Proskauer

Will the Role of Facial Recognition Grow in a Post-COVID-19 World?

New Media and Technology Blog on **March 31, 2020**

An interesting *New York Times* article last week posited that governments' use of digital surveillance techniques for the COVID-19 response – such as the tracking of geolocation to gauge quarantine restrictions – would lead to more pervasive digital tracking in the future. On a related note, there have been reports of an increased use of facial recognition technologies as governments use digital tools to respond to the outbreak.

These developments bring to mind some interesting questions:

In the future, given our collective experience with this invisible foe, will there be a move away from contact-based security and access control systems to "germless" and "touchless" processes?

If so, what role will be played by facial recognition and other biometrics-based systems in that shift?

Facial recognition is already in place and has, in some cases, began to replace contact-based systems. For example, facial recognition is being used in airports for security screenings, baggage drops, passport control and gate check-ins – and is largely being presented as an option to travelers to ease overcrowding and speed up processing time. Further, in March 2017, the President issued an executive order expediting the deployment of biometric verification of the identities of certain foreign travelers crossing U.S. borders. Indeed, U.S. Customs and Border Protection continues to roll out biometric scanning at checkpoints, such as recently at the Brownsville, Texas Port of Entry (but in December 2019 decided against making it mandatory for U.S. citizens to participate in airport facial recognition scanning when entering/leaving the country).

Thus, given these existing uses of the technology today, will the world's coronavirus experience spur the adoption of even wider use of facial recognition and similar "touchless" systems in the United States and abroad? If so, it is possible that facial recognition and similar technologies that minimize face-to-face encounters will become the norm for "checking in" large numbers of people, not only at airports and border crossings, but at stadiums, commuting systems, office buildings, government meetings and even at grocery stores (with the development of "cashierless" technology). Other "touchless" forms of biometrics – iris recognition, gait, etc. – may also see increased adoption. If so, it is possible that "contact" forms of biometrics (e.g., fingerprint systems) may be deemphasized over time, although that is likely to be a slow process due to the significant level of incumbent fingerprint-based systems in use today.

It is not clear that existing and emerging laws would support, in a consistent and balanced manner, such a widespread use of biometrics. As it stands, the legislative landscape in the United States associated with facial recognition addresses is inconsistent and complex.

A number of states have laws that address biometric information. Most notably, the Illinois Biometric Information Privacy Act has been the source of quite a bit of class-action litigation related to facial recognition technology. Also, among other state laws that address biometrics, the California Consumer Privacy Act (CCPA) includes "biometric information" within its definition of "personal information" regulated under the Act (See Cal. Civ. Code §1798.40(o)(1)(E)) and New York's SHIELD Act, which recently amended the state's data breach notification law and data security requirements, includes "biometric information" within its definition of "private information." Last year, California enacted a three-year moratorium on the use by law enforcement of facial recognition (and other biometric surveillance) in connection with body cameras. Numerous municipalities also have enacted restriction on the use of facial recognition. On the federal level, a number of the recently introduced privacy bills, including Senator Cantwell's Consumer Online Privacy Rights Act, take direct aim at facial recognition and biometrics.

The laws address important concerns associated with privacy, data security, and the shortcomings and failures of facial recognition technology. The issues they intend to address include how data is captured, how is it processed, how is it stored, how it is used, and who has access to it. In addition, there are significant concerns related to racial discrimination and the possibility of false positives or negatives, as well as inaccurate results or insufficient testing. Unfortunately, however, while many of these laws and proposals address issues associated with private sector, government and law enforcement use of facial recognition technology, they are in many ways inconsistent and difficult to satisfy across multiple jurisdictions.

Public health experts are saying that another similar pandemic is possible – and even likely – in the future. In order to use biometrics effectively to mitigate such risk, we need a uniform regulatory structure promoting such use while also protecting the privacy and civil rights of individuals. After the current crisis is resolved and life is back to normal, it may be worthwhile for representatives of the nation's technology community, civil rights and privacy advocates, and the legal community to work together to find a regulatory structure that protects privacy and civil rights while encouraging the use facial recognition to reduce the likelihood of similar public health emergencies in the future.

Proskauer's cross-disciplinary, cross-jurisdictional Coronavirus Response Team is focused on supporting and addressing client concerns. Visit our Coronavirus Resource Center for guidance on risk management measures, practical steps businesses can take and resources to help manage ongoing operations.

View Original

Related Professionals

- **Jeffrey D. Neuburger**