KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

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

Comments of the Center for Democracy & Technology In regards to the FTC Consumer Privacy Roundtable

Privacy Roundtables – Comment, Project No. P095416

February 26, 2010

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 is one source of some of the necessary protections and may already apply to entities providing or using identity-related services.

I. Introduction

In our November 2009 paper, *Issues for Responsible User-Centric Identity*, CDT made clear that we believe that user-centric federated identity has great promise to make online interactions easier, more secure, and more easily controlled by the user if key questions relating to privacy, security and recourse are addressed properly.[1]

CDT has continued to look for answers to these questions and to develop innovative ways to enforce those solutions. Through this work, we also looked at existing structures that address similar issues, giving individuals control over information about themselves. It was during this review that the breadth of the Fair Credit Reporting Act (FCRA) became apparent.

While it is critical that government not adopt overly intrusive regulations that would discourage this nascent industry from growing, identity providers must be covered under some type of private or public legal regime in order to ensure that they properly safeguard consumer privacy. One approach would be for the industry itself to establish a trust framework based on contract that requires identity providers to offer a three-party contract that imposes restrictions on, and gives enforcement rights to, the identity provider, relying parties and users.[2] A second approach may rely on existing regulatory

---

[1] Center for Democracy & Technology, *Issues for Responsible User-Centric Identity* (Nov. 2009), http://www.cdt.org/files/pdfs/Issues_for_Responsible_UCI.pdf.

[2] See *Comments of the Center for Democracy & Technology In the Matter of A National Broadband Plan for our Future – NBP Public Notice #29*, 22-23 (Jan. 2010), *available at* http://www.cdt.org/files/pdfs/20100125_cdt-fcc_comments.pdf, for an explanation of how this contract approach would work.

frameworks. The focus of these comments is the potential application of the FCRA to identity providers. We have previously suggested that if both these options fail, however, there is a need for a new policy and/or law to govern these entities.[3]

While it is an open question, the FCRA may be read to 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.

II. Background: Understanding Identity Management

In the digital context, identity is a claim or set of claims about the user.[4] 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

---

[3] *See Comments of the Center for Democracy & Technology In the Matter of A National Broadband Plan for our Future – NBP Public Notice #29* (Jan. 2010), *available at* http://www.cdt.org/files/pdfs/20100125_cdt-fcc_comments.pdf.

[4] Kim Cameron, Identity Weblog, *The Laws of Identity* (May 12, 2005), http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf (defining digital identity as "a set of claims made by one digital subject about itself or another digital subject"). *See also* Center for Democracy & Technology, *Privacy Principles for Identity in the Digital Age: Draft for Comment – Version 1.4* (Dec. 2007), http://www.cdt.org/files/pdfs/20071201_IDPrivacyPrinciples.pdf (using a somewhat different definition of identity: "The identity of X is the set of information about individual X, which is associated with that individual in a particular identity system Y. However, Y is not always named explicitly.").

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 consider here the possible application of the FCRA to cover identity providers.

III. The FCRA Definitions[5]

The FCRA regulates consumer reporting agencies and the dissemination of information contained in consumer reports. The definitions of these two terms are critical to understanding the Act's complicated structure. First, 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 . . . for the purpose of furnishing consumer reports to third parties . . . ."[6]

The Act then 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, or employment or a range of "other purposes" defined in the statute.[7]

In creating such circular definitions of CRAs and consumer reports — CRAs issue reports and consumer reports are issued by CRAs — Congress left a lot of room for interpretation of both terms. Therefore, the FCRA cases necessarily scrutinize both definitions in great detail and courts often scrutinize them together.[8]

The "other purposes" authorized under the definition of "consumer report" include disclosure when there is "a legitimate business need for the information in connection with a business transaction that is initiated by a consumer."[9] 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

---

[5] Much of this analysis comes directly from a 1999 staff opinion letter from the FTC on whether reporting of public records alone makes a furnisher a CRA, see http://www.ftc.gov/os/statutes/fcra/sum.shtm. Unfortunately, the Commission has since stopped responding to staff opinion requests on the FCRA.

[6] 15 U.S.C. § 1681a(f).

