Protecting Privacy in Online Identity: A Review of the Letter and Spirit of the Fair Credit Reporting Act's Application to Identity Providers

March 9, 2010
Tags: Array
Policy Posts are in-depth analyses on current tech policy issues from CDT experts. Sign up to receive the latest Policy Posts here:

1) CDT Submits Comments in regards to the FTC's Third Consumer Privacy Roundtable

2) Understanding Identity Management

3) The Letter: Identity Providers May Be Consumer Reporting Agencies under the Fair Credit Reporting Act

4) The Spirit: Ensuring Identity Providers Protect Privacy

---

1) CDT Submits Comments in regards to the FTC's Third Consumer Privacy Roundtable

CDT has submitted comments for the FTC's third and final public roundtable discussion exploring privacy. The comments highlight the need to develop some type of private or public legal regime that ensures identity providers properly safeguard consumer privacy in the emerging identity management industry. CDT also separately submitted comments on health information privacy.

In order to fully realize the benefits of user-centric federated identity, identity providers and relying parties must provide control to users and protect their privacy, and there must be some mechanism to enforce such obligations. The Fair Credit Reporting Act (FCRA) is one source of some of the necessary protections and may already apply to entities providing or using identity-related services.

CDT Consumer Privacy Roundtable Comments [1]: Protecting Privacy in Online Identity: A Review of the Letter and Spirit of the Fair Credit Reporting Act's Application to Identity Providers

CDT Consumer Privacy Roundtable Comments [2]: Health Information Privacy: Current Trends, Future Opportunities

---

2) Understanding Identity Management

In the digital context, identity is a claim or set of claims about the user. This identification is often subject to authentication – that is, the process of verifying that the identification claim is, in fact, true. The process of claiming identity, authenticating identity, and authorizing that identity to use certain services is described as identity management.

Traditionally, identity exchange has been a direct interaction between user and service provider, exemplified by systems that rely on user name and password. However, this model is rapidly evolving as Web services and Internet applications now frequently require new forms of identity information. Some of these new models for identity management place the user in the middle of an interaction between an identity provider and an online service. This method, called federated identity, allows service providers to rely on trusted third parties to authenticate users of their service. Often, this eases use for users by reducing the number of sign-in credentials they must remember.

Some of the federated identity technologies developed to address problems with traditional identity

solutions can also be described under the loosely defined term “user centric identity.” This term refers to systems where users, rather than service providers, control their identity credentials. This is similar to the offline world, where we carry a variety of identity documents issued by different authorities, and we choose which identity credential or authenticator to present in each transaction. These new online systems must be designed with privacy and security as foremost concerns due to the often-sensitive nature of the information held by the identity provider.

If carefully designed and implemented, such user-centric, or federated, identity systems can give the user greater privacy protections and greater control over what information is provided in connection with any given transaction. They can also provide the relying party with greater assurance that the information provided is accurate, while lowering costs for services that no longer have to implement their own identity management systems. However, consumer privacy will not be adequately protected if identity providers are allowed to operate without being governed by a sufficient legal regime. Thus, we suggest that the application of the FCRA is one possible approach to protecting privacy in the online identity space.

Center for Democracy & Technology, Issues for Responsible User-Centric Identity [3]
Kim Cameron, The Laws of Identity [4]

---

3) The Letter: Identity Providers May Be Consumer Reporting Agencies under the Fair Credit Reporting Act

While it is still very much an open question, the FCRA may, in certain circumstances, cover identity providers, which would require them to comply with a pre-existing statutory regime and certain Fair Information Practice (FIP) principles that are already incorporated into the law.

FCRA regulates the collection, dissemination and use of consumer information. The law defines a “consumer reporting agency” as any person “which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.” The Act defines a “consumer report” as the communication of “any information” by a consumer reporting agency (CRA) that bears on a consumer’s “credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living” that is “used or expected to be used or collected in whole or in part” for the purpose of serving as a factor in establishing eligibility for credit, insurance, employment, or a range of “other purposes” defined in the statute.

The “other purposes” authorized under the Act include “a legitimate business need for the information in connection with a business transaction that is initiated by the consumer.” In its FCRA commentary, the FTC recognized that “a party has a permissible purpose to obtain a consumer report on a consumer for use in connection with some action the consumer takes from which he or she might expect to receive a benefit that is not more specifically covered” as credit, insurance or employment.

