500,000 customers claiming that it was anonymous
  - later it was found that it would only take a little bit of knowledge about the subscriber to identify that subscriber's record in the dataset

- In 2013, the New York City Taxi and Limousine Commission published a dataset with more than 173 million individual taxi trips containing the pickup and dropoff location times and supposedly anonymized licence numbers
  - The dataset had not been correctly anonymized, so the original licence numbers could be identified and even the individual drivers of those taxis

Practicing Anonymisation

SQUIRE PATTON BOGGS

- Identify applicable law
- Determine whether to apply one definition to personal data and anonymized data
  - global approach?
  - by applicable law?
- Identify promises made to consumers, employees, customers, vendors, business partners, etc.
  - “aggregated” ≠ anonymous
- Determine the necessary controls in the right place at the right time
  - internal
  - contractual

SQUIRE PATTON BOGGS

Questions?


Thank You!

Global Coverage

SQUIRE PATTON BOGGS

Abu Dhabi
Atlanta
Beijing
Berlin
Birmingham
Böblingen
Bratislava
Brussels
Cincinnati
Cleveland
Columbus
Dallas
Darwin
Denver
Dubai
Frankfurt
Hong Kong
Houston
Leeds
London
Los Angeles
Madrid
Manchester
Miami
Milan
New Jersey
New York
Palo Alto
Paris
Perth
Phoenix
Prague
Riyadh
San Francisco
Santo Domingo
Seoul
Shanghai
Singapore
Sydney
Tampa
Tokyo
Warsaw
Washington DC

Africa
Brazil
Caribbean/Central America
India
Israel
Mexico