[7] 15 U.S.C. § 1681a(d).

[8] *See, e.g.*, McCready v. eBay, Inc., 453 F.3d 882 (7th Cir. 2006); Reynolds v. Lemay Buick-Pontiac-Cadillac-GMC, Inc., No. 06-C-292, 2007 U.S. Dist. LEXIS 55641 (E.D. Wis. July 30, 2007).

[9] 15 U.S.C. § 1681b(a)(F)(i).

credit, insurance or employment.[10] Thus, as discussed below, the FTC commentary and the plain language of the statute suggest a potentially broad understanding of what could constitute a permissible consumer purpose in order to make a conveyance of information a consumer report within the statute. However, we first address the reasons to believe identity providers may not be covered under the Act.

IV. Limits of Applicability

Considering the broad definitions in the Act, courts have read the applicability of the FCRA relatively narrowly.

The Seventh Circuit interpreted the "business transaction" language particularly restrictively in *Ippolito v. WNS, Inc.*[11] The *Ippolito* court discussed in detail the apparent conflict between the definition of "consumer report" in § 1681a(d) and the definition of "other purposes" in § 1681b(3)(E), which is now § 1681b(a)(3)(F) after the 1996 amendment:

> The significant problem § 1681b(3)(E) causes is that if its broad 'business transaction' language is incorporated without qualification into the definition of 'consumer report,' most of the other provisions of §§ 1681a(d) and 1681b(3) would be rendered a nullity. If Congress intended information concerning any 'business transaction' involving a consumer to fall within the definition of a consumer report, there would have been no reason to place into the statute § 1681a(d)'s precisely drawn language referring to information 'used or expected to be used or collected . . . for the purpose of serving as a factor in establishing the consumer's eligibility for (1) credit or insurance to be used primarily for personal, family, or household purposes, or (2) employment purposes . . ."[12]

While *Ippolito* was decided prior to the Consumer Credit Reform Act of 1996, it is still often cited by federal courts. On the other hand, the current language in Section 1681b(a)(3)(F) (formerly Section 1681b(3)(E)) seems to at least partly reduce the conflict by limiting covered business transactions to ones "initiated by the consumer." Prior to the 1996 amendment, the Seventh Circuit wrote:

---

[10] 16 C.F.R. Pt. 600, App. (Comment to Section 604(3)(E)) (1993). When the FCRA was amended in 1996 this section moved to Section 604(3)(F)(i), but the general applicability of the FTC's commentary has not changed and it continues to be relied upon by the courts. *See, e.g.*, Wallace v. Finkel, No. 2:06CV05-SRW (WO), 2006 U.S. Dist. LEXIS 42271 (M.D. Ala. June 22, 2006). The FTC is the agency empowered to administer and enforce the FCRA. Thus, "[w]hile the commentaries and opinions of the FTC are not law, . . . [t]he Supreme Court has long recognized that an agency's interpretation of a statute it is entrusted to administer should be given 'considerable weight' and should not be disturbed unless it appears from the statute or legislative history that Congress intended otherwise." *Id.* (citing Chevron, U.S.A., Inc. v. Natural Resources Defense Council, 467 U.S. 837, 843 (1984)). As a result, the FTC commentary remains particularly relevant here.

[11] 864 F.2d 440 (7th Cir. 1988).

[12] *Id.* at 451.

> [T]he definition of 'consumer report' has essentially been limited to information that is 'used or expected to be used or collected' in connection with a 'business transaction' involving one of the 'consumer purposes' set out in the statute, that is, eligibility for personal credit or insurance, employment purposes, and licensing.[13]

A significant reason for having suggested such a limitation was to keep the definition of "consumer report" and the statute "within the bounds Congress intended."[14] That is, Congress enacted the FCRA to "regulate the dissemination of information used for consumer purposes, not business purposes."[15]

The FTC's commentary, however, suggests a broader understanding of what could potentially constitute a 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."[16] 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.