The FTC’s commentary suggests a potentially broad understanding of what could constitute a permissible consumer purpose under the FCRA. For example, “a consumer report may be obtained on a consumer who applies to rent an apartment, offers to pay for goods with a check, applies for a checking account or similar service, seeks to be included in a computer dating service, or who has sought and received over-payments of government benefits that he has refused to return.” Significantly, these examples do not include credit, employment or insurance, but all involve the use of a screening of background or reputation to deliver the service, which suggests that identity providers could be covered under the FCRA as CRAs.

Depending on how identity providers develop and what uses their services are put to, these entities may indeed be doing specialized types of background checks initiated by consumers for online consumer or government services that Congress envisioned regulating when enacting the FCRA.

CDT Consumer Privacy Roundtable Comments [1]: Protecting Privacy in Online Identity: A Review of

the Letter and Spirit of the Fair Credit Reporting Act's Application to Identity Providers

The Fair Credit Reporting Act [5]

FTC FCRA Commentary [6]

---

4) The Spirit: Ensuring Identity Providers Protect Privacy

Whether or not FCRA applies, the statute details certain FIPs-like obligations that identity providers and relying parties – entities using, or relying on, identity information – should incorporate into their practices. The FCRA requirements offer, at least, a good starting point for the FIP principles that should be implemented in this space.

For example, if identity providers are considered CRAs, they would have to comply with the following FIPs-like obligations:

- File Disclosure – CRAs must provide individuals access to information about themselves.
- Access and Correction – CRAs must investigate all disputes of incomplete or inaccurate information unless the dispute is frivolous and must correct or delete inaccurate, incomplete, or unverifiable information within 30 days.
- Timeliness – CRAs may not report outdated negative information. In most cases, a CRA may not report negative information of any kind that is more than seven years old.
- Use Limitations – CRAs may only provide information about individuals to persons with a valid need as defined by the Act.
- Disclosures to Relying Parties – CRAs must notify relying parties about the restrictions under the Act.
- Disclosures to Data Furnishers – CRAs must notify data furnishers about the restrictions under the Act.

If identity services are covered under the FCRA, relying parties would also have a number of important FIPs-related obligations including:

- Use Limitation – Relying parties are responsible for limiting the purposes for which they use data to those stated in the Act.
- Certification of Purpose – Relying parties must certify to the CRA (by a general or specific certification, as appropriate) the permissible purpose(s) for which the report is being obtained and certify that the report will not be used for any other purpose.
- Notification of Adverse Action – Relying parties must notify individuals when an adverse action has been taken based on information contained in a consumer report. Relying parties must also notify individuals when an adverse credit decision has been taken based on information obtained from third parties other than CRAs. The specific type of notification required depends on whether the information used came from a CRA, a non-CRA, or an affiliate.
- Notification of an Address Discrepancy – CRAs must notify relying parties that request reports when the address for a consumer provided by the requesting party in requesting the report is different from the address in the consumer's file. Relying parties must comply with regulations specifying the procedures – issued by the FTC and banking and credit union regulators – to be followed when this occurs.
- Proper Disposal of Records – All users of consumer report information must have in place procedures to properly dispose of records containing this information.

The FCRA also significantly limits the use of medical information in consumer reports and provides a number of statutory obligations for creditors, employers, and investigative consumer report resellers that could possibly apply to specific parties depending on the circumstance.

What is particularly critical here is the spirit of the Act. Whether or not FCRA applies, conforming to such FIPs-like principles will significantly benefit consumer privacy and instill the trust necessary to

help identity providers grow.

CDT Consumer Privacy Roundtable Comments [1]: Protecting Privacy in Online Identity: A Review of the Letter and Spirit of the Fair Credit Reporting Act's Application to Identity Providers

The Fair Credit Reporting Act [5]

-
- Privacy
- FTC
- fcra

Copyright © 2013 by Center for Democracy & Technology.
The content on this website that originates with CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. Details.
Source URL:
https://www.cdt.org/policy/protecting-privacy-online-identity-review-letter-and-spirit-fair-credit-reporting-act%E2%80%99s-appli

Links:
[1] http://www.cdt.org/files/pdfs/CDT%203rd%20Privacy%20Roundtable%20Comments%20-%20Protecting%20Privacy%20in%20Online%20Identity.pdf
[2] http://www.cdt.org/files/pdfs/FTCRoundtableTestimony.pdf
[3] http://www.cdt.org/files/pdfs/Issues_for_Responsible_UCI.pdf
[4] http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf
[5] http://www.ftc.gov/os/statutes/fcra.htm
[6] http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=0757cfbc2fa0f9f4c15e493caab54e1d&rgn=div9&view=text&node=16:1.0.1.6.63.0.45.3.49&idno=16