The Risk of Centralized Storage for Biometric Data

Toronto – August 25, 2015

In June 2015, the United States Office of Personnel Management (OPM) suffered a data breach stealing the records of 21.5 million people. The stolen data included detailed background security-clearance-related information. More alarmingly, it also included 1.1 million fingerprints resulting in the compromise of secret agents, as they could be identified by their fingerprints even if their names had been changed. Astoundingly, the OPM was using simple passwords to protect fingerprint information which was also not encrypted.

In response to the breach, the Department of Homeland Security announced that federal personnel will soon be required to use a three-factor authentication method that includes a smartcard, a password and their fingerprints for logging on to computers. The smartcard will contain a digitized fingerprint, moving away from central storage of biometric data.

Three-factor authentication includes:

- Something you know (like a password)

- Something you own (like a smartcard)

- Something you are (like finger print or face biometrics)

These three factors are generally under the control of the individual and no one else. The strongest authentication method is biometric, because it cannot be stolen. The smartcard is next; while the card can be stolen it can be cancelled quickly, similar to measures taken with a lost or stolen credit card. Passwords are the weakest because they can be stolen, and unlike smartcards, password theft typically goes unnoticed until use is detected. The OPM data breach is such an example.

We all know how laborious and painful password management is. To be secure, passwords need to be complicated, lengthy and different for every application – making them impossible to retain by memory. As a result, simple to remember passwords are often used. The following is SplashData's list of the top ten passwords used by consumers:

123456	password
12345	12345678
qwerty	123456789
1234	baseball
dragon	football

Password vault apps like LastPass help consumers retain their ongoing list of difficult-to-remember passwords by aggregating all of them under one single password. Such password managers can be a smart way to increase online security – that is, until they get hacked. In June 2015, LastPass was hacked resulting in the theft of email addresses, password reminders, server per user salts (data added to passwords to make them harder to crack) and authentication hashes for 7 million users. It is not surprising that password vault companies get targeted by hackers; they keep centralized servers full of passwords. What hacker would pass up that opportunity?

Like the OPM, LastPass learned (the hard way) that centralization of data should not be conducted because it creates an enticing target for hackers. Decentralization eliminates the target and makes hacking much more difficult. Logical? Frankly, yes.

Many privacy authorities worldwide have already passed or are in the midst of passing legislation to prevent the collection and centralization of private biometric data. Why? To protect consumers.

In 2011, the Office of the Privacy Commissioner of Canada, echoed by the Ontario Privacy Commissioner, issued guidance on the use of biometrics such as facial recognition in both the public and private sectors. The document, entitled "At Your Fingertips – Biometrics and the Challenges to Privacy", proposes several principles aimed at mitigating privacy challenges associated with biometric systems including:

"Store biometric information locally rather than in centrally located databases to minimize the risk of data loss or inappropriate cross-linking of data across systems."

On October 15, 2012, Facebook disabled the "tagging facial recognition" feature for users in the European Union following an investigation by the Irish Data Protection Authority (DPA). The Hamburg DPA also declared that Facebook was in violation of the EU's data protection laws with regard to the use of facial recognition, and took measures to force Facebook to amend its practices as well as destroy its data base of facial images collected in Germany to date.

As a result, when Google launched "Google Photos" in June 2015, it disabled face recognition for Canada and European Union countries. In July 2015, Facebook launched "Facebook Moments" and face recognition was disabled for Canada and European Union countries because their laws make it illegal to centrally collect and use biometric data.

U.S. laws around biometric identification are sparse but growing at the state level. Illinois has introduced Biometric Information Privacy Act ("BIPA"). Texas has statutory provisions (Bus. & Com. Code Ann. § 503.001). BIPA damages for each violation are the greater of liquidated damages ($1,000 for a negligent violation or $5,000 for an intentional or reckless violation) or actual damages, and injunctive relief and attorneys' fees and costs are also available. Texas law subjects violators to a civil penalty (which may be enforced by the Texas Attorney General) of up to $25,000 for each violation.

Alaska and Washington have similar legislation pending. Under the proposed Alaska statute, collection of biometric identifiers without express, documentable consent would give rise to a private right of action for any intentional violations of the statute. H. B. No. 144, 28th Legislature, 1st Sess. (Alaska 2013). The Washington bill, which has passed in the House and is moving through the Senate, seeks to prevent the capture and/or sale of a biometric identifiers for commercial use, unless the subject is first informed and consents.

Iowa, Nebraska, North Carolina and Wisconsin include various types of biometric data in their definition of "personal information" for purposes of data security breach notification laws, which require notice to data owners in the event of a data breach involving biometric information.

At present, the result is a class action lawsuit. Between May and July 2015, plaintiffs sued Facebook and Shutterfly for purportedly capturing biometric data in violation of Illinois' Biometric Information Privacy Act, 740 ILCS 14 (West), and are the first to test the Illinois BIPA law.

Thankfully these laws are being legislated to protect the consumer. If not for these and future legislation, the consumer is a sitting duck.

We have a big problem - security. One very large aspect of which relates to password authentication. Biometrics is proving to be a very effective solution to this problem. As demonstrated in hacking vulnerability and privacy legislation, the collection of biometric data is fraught with major issues, some of which being illegal. As demonstrated by the Department of Homeland Security's plan to use smartcards to store digitized fingerprints (while expensive in terms of capital and ongoing operating costs), the result is the end of centralized storage of biometric data.

The bottom line is this; anyone looking to use biometrics to improve security and privacy should veer away from centralized collection and storage of biometric data. There are many client-side solutions that provide much safer alternatives.

Prepared by Don Waugh (Co-CEO, Applied Recognition)

Applied Recognition is the creator of Ver-ID, a client-based face authentication software that operates on all Windows, Mac, Android, iOS, Blackberry desktop and mobile devices. Embedded and integrated on a user's device, Ver-ID provides basic two-factor authentication, including "Something You Own" and "Something You Are" biometrics. Ver-ID security can be augmented with "Something You Know", should it be warranted. Most importantly, Ver-ID is designed to integrate with existing password-based systems, augmenting protection and delivering face authentication security to any SaaS, Cloud, Web or independent application.