600 14th Street, N.W., Suite 300
Washington D.C., 20005

September 11, 2020

Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
14th Street and Constitution Ave., NW
Washington, D.C. 20230

Subject: BIS Notice of Inquiry on Advanced Surveillance Systems and Other Items of Human Rights Concern, BIS Docket No. BIS-2020-0021

Reference: RIN 0694-XC06

Attention: Steven Schrader, Foreign Policy Division, Office of Nonproliferation and Treaty Compliance

Dear Mr. Schrader:

On behalf of International Business Machines Corporation ("IBM"), we are submitting the following comments in response to the Bureau of Industry and Security's ("BIS") Notice of Inquiry regarding, Advanced Surveillance Systems and Other Items of Human Rights Concern, 85 Fed. Reg. 43,532 (BIS July 17, 2020) ("Notice of Inquiry"). IBM welcomes this opportunity to comment on the appropriate export controls for facial recognition technologies to address their implications for potential human rights abuses.

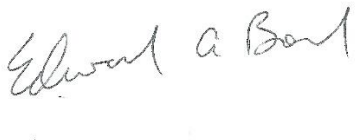
To that end, the following comments will provide a brief overview of the technical capabilities of various types of facial recognition systems. We will then describe the opportunities, and limitations, of potential controls focused on the individual components of this technology. Prior to concluding, we will then offer recommendations for BIS to consider as it moves forward with how best to regulate this emerging technology.

In particular, our recommendations include:

1. Updating the Crime Control country groups to reflect a country's human rights record;
2. Imposing new export controls on "1-to-many" facial recognition software; and
3. Making any export controls multilateral through the Wassenaar Arrangement or other mechanisms.

IBM commends BIS for this timely and important Notice of Inquiry. We thank you in advance for considering these comments and welcome the opportunity to engage with the agency as it moves forward in this process.

Respectfully submitted,



Edward A. Bond
Director, Export Regulation Office
Government & Regulatory Affairs
IBM Corporation

600 14th Street, N.W., Suite 300
Washington D.C., 20005

IBM Response to "BIS Notice of Inquiry on Advanced Surveillance Systems and Other Items of Human Rights Concern"

IBM has a strong corporate commitment to the responsible use of technology. For example, on June 8, 2020, IBM CEO Arvind Krishna sent a letter to the U.S. Congress outlining detailed policy proposals to advance racial equality in our nation. The letter also noted that, in the context of addressing responsible use of technology by law enforcement, IBM has sunset its own general purpose facial recognition and analysis software products. Specifically, the letter, attached as Exhibit 1, stated:

> IBM no longer offers general purpose IBM facial recognition or analysis software. IBM firmly opposes and will not condone uses of any technology, including facial recognition technology offered by other vendors, for mass surveillance, racial profiling, violations of basic human rights and freedoms, or any purpose which is not consistent with our values and Principles of Trust and Transparency. We believe now is the time to begin a national dialogue on whether and how facial recognition technology should be employed by domestic law enforcement agencies.

The Notice of Inquiry is appropriately timed as it seeks to address the myriad concerns with facial recognition and its potential misuse to commit human rights violations. Our comments will focus on the following issues:

1. The different types of facial recognition and which should be subject to export controls;
2. Export controls on the "components" of a facial recognition system;
3. The critical role of "training data" in limiting the scope and functionality of a facial recognition system;
4. The use of measurement vectors as technical control parameters; and
5. The appropriate imposition of end use and end user controls on facial recognition technologies.

Overview of Facial Recognition Applications

It is important for BIS to understand that not all technology lumped under the umbrella of "facial recognition" is the same. While these systems may include the same basic components (cameras, storage capacity, computing power, software algorithms), they fall into three distinct categories:

> Face Detection - these systems are capable of distinguishing a face from other objects, without identifying that face as belonging to a particular individual. These systems are capable of performing relatively benign tasks, such as counting and analyzing flows of people, bicycles, and cars in order to track and alleviate congestion.
>
> Facial Authentication - this application works by comparing the features of a face image with those of a single stored facial template. 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, or for the users of personal communications devices as an alternative to fingerprints as means of biometric access control.
>
> Facial Matching - these systems attempt to match a face to a database of stored facial templates. 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.

In considering whether and how best to regulate any technology – from nuclear power to the internet - it is imperative to consider both the use-case and the ultimate end-user. Facial recognition systems are no different. 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.

Instead of simply imposing export controls on an entire category of technologies with so many possible applications, including many that are helpful and benign, BIS should employ precision regulation that applies restrictions and oversight to particular use-cases and end-users where there is greater risk of societal harm. Regulations should be targeted to the use-case of a particular technology, and technology used in different

situations by different users should be governed by different rules. 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.

Importantly, however, there are also clear use-cases that must be off limits. As noted in IBM's June 8, 2020 letter to Congress, any use of facial recognition for mass surveillance or racial profiling is a violation of basic human rights and freedom, and no society should tolerate the use of technology to further such injustices. Government regulations need to be updated to ensure that exports do not facilitate human rights abuses through the use of technologies such as facial matching in regimes known for human rights violations.

