IBM **Policy Lab**

Bold Ideas for a Digital Society

Precision Regulation and Facial Recognition

By Christina Montgomery, Chief Privacy Officer, IBM
& Ryan Hagemann, co-Director, IBM Policy Lab

AI is systemic in our daily lives. Its algorithms improve supply chains so you can get your packages in days rather than weeks. AI systems predict when your car will need maintenance, they help with the efficient delivery of energy to our homes and offices. And innovations such as AI applications in health care and agriculture are improving peoples' lives the world over. Yet, at the same time, people are asking very important questions about potentially negative impacts of technology.

As policy makers worldwide consider how to address questions of trust in technology, IBM has consistently advanced the principle of precision regulation. This approach emphasizes carefully targeting policy to address legitimate concerns while promoting innovation, protecting consumer rights and ensuring accountability. Just as we called for this approach to stop the spread of **harmful online content**, we also believe it could help lawmakers address the privacy and civil rights concerns that have been raised around AI. As an example, consider facial recognition.

Our face is the most intimate and personal expression of our identity. It's who we are. So, it's perfectly reasonable for society to have some uneasiness about any technology capable of capturing, storing, and analyzing facial images, or potentially using them as a means of identification. However, blanket bans on technology are not the answer to concerns around specific use cases. Casting such a wide regulatory net runs the very real risk of cutting us off from the many – and potentially life-saving – benefits these technologies offer.

At IBM, we believe a precision regulation approach can inform a reasonably-balanced governance framework for facial recognition systems. But before considering what such a framework would look like, it's essential that policymakers fully understand that not all technology lumped under the umbrella of "facial recognition" is the same. While these systems may all include the same basic components, they fall into three basic and distinct categories:

1. ***Face Detection*** **-** these systems are capable of detecting that an object in a photo or video is, in fact, a face, and distinguishing it from other objects present. Importantly, it does this without identifying a face as belonging to a particular individual. Why is this helpful? In urban areas, it can help count and analyze flows of people, bicycles, and cars to reduce congestion or boost safety. It also could be used to estimate the crowd size at, say, a major sporting event.

2. ***Facial Authentication*** **-** this application is familiar to many smartphone users, who use it dozens of times per day to unlock their device or access apps. It works by comparing the features of a face image with those stored in a single, previously-stored profile. The technology maps the features of an individual's face for "1-to-1" authentication purposes, and is increasingly being deployed in airports to expedite boarding for travelers who opt-in.

3. ***Facial Matching*** **-** these systems attempt to match a face using features of a face image to those stored in a database. Facial matching is often associated with public safety and law enforcement applications, where it can be used to aid the search for missing children or help investigators more rapidly locate suspects. Unlike facial authentication systems, facial matching relies on "1-to-many" matching.

Each of these technologies and their uses can raise specific questions and possible concerns, ranging from privacy and civil liberties to user security and safety. In considering whether and how best to regulate any technology - from nuclear power to the internet - it is imperative to consider both the use and the ultimate end-user. Facial recognition systems are no different.

Instead of simply banning an entire category of technologies with so many possible applications, including many that are helpful and benign, policymakers should employ precision regulation that applies restrictions and oversight to particular use-cases and end-users where there is greater risk of societal harm. Broad rules that fail to differentiate between these various applications likely will lead to unintended consequences that can reach far beyond the issues targeted by the original regulation. For example, recent municipal bans on the use of facial recognition technology by government may cut consumers off from a convenience that could make one aspect of air travel a little less frustrating or aid first responders in rapidly identifying victims of a natural disaster. It simply does not make sense to subject a smartphone and a police body camera to the same regulatory treatment. The same technology used in different situations by different users should be governed by different rules.

There are also clear use cases that must be off-limits. For example, any use of facial recognition for mass surveillance or racial profiling is a clear violation of basic human rights and freedom, and no society should tolerate the use of technology to further such injustices. And providers of facial recognition technology must be accountable for ensuring they don't facilitate human rights abuses by deploying technologies such as facial matching in regimes known for human rights violations. The principles and laws that apply to the world of atoms should also apply to the world of bits.

