Stakeholder Issue Nos. 11(b) and 11A

Should the code define Secure Storage of Information? Should context matter and, if so, how?

"Parties to this Code of Conduct should use commercially reasonable measures to secure facial template information."[1]

How should the code address transmission of Facial Recognition Data?

Should the code address security of Facial Recognition Data in transmission and,if so, how? Do recognized technical standards exist that pertain to transmission?

[Option A] "When storing information contained in a face recognition system parties to this Code of Conduct using facial recognition must use commercially reasonable measures to protect against such risks as loss or unauthorized access, destruction, use, modification or disclosure of this data"[2]

[Option B] "Parties to this Code of Conduct using facial recognition use encryption in-transit for any transmission of facial recognition data. If it is happening over a network, it should use Transport Layer Security with a sufficient cryptographic cypher suite and key size to protect that information for many years. If the data is not being transmitted over a network, such as via a USB or hard drive, it should be encrypted at rest using good using a FIPS 140-2 level 1 or higher validated cryptographic module. Facial recognition information with an expected lifetime beyond 2030 shall be protected using cryptographic techniques with a minimum of 128 bits of security", to protect against such risks as unauthorized access or disclosure of this data[3]

[1] Based, in part, Article 4A-202 of the Uniform Commercial Code (the "UCC") requirements for bank transfers: "If a bank and its customer have agreed that the authenticity of payment orders . . . will be verified pursuant to a security procedure, a payment order . . . is effective as the order of the customer . . .if: (a) The *security procedure is a commercially reasonable method* of providing security against unauthorized payment orders;"

[2] This is based on ACLU principles prepared for group

[3] Submitted by Michelle DeMoy of CDT

Stakeholder Issue No. 12

Risk: Security: commercial facial recognition data could be subject to data breaches that result in sensitive biometrics being revealed to unauthorized entities; insufficient security procedures could result in biometric identity theft.

Which entities would be best situated to provide for security?

This document should apply to all uses of facial recognition and facial detection technology regardless of medium.

What data should be subject to security obligations in the code?

[Option A] "Parties to this Code of Conduct should use appropriate security for the context of party's relationship with consumers."[4]

[Option B] "The security obligations for parties to this Code of Conduct should use the security standards described above for all biometric data, regardless of context."[5]

Most states currently have breach notification laws. Should the code impose additional data breach notification obligations (not otherwise subject to state law)?

[Option A] No additional language needed as 47 state data breach laws already cover unauthorized acquisition of PII. And regardless of whether an entity adopts the guidelines or not, these state laws apply. Finally, when the federal government passes a national data breach standard, this section can create confusing or conflicting obligations for parties to the guidelines.

[Option B] State data breach laws should be implemented when biometrics are included in the definition of PII. When biometrics are not addressed, companies should append their obligations to include "an individual's unique biometric data [includes] fingerprint, voice print, retina or iris image, or any other unique physical representation."[6]

Are there contexts in which the code should require encryption of Facial Recognition Data?

[Option A] "Encryption obligations should be appropriate for the context of the party's relationship with consumers"

[Option B] "Biometric data should be encrypted at rest and in transit, with strong encryption intended to protect that information for at least 15-20 years"[7]

---

[4] This is because different data is treated differently. If it is just hair color it might receive a lower protection than iris.

[5] Submitted by Michelle DeMoy of CDT

[6] Submitted by Michelle DeMoy of CDT – Wisconsin – Wis. Stat. § 134.98

[7] Submitted by Michelle DeMoy of CDT

Should the code distinguish between unencrypted data and those that are Encrypted? Could the code do so by establishing a "material risk of harm" threshold for notice, where a "material risk of harm" would arise when unencrypted templates are revealed to unauthorized entities?

It's difficult to enumerate all scenarios. Instead, it is better to make encryption obligations appropriate for the context of their relationship with consumers. However, there can be an exception for data accessed that is encrypted.

Would treating Encrypted data as not triggering a material risk of harm provide companies with appropriate incentives to design and implement robust security protections?

This should not constitute a data breach as most states treat unauthorized acquisition of encrypted data as not constituting a data breach.[8] Moreover, treating unauthorized acquisition of encrypted data could discourage incentives for encryption.

[8] See e.g. CA CIVIL CODE § 1798.80-1798.84 "when either the name or the data elements are *not* encrypted or redacted" (emphasis added)