From: Andy Williams
To: privacyrfc2018
Subject: RFC Docket No. 180821780-8780-01
Date: Wednesday, September 26, 2018 11:37:44 AM

Request for Comments on Developing the Administration's Approach to Consumer Privacy

User data may include personally identifiable information, behavioral analytics and telemetry, sentiment, financial transactions, personal communication transactions and device logs, sensor data, and identifiers.

If the user requests a company to delete data, regardless of anonymization, they must delete all rows and data in their systems and backups. Not a delete/hidden flag but a hard delete. In some industries, such as healthcare, databases are not designed to hard delete data. Patient data critical and requires auditing. There may be a "delete flag" that is flipped in a row in the database but the record still exists on the backend. If the database is compromised, the attacker can see this soft deleted data because it is still present. Behavioral analytics is not crucial to keep.

Specific requirements for user and administrator authentication.

Data must be secured in transit and at rest.

Firewalls, intrusion detection, and prevention must be implemented.

Perform annual audits by a third party.

Service level agreement to insure timely security updates to software products and hardware involved in collection, transmission, and storage of data.

If an entity acts as an intermediary to another entity to process the transaction they must not be able to view or store the data and each transaction must use a unique identifier. Example: if a user makes a purchase on a credit card machine or online shopping cart, the merchant does not need to see the credit card number nor pass a credit card number. Instead, transmit a unique identifier for that transaction for that particular account so that an attacker cannot collect credit card numbers for later reuse.

Anonymization does not supersede the user's choice to opt-out or remove their data. If the user does not want their data collected, it must be removed even if it was anonymized.

Full disclosure of third parties and affiliates who have access to data and what specific types of data on the user are accessible or transferred to third parties prior to and continually accessible. All entities must be represented and individually consented at time of collection and previews of the data each entity collects must be acessessible by the user.

Each third party must request access and permission must be optionally one-time if it is for a permanent access.

End users must have the ability to see what it is that is collected on them. Not only descriptions and examples, but also the actual data on them.

The user must receive notification during collection and information on the frequency and amount of data prior to collection.

Entities must report what data is collected of the user on an annual basis.

The user must have the ability to export the data in acceptable standard formats for each type of collected data if they so choose. Examples of standard formats include plain text, xml, json, csv, jpg, png, bmp, tiff, or any other open standard.

To request deletion of user data the user must be able to request deletion electronically, it must be an easily discoverable feature.

To opt-out or remove data, the user must not have to provide more information to verify their identity than what they have collected. That is, the user must not have to mail a copy of a driver's license, write a letter, or provide additional identifiers to verify identity than what the entity has.

Opt-out or deletion procedures must be free of charge to the end-user.

If deletion is unfeasible, the data can optionally be scrambled.

https://chiefmartec.com/2018/04/marketing-technology-landscape-supergraphic-2018/

https://datatransparencylab.org/