Controls on the Components of a Facial Recognition System

As the Notice of Inquiry mentions, the major components of a facial recognition system are (1) input camera(s), (2) data storage, (3) processing computer, and (4) the software algorithms needed to model facial images.

IBM believes that any controls on facial recognition or other biometric technologies should be based on the principle of precision regulation - a narrow and targeted approach to regulating particular technological use-cases rather than broad/horizontal rules that apply to entire categories of technology (i.e., regulating *how* the technology is used, rather than the technology itself).

As such, we believe that it is appropriate to control facial recognition technologies that employ "1-to-many" matching end uses. This is the type of facial recognition technology most likely to be used for mass surveillance, racial profiling, or other violations of human rights. To effectively target export controls on these particular use-cases of facial recognition technologies, we believe such rules should focus on the high-resolution cameras used to collect data and the software algorithms used to analyze and match that data in the context of a "1-to-many" facial recognition system.

The computers used for the storage of data or the processing of collected information are difficult to use as the focal point for facial recognition controls, because they are often

commodity products that could be used for many different purposes. However, if the goal is to deny a repressive regime access to a mass surveillance facial recognition system, computing power that is part of a facial recognition system does become an important factor. Mass surveillance facial recognition systems that include high resolution cameras, computer systems, and software algorithms, require enormous amounts of computing power that involve billions of dollars of investment. Targeting specific end use and end user controls to limit a repressive regime's ability to obtain such large scale system components – specifically in the context of its use in an integrated facial recognition system – would be an effective mechanism for limiting the human rights abuses of a mass surveillance system. This would also be consistent with BIS's approach to controls on fingerprint analysis equipment.[1]

Facial Recognition Training Data

While it may be difficult to control, a critical component of any facial recognition system is the training data – the database of faces from various sources (mug shots, Twitter, Facebook, Google). A critical concept for the use of this data is the consent of the individual. For example, with regard to "1-to-1" facial recognition technology that is used in smartphones, the consent of the individual is implied by the fact that the user has set up the facial recognition functionality to unlock the phone. For mass surveillance databases of faces obtained from various sources, the consent of the individual may be unclear or non-existent.

Facial recognition systems do not work without this data. Controlling access to such data from online sources could be an effective way to limit certain human rights abuses. Limiting access to the training data can be an effective method for limiting the ability of a facial recognition system to conduct mass surveillance and do "1-to-many" matching.

Of course, we understand that this may be outside the scope of this Notice of Inquiry, and it could arguably be outside the scope of the Export Administration Regulations ("EAR"), as defined in Section 734. However, we believe that it is important for BIS to understand the full scope of a facial recognition system.

---

[1] See Guidance for ECCN 3A981 with respect to controls on fingerprint analysis equipment ("Thus this ECCN is aimed at entire systems and support equipment that would be useful for large scale identification systems, which include devices such as fingerprint scanning and booking stations that electronically capture single or multiple fingerprints.") available at: https://www.bis.doc.gov/index.php/policy-guidance/product-guidance/fingerprint-analysis-equipment

Technical Parameters for Export Controls on Facial Recognition

Any export controls on facial recognition should focus on those aspects of the technology that pose the greatest risks to human rights, namely broad facial recognition that relies on "1-to-many" matching. To the extent possible, BIS should focus on controlling facial recognition technologies around certain unacceptable use-cases and for use by potentially problematic end users. The end use and end user matter greatly.

However, there are some technical parameters in facial recognition software that can serve as a guideline for export controls. Facial recognition works by taking measurements across different vectors on a person's face. Currently, the industry standard is 128 vectors. In a "1-to-many" use-case scenario, those vectors are then compared to a database of faces – for example, mug shots – in order to attempt an identification. The software algorithms that conduct this analysis will then return a probability of a match based on a comparison of the vector measurements to the database of faces. The more vectors that you can capture, the better the accuracy of the match.

In an effort to limit the ability of repressive regimes to take advantage of facial recognition technologies, IBM would recommend controls on "1-to-many" facial recognition software.

It is vitally important that whatever controls on facial recognition technology are adopted by the United States be made multilateral. Given the globally diffuse nature of many of these technologies, in order for export controls to be most effective the U.S. Government should endeavor to make any export controls multilateral through the Wassenaar Arrangement. We believe many members will be interested in cooperation on this topic. Should consensus within Wassenaar prove impossible, the United States should consider ad hoc plurilateral arrangements with like-minded allies to maximize the international application of export controls on facial recognition used in ways that pose human rights concerns.

End Use and End User Controls on Facial Recognition

Facial recognition export controls should focus on countries and end users of concern. In particular, controls on the most powerful types of facial recognition technology should be focused on those countries that have a history of human rights abuses, in particular

those who may employ "1-to-many" matching functionality. Any export controls on facial recognition technologies should be combined with end use and end user controls targeting those whose misuse of these technologies poses the greatest threat to human rights. One approach would be to identify specific companies or government agencies that are the target of these controls, in addition to broad country-based limits. In the latter context, BIS should update the Country Chart in Supplement No. 1 to Part 738 of the EAR to include those countries that pose the potential for human rights abuses related to the use of mass surveillance. IBM recommends updating the Crime Control country groups to reflect a country's human rights record.

We thank you for the opportunity to provide the above comments and we look forward to contributing further to this process.