It is also important to note that not all reports containing information on a consumer are "consumer reports" under the Act. The district court in *Forrest v. Secured Funding Corporation* wrote:

> The key phrase is "used or expected to be used or collected," which encompasses: (1) how the person who requests the report actually uses it, (2) how the consumer reporting agency that prepares the report "expects" it to be used, and (3) the purpose for which the consumer reporting agency originally "collected" the information contained in the report.[17]

In addition, when a consumer has provided all of the information directly to an entity that otherwise may be covered under the FCRA, the entity probably would not be considered a CRA.[18] This is an important exception and significantly affects when an identity provider would be acting as a CRA under the statute. For example, if an identity

---

[13] *Id.*

[14] *Id.* at 452.

[15] *Id.* However, clearly distinguishing between a "business purpose" and a "consumer purpose" can be challenging.

[16] *See supra* note 10.

[17] No. 05-C-1324, 2007 U.S. Dist. LEXIS 1757 (E.D. Wis. Jan. 8, 2007).

[18] 15 U.S.C. § 1681a(d)(2) ("the term 'consumer report' does not include . . . any report containing information solely as to transactions or experiences between the consumer and the person making the report").

provider provides a relying party with a "consumer report" that contains information "solely as to transactions or experiences between the consumer and the [identity provider]," then this communication of information is not considered a "consumer report" under the Act.

A. Coverage of Data Brokers under the FCRA

Whether data brokers function, at times, as CRAs under the FCRA has been the source of ongoing debate. While data brokers claim that the services they offer that serve some of the same purposes as identity services are not subject to the FCRA, it is still an open question.[19] That is, "whether an entity is acting as a consumer reporting agency in a particular situation is a fact-specific inquiry. While credit bureaus such as Equifax may be paradigmatic CRAs, the term can extend beyond such entities."[20] Nevertheless, these companies have often developed innovative ways to avoid falling under the FCRA definitions when utilizing databases for identity verification purposes, which has raised concerns from many privacy advocates.[21] The lack of clarity in the data broker situation leaves open questions about the existing regulatory structure for identity providers.

B. McCready v. eBay, Inc.

The case that offers the most relevant analysis to whether identity providers might be covered by the FCRA is *McCready v. eBay, Inc.*[22] The most pertinent facts are as follows:

> McCready operated an online business in which he bought and sold various items through several accounts he had registered with eBay . . . McCready's dealings left several eBay users dissatisfied, and they used eBay's Feedback Forum to voice their displeasure. The buyers complained that McCready failed to deliver the goods he sold or delivered goods of lower quality than he had advertised. eBay notified McCready of

[19] *See, e.g.*, Electronic Privacy Information Center, *Request for investigation into data broker products for compliance with the Fair Credit Reporting Act* (Dec. 16, 2004), *available at* http://epic.org/privacy/choicepoint/fcraltr12.16.04.html ("if a data product originates from a consumer report database, the product remains protected by the FCRA"); Marricone v. Experian Information Solutions, Inc., No. 09-CV-1123, 2009 U.S. Dist. LEXIS 93003 (E.D. Pa. Oct. 6, 2009) (denying a motion to dismiss plaintiff's FCRA claims against LexisNexis Risk and Information Analytics Groups, Inc. acting as a consumer reporting agency).

[20] *Id. But see* Knechtel v. ChoicePoint, Inc., No. 08-5018, 2009 U.S. Dist. LEXIS 109521 (Nov. 23, 2009) (granting defendant's motion to dismiss FCRA claims because plaintiff failed to sufficiently plead that defendants are a consumer reporting agency). "As far as the Court can ascertain from the facts alleged, Defendants are merely a conduit of information, as opposed to an entity that in any way re-organizes or filters information . . . Defendants are a mere purveyor of unadulterated information, which is insufficient to state a claim under the FCRA." *Id.*

[21] *See Exploring the Offline and Online Collection and Use of Consumer Information: Hearings Before the Subcomms. on Commerce, Trade and Consumer Protection and Communications, Technology and the Internet of the House Comm. on Energy and Commerce*, 111th Cong. (Nov. 19, 2009) (statement of Pam Dixon, Executive Director, World Privacy Forum), *available at* http://www.worldprivacyforum.org/pdf/TestimonyofPamDixonfs.pdf.

