INFLECTION POINTS: FACIAL RECOGNITION TECHNOLOGY IN THE UNITED STATES AND CHINA

SAMUEL CURTIS

9 · 30 · 2020

INFLECTION POINTS:
Facial Recognition Technology in the United States and China

INTRODUCTION

Facial recognition technology (FRT) has made a swift foray into the public sphere. With numerous advantages over other biometric surveillance techniques—such as the ability to surveil at a distance, and without subjects' knowledge—FRT has entered the global market as the ostensible be-all and end-all of 21st century surveillance technology. Its success has been catalyzed by advancements in machine learning, steep drops in hardware and computation prices, and an ever-growing desire in public and private sectors for surveillance and security.

***A NOTE ON TERMS**: FRT takes many forms, from providing identification on mobile devices, access control (permitting or denying entry past a checkpoint) into private places, and private and public surveillance. This article focuses primarily on the use of FRT by public security entities, such as national, state, or local police and counterterrorism forces.*

The use of technology in surveillance has also been one factor accelerating tensions between the United States and China. Last year, the US Commerce Department sanctioned nine Chinese surveillance technology companies for being "complicit in human rights violations and abuses committed in China's campaign of repression, mass arbitrary detention, forced labor and high-technology surveillance against Uighurs, ethnic Kazakhs, and other members of Muslim minority groups in the Xinjiang Uighur Autonomous Region."[1] More recently, facial recognition companies in the United States have faced a reckoning of their own, with industry leaders IBM, Amazon, and Microsoft deciding to pause or terminate the development of their technology for police forces following pressure from civil rights advocates and an upswell of antiracist activism.[2]

As with all public surveillance tools, FRT exacerbates existing power asymmetries between people and the state and places a burden on governments to use and store information responsibly. The degree of people's trust towards their governments, which differs greatly between the United States and China, may be the most salient determinant of the role the technology plays in each respective country. As the United States and China are the predominant developers and exporters of FRT, their decisions over the next few years will steer adoption of the technology—shaping state surveillance, municipal policing portfolios, and day-to-day civilian life worldwide.

This report provides an outline of the current FRT systems deployed by public security entities in the United States and China, and the laws, development initiatives, and practices that molded these surveillance networks. It investigates how the various stakeholders—government entities, domestic FRT companies, civil advocacy groups, and the general public—have played a role in the deployment of FRT in each country. Finally, it analyzes the differences and similarities between the two countries' FRT programs, and to what extent there are possibilities for constructive dialogue between the two countries on the responsible development or curtailment of FRT.

INTERNATIONAL CONTEXT

FRT is quickly being embraced around the world by authoritarian and democratic countries alike. A 2019 Carnegie Endowment report found that at least 64 governments are using FRT to some degree, and this number has increased drastically over the course of just a few years.[3] Some governments are using the technology to enhance border security or react to or prevent crimes; others utilize FRT with the prima facie goal of quelling opposition and cementing their grip on power.

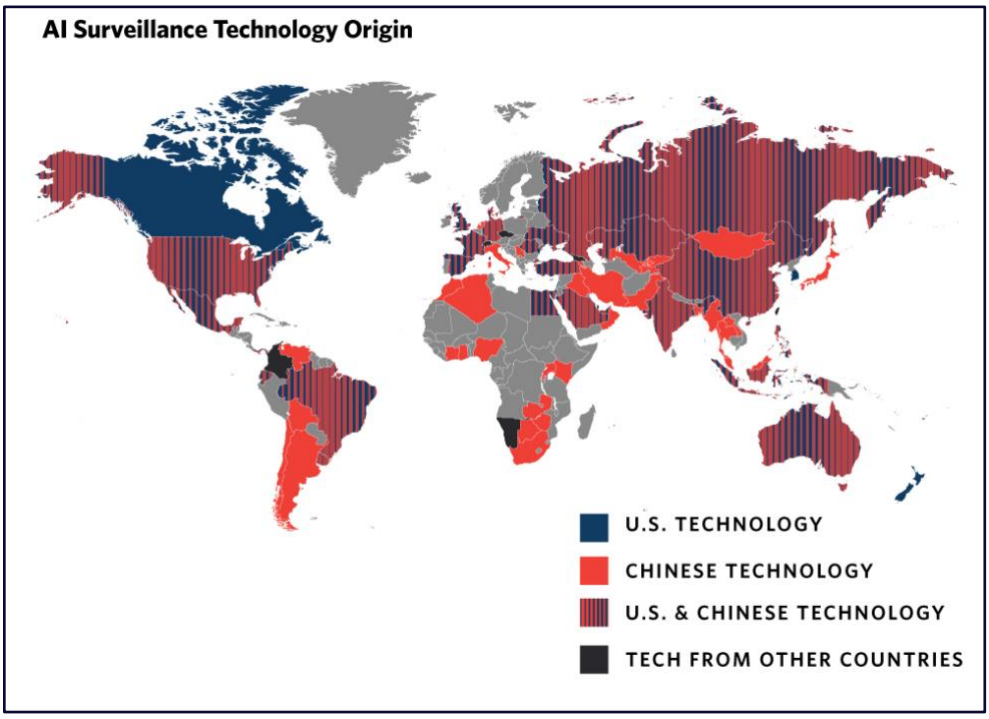


Figure 1: Regional Difference in Chinese Pharmaceutical Developments

Source: The Carnegie Endowment. https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847

Note: This map of AI surveillance technology includes not only FRT but also smart city/safe city platforms and smart policing technology.

The COVID-19 pandemic has catalyzed the demand for surveillance technologies to aid contact tracing and access control efforts worldwide. Surely, the disparate responses by the surveillance-skeptic United States and surveillance-heavy China have been influential in this respect. In particular, demand has soared for FRT capable of recognizing masked faces and performing simultaneous infrared sensing.[4] Even though these new features are relatively untested (and some demonstrably shoddy),[5] many governments are eager to invest in unproven tools to bolster their surveillance capabilities.

Chinese companies