At IBM, we believe in the power of innovation to make the world a smarter, healthier, and more prosperous place. And although technology itself is neutral, we fully appreciate that some

Policymakers should employ precision regulation that applies restrictions and oversight to particular use-cases and end-users where there is greater risk of societal harm.

technology could be deployed in ways that negatively impact society's trust and confidence in its potential. That's why we are committed to the responsible stewardship and deployment of new technologies, and why we believe precision regulation can strike the right balance between unlocking benefits and mitigating legitimate concerns.

Specific provisions we believe it would be appropriate to address through such regulation include:

Notice and Consent – as a general rule, organizations should be required to obtain an individual's consent before using facial recognition to authenticate their identity. In practice, obtaining this consent will look different based on the context in which the technology is deployed, but the ultimate responsibility for acquiring that consent should rest with the organization actually deploying the facial recognition system. For example:

- Social media platforms that scan uploaded photos for images of a user's face should be required to gain that user's express opt-in consent before the feature is activated. People deserve a clear, up-front understanding of how their image will be used and a chance to avoid that use if they're not comfortable with the details.

- Public signs that detect an individual's gender, age, or expression in order to deliver a more customized experience in a retail store or provide a more targeted advertisement experience should also be required to provide clear notification that face analytics is being used so a person can decide whether to participate or simply walk away.

These common-sense limitations that respect user's right to choice, and control over their personal information, should be the baseline for any responsible company or organization. And companies that choose not to comply should be subject to the full force of regulatory enforcement.

Export Abroad - The U.S. Department of Commerce maintains a list - the Commerce Control List, or CCL - of so-called "dual use" products that have both commercial or military applications and are therefore tightly controlled or all out prohibited for export to certain countries depending on how they will be used. That two-fold consideration - where the technology is going and how it will be used - is already used to limit the export of fingerprint and voice print identification and analysis scanners, and other devices capable of biometric identification. Facial recognition is not included on this control list, but that should be changed, especially for products capable of "1-to-many" matching. This is a proven approach to ensuring that U.S. technologies are not used by bad actors in ways that would violate American values.

Law Enforcement - there also are reasonable approaches that can balance the need for law enforcement's access to tools that can keep people safe while respecting Americans' privacy and civil liberties. In order to strike that balance, people need to trust this technology; and transparency breeds trust. As such, law enforcement use of facial recognition should be disclosed in regularly published reports mandated either by the Department of Justice or state attorneys general. And because the insights produced by this technology need context that can only be meaningfully provided by humans, we also agree that law enforcement agencies should require human involvement and validation at appropriate points in investigative processes that use facial recognition.

One example of an effort to apply precision regulation to facial recognition has just come from the United Kingdom, where the Information Commissioner has called for a "**binding code of practice**" to "give the police and the public enough knowledge as to when and how the police can use [live facial recognition] systems in public spaces." Live facial recognition, or LFR, is a subset of the "facial matching" category discussed above, and the commissioner's approach is very much consistent with our notion of requiring greater transparency and disclosure into the use and impact of these systems. As lawmakers worldwide grapple with public debate over this technology, different jurisdictions will develop different approaches based on their laws and customs, but the idea of applying precision to balance benefits and risks can be universal.

Policymakers should not wait to address public concerns over facial recognition. But calls for blanket bans are neither helpful nor practical. Why ban a technology that could save time, save money, or save lives? Government, industry and civil society groups must work together to move beyond lofty, hollow pronouncements, and focus on practical solutions to a very real-world problem. That's a conversation IBM welcomes.

About IBM Policy Lab

The IBM Policy Lab is a new forum providing policymakers with a vision and actionable recommendations to harness the benefits of innovation while ensuring trust in a world being reshaped by data. As businesses and governments break new ground and deploy technologies that are positively transforming our world, we work collaboratively on public policies to meet the challenges of tomorrow.