[22] 453 F.3d 882 (7th Cir. 2006).

> the complaints and informed him that his accounts would be suspended if he did not resolve them. After investigating the claims, eBay suspended McCready's accounts for June or July 2002, and advised him that he would be reinstated if he reimbursed the claimants. Rather than make good on his sales, McCready embarked on retaliatory litigation.[23]

McCready alleged that eBay's "feedback profile" contained false and misleading comments made by other users of eBay and claimed that eBay's Feedback Forum is a "consumer report" under the FCRA. The Seventh Circuit rejected the FCRA claim; however, its analysis offers insight into what background and reputation-based services may be covered under the statute. In determining that eBay's Feedback Forum was not a "consumer report," the Seventh Circuit offered the following analysis:

> [G]iven the broad statutory purpose of preserving individuals' privacy, a "consumer" under § 1681a(d)(1) must, at minimum, be an identifiable person. Moreover, the FCRA applies only to "consumer reports" which are used for consumer purposes; "[i]t does not apply to reports utilized for business, commercial or professional purposes."
> . . .
> eBay's Feedback Forum sorts information according to eBay users' self-anointed 'usernames,' which leaves intact their anonymity outside the eBay universe to the extent they desire to retain it. And it is clear that the Feedback Forum is used to inform eBay users' decision to buy from, or sell to, a particular user, an inherently commercial activity. Because the Feedback Forum cannot be considered a "consumer report," by extension eBay cannot be considered a "consumer reporting agency" within the FCRA. Nor does eBay exert any control over what is said in the Forum, which contains mere opinions of people not in eBay's employ.[24]

McCready, therefore, offers three instructive tests to determine whether coverage under the FCRA is applicable: 1) Is the consumer identifiable? 2) Is the consumer report used for a consumer purpose or business purpose? and 3) Is information within the consumer report factual in nature or mere opinion? Each of these questions should be analyzed to determine whether FCRA coverage could extend to identity providers.

V. Applicability to Identity Providers

Each of the three tests from *McCready* demonstrates why identity providers may or may not be covered as CRAs.

First, while it may seem entirely logical that all identity providers have identifiable information on individuals, it probably actually depends on the uniqueness of the identifier. For example, a five-digit zip code can be used as an identity attribute, but it is

[23] *Id.* at 885-86.

[24] *Id.* at 889.

not sufficient information by itself to identify an individual for FCRA purposes.[25] The identity authentication assurance level, or degree of confidence in the identifier, is also likely important in determining whether an individual is identifiable for FCRA purposes. While self-assertion systems may still be identity systems, especially where the system makes sure that claimed identities are unique, such as in the eBay reputation system, these systems might provide low levels of assurance. It is exactly for this reason that the Office of Management and Budget (OMB) developed guidance on levels of assurance for e-authentication of government services. Individuals self-asserting certain attributes or using a pseudonymous identity within a system would fall under the lowest level of assurance.[26] A truly pseudonymous user name used to comment on a blog post or to operate within the eBay reputation system is obviously less of a concern than an individual's health records held by his or her insurance company. Thus, the assurance level in the identity space would seem to play a role in determining whether identity providers would be "identifying" individuals in a cognizable way.

Under the consumer purpose test, *McCready* clearly demonstrates that reputation and identity services that relate to a person acting as a business are not likely to be seen as serving consumer purposes. However, the question is still open as to whether a court would rely on the *Ippolito* preference for only considering consumer purposes to be eligibility for personal credit or insurance, employment, and licensing or the broader interpretation used by the FTC in its commentary, which includes all consumer uses in background services when all other CRA tests have been met.

Lastly, the type of information used by identity providers in most cases would seem to be more than "mere opinions of people," but *McCready* does seem to make clear that entities providing authentication services based primarily on reputation would not be considered CRAs.

