CORPORATE COUNSEL
An ALM Website
corpcounsel.com | March 23, 2015

FCRA and the Use of Facial Recognition Technology

From the Experts

Paul Bond and Albert Hartmann

Photo by Mirko Tobias Schäfer, via Flickr

Most shopkeepers would be delighted if they could tell, just by looking at them, which shoppers had previously been detained on suspicion of shoplifting. Retailers also could prevent significant fraud losses if prior check-bouncers and identity thieves had their mugshots pinned to their jacket as they walked to the checkout line. While we don't walk around with this information visible to the world, our faces are almost always visible for all to see. Increasingly, that's just as useful.

Federal and state agencies have long maintained massive databases of face-linked profiles. Private companies—from social media sites to data brokers to industry consortiums—now provide consumer-facing businesses with similar information as well as the technology not only to identify and authenticate customers, but also to personalize how businesses interact with them. When cameras match faces with profiles, businesses know their customers better.

But in adopting this new technology, businesses must consider the potential application of longstanding consumer protections. For example, the federal Fair Credit Reporting Act (FCRA) has, for decades, regulated the use of consumer reports by businesses. Many businesses equate "consumer reports" with only bottom-line creditworthiness scores from traditional consumer reporting agencies (CRAs). However, the reach of the FCRA is far greater, and it encompasses information wholly unrelated to credit.

The FCRA provides consumers certain rights to notice of the use of consumer reports. These include the consumer's right to obtain full file disclosures and to challenge allegedly inaccurate information. Of course, the FCRA provides these rights by imposing correlative duties on those who use consumer reports, those who furnish the underlying information and, most of all, on CRAs.

The law allows consumers to recover actual damages as well as attorney's fees. In the case of willful violations, which can be premised on merely reckless conduct, consumers also can recover statutory penalties between $100 and $1,000 per violation. Courts routinely allow consumers to obtain these statutory damages for technical FCRA violations—usually sought on a class basis—even without proof of harm.

Depending on how a business adopts facial recognition technology, it may be using consumer reports, furnishing information to a CRA or may even become a CRA itself. However, FCRA liability is by no means an inevitable result, and care can be taken to reduce the risk of being unexpectedly thrust into the FCRA context.

Use Case No. 1: First-Party Use of Data

Store A has an archive of photos of people who have stolen there before or

bounced checks. Store A does not share this information with any other company, but just uses it, with facial recognition technology, to flag such people in its own store. Loss-prevention specialists follow bad actors around closely. Cashiers refuse to take their checks.

No one in this use case is making any "communication" as required by the definition of consumer report. 15 U.S.C.A. § 1681a(d)(1) A company cannot "communicate" consumer reports with itself. Therefore, the FCRA should not apply, regardless of how the store uses the information. Of course, other consumer protections may still apply.

Use Case No. 2: Direct Transmission of Experience Data

The FCRA provides that a consumer report does not include "any . . . report containing information solely as to transactions or experiences between the consumer and the person making the report," nor to such information shared between entities subject to common corporate ownership or control. 15 U.S.C. § 1681a(d)(2)(A)(i)-(ii)

Suppose Banks A1, A2 and A3 are separate legal entities, but all are owned by Bank Holding Company A. Each bank has a facial database of individuals who that bank has ejected for suspicious or disruptive behavior at any branch. The banks use this information, with facial recognition technology, to alert branch security as soon as the individual walks in the door. The banks can share this information with each other for use in their facial recognition programs without invoking the FCRA.

However, this conclusion rests heavily on all of the information shared being experience data. If someone at Bank A1, for example, decides to "enrich" the shared database with information from law enforcement, banks not controlled by Bank Holding Company A or any other source, then this nonexperience data would likely trigger application of the FCRA.

Use Case No. 3: Multilateral Direct Transmission of Experience Data

Each of bicycle-rental chains A, B and C has an archive of photos of people who never returned bikes, and probably provided false information at the time of the rental. Each chain shares this information directly with the other chains. If someone coming to rent a bike matches a person in the database, the chain refuses to rent or requires a bigger deposit. (The latter constitutes risk-based pricing, itself a possible adverse action under the FCRA.)

Because each bike rental chain only shared its own experience data with the other chains, there was no consumer report and the FCRA should not apply. However, this use case assumes that each chain maintains a separate database of the pooled data that is not shared with any other entity.

Use Case No. 4: Multilateral Transmission of Experience Data Through a Central Organization

Each of Stores A, B and C has an archive of photos of people who have intentionally damaged mobile phones covered by an insurance replacement plan to obtain a new device. Each store shares this information with a central organization (DataCo). Each store pulls information from DataCo, with facial recognition technology, to identify these people and require them to pay more for replacement insurance, or bar them from buying the insurance at all.

In this instance, we may have a consumer report, and DataCo may be a CRA. Store B isn't getting the information from Store A anymore—all information is coming from DataCo, which did not have any transaction or experience with any of the consumers.

The information bears on the consumer's "credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living"—the hallmark of a consumer report—and may result in the individual's paying more for insurance than a consumer not in DataCo's database, or being denied insurance altogether. If the FCRA applies, the store would be required to provide an adverse action notice, and the consumer would have to be able to see and challenge his DataCo file—or the store and DataCo could face an FCRA lawsuit.

The Bottom Line

Facial recognition technology will benefit a wide range of businesses. When a particular use of this technology may result in adverse actions—like denial of service, risk-based pricing increases or even a call to law enforcement—an FCRA analysis should be done. Is any information being shared? Is there an exception that keeps that information from being a consumer report when shared directly with another entity? Where does the underlying information come from? How, and with whom, is the information shared? Where is it stored? Answering these questions today will keep facial recognition deployment from being an FCRA pie in the face tomorrow.

Paul Bond is a partner in the intellectual property, information and innovation practice at Reed Smith. He focuses on data security, privacy and management. He is a member of the International Association of Privacy Professionals and sits on the board of directors of the Identity Theft Resource Center. He can be reached at pbond@reedsmith.com. Albert Hartmann is a counsel in the same practice group and concentrates on the defense of class action privacy claims in state and federal courts. He has successfully defended clients against claims for violations of the federal Fair Credit Reporting Act for more than a decade. He can be reached at ahartmann@reedsmith.com.