VI. Responsibilities of Identity Providers As CRAs

If identity providers are considered CRAs, they would have to take certain steps to comply with the FCRA, including complying with several 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

[25] However, the combination of various identity attributes, such as five-digit zip code, gender and date of birth, can be used to uniquely identify an individual with at least an 87% certainty. *See* Latanya Sweeney, *k-Anonymity: A Model for Protecting Privacy*, 10 INT'L J. OF UNCERTAINTY, FUZZINESS & KNOWLEDGE-BASED SYS. 557 (2002), *available at* epic.org/privacy/reidentification/Sweeney_Article.pdf (noting that 87% of the U.S. population likely can be uniquely identified based only on three characteristics: five-digit zip code, gender and date of birth).

[26] *See* Office of Mgmt. & Budget, M-04-04, *Memorandum to the Heads of All Departments and Agencies: E-Authentication Guidance for Federal Agencies* (Dec. 16, 2003), http://www.whitehouse.gov/OMB/memoranda/fy04/m04-04.pdf (describing the four levels of assurance necessary for particular government transactions).

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.[27]

VII. Responsibilities of Relying Parties of CRA Data

If identity services are covered under the FCRA, "relying parties" – entities using, or relying on, identify information – 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.[28]

- 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.[29]

- Notification of Adverse Action[30] — Relying parties must notify individuals when an adverse action has been taken based on information contained in a consumer report.[31] Relying parties must also notify individuals when an adverse credit decision has been taken based on information obtained from third parties other than CRAs.[32] The specific type of notification required depends on whether the information used came from a CRA, a non-CRA, or an affiliate.[33]

---

[27] For more detail about the responsibilities of CRAs under the FCRA, see generally 15 U.S.C. §§ 1681e, 1681g.

[28] *See* 15 U.S.C. § 1681b.

[29] *See* 15 U.S.C. §§ 1681e(a), 1681b(b)(1).

[30] "The term "adverse action" is defined very broadly by Section 603 of the FCRA. "Adverse actions" include all business, credit, and employment actions affecting consumers that can be considered to have a negative impact – such as unfavorably changing credit or contract terms or conditions, denying or canceling credit or insurance, offering credit on less favorable terms than requested, or denying employment or promotion.

[31] 15 U.S.C. § 1681m(a).

[32] *See* 15 U.S.C. § 1681m(b).

- 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.[34]

- Proper Disposal of Records — Section 628 of the FCRA requires that all users of consumer report information have in place procedures to properly dispose of records containing this information. The FTC, SEC, and banking and credit union regulators have issued regulations covering disposal.[35]

There is also a range of other obligations for creditors, employers, investigations resellers and medical records that could possibly apply to specific parties depending on the circumstance.

Liability under the FCRA includes state or federal civil enforcement actions, as well as private lawsuits.[36] In addition, any person who knowingly and willfully obtains a consumer report under false pretenses may face criminal prosecution.[37]

VIII. Government Agencies

Given the current push to develop identity solutions for the federal government, another open question that is important is whether there is federal sovereign immunity under the FCRA.

FCRA clearly defines the term "person" in Section 1681a(b) as "any individual, partnership, corporation, trust, estate, cooperative, association, *government or governmental subdivision* or agency, or other entity."[38] However, it still remains unclear whether this is considered by the courts to be a sufficiently unequivocal express waiver of immunity.

First, it appears settled that there is State sovereign immunity under the Act. For example, in *Densborn v. Trans Union, LLC, and Illinois Student Assistance Commission*, a district court in Illinois held that "because Congress enacted the FCRA pursuant to its authority under the *Commerce Clause*, it lacks the authority to abrogate a State's sovereign immunity through the statute."[39] Congress may

[33] *See* 15 U.S.C. §§ 1681m(a), 1681m(b)(1), 1681m(b)(2).

[34] *See* 15 U.S.C. § 1681c(h).

[35] *See* 15 U.S.C. § 1681w.

[36] 15 U.S.C. §§ 1681n, 1681o, 1681s.

[37] 15 U.S.C. § 1681q.

[38] 15 U.S.C. § 1681a(b) (emphasis added).

[39] No. 08 C 3631, 2009 U.S. Dist. LEXIS 10250, at *2 (N.D. Ill. Feb. 10, 2009).

abrogate the States' sovereign immunity only pursuant to a valid grant of constitutional power. However, under the Supreme Court's precedent in *Hibbs* and *Seminole Tribe*, a valid grant of constitutional power is limited to Congress' power under Section 5 of the Fourteenth Amendment.[40] In other words, Congress may not abrogate a State's Eleventh Amendment immunity from private suits by citizens of the State in federal courts pursuant to Article I's Commerce Clause.

There are two other exceptions to Eleventh Amendment sovereign immunity. First, a State may voluntarily consent to suit in federal court. And second, under the Ex parte Young doctrine, a plaintiff may file suit against state officials seeking prospective equitable relief, typically an injunction, for ongoing violations of federal law.[41]

The situation is different with respect to federal agencies. Congress may waive federal sovereign immunity by statute. The waiver, however, must be unequivocally expressed in statutory text and will not be implied.[42] Whether Congress has done so in the FCRA is an open question. For example, in *Talley v. United States Department of Agriculture*, a district court in Illinois held "that the term 'government or governmental subdivision or agency' in the FCRA is an express waiver of the United States' sovereign immunity." Significantly, "[t]his waiver is not overridden by a subsequent express preservation of [the United States'] sovereign immunity" as was the case with Truth in Lending Act claims, a statute under the Consumer Credit Protection Act.[43] Of particular significance to this district court was the fact that the FCRA is also a part of the Federal Consumer Protection Act and it does not contain the additional preservation of sovereign immunity that is found in the TILA.

However, the same district court (through a different federal judge) reached a different conclusion in *Bormes v. United States*.[44] There, the court emphasized "other federal statues have unequivocally waived the United States' sovereign immunity by expressly inserting the specific term 'United States' into the statutory language."[45] Such was the case in the Federal Torts Claims Act and is not the case with respect to the FCRA. And "a separate section of the FCRA [Section 1681u(i)] expressly provides that the United States may be liable for certain violations." The court concluded that because "the section of the FCRA under which Bormes seeks relief, 15 U.S.C. § 1681n, has not so unequivocally waived

---

[40] *See* Nev. Dep't of Human Res. v. Hibbs, 538 U.S. 721, 726 (2003); Seminole Tribe of Fla. v. Fla., 517 U.S. 44, 59-66 (1996) (holding Congress may not abrogate a State's Eleventh Amendment immunity from private suits by the citizens of the State in federal courts pursuant to Article I's Commerce Clause).

[41] 2009 U.S. Dist. LEXIS 10250, at *2.

[42] Lane v. Pena, 518 U.S. 187, 192 (1996).

[43] No. 07 C 0705, 2007 U.S. Dist. LEXIS 50388, at *2 (N.D. Ill. July 12, 2007).

[44] 638 F. Supp. 2d 958 (N.D. Ill. 2009).

[45] *Id.* at 961.

the sovereign immunity of the United States, Bormes fails to present a claim under which relief can be granted."[46] The Seventh Circuit is currently reviewing this issue.

IX. Conclusion

The popular perception is that the FCRA only applies to eligibility for credit, employment and insurance, but a plain reading of the statute suggests that it also applies to consumer eligibility for other purposes. 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 for online consumer or government services that Congress envisioned regulating when enacting the FCRA. However, we recognize that even if it is found that these types of background checks are generally covered, there are other factors, including whether the service provides the kind of unique identification that Congress intended, that will ultimately determine if an identity provider is specifically covered as a CRA under the Act.

This uncertainty for identity providers leaves many open questions. And it does not seem to be in the interest of a nascent industry that will have to interact directly with the public to push the limits of the law.

User-centric identity providers have another option: they can develop practices through their trust frameworks that comply with the FCRA, in spirit and in letter. Providers that offer services with consumers as the primary audience, or at least on equal footing to relying parties, will have little problem conforming to the FIPs laid out in the statute, which emphasize consumer notice, consent, access, correction, timeliness and secondary use limitations. On the other hand, providers that place the consumers behind the interests of the relying parties will have more difficulty complying with the statute.

There is no need to risk the threat of greater regulation when it is in identity providers' interest to utilize trust mechanisms that offer users the necessary control from the beginning, especially when those mechanisms can be judged to be in compliance with current law.

[46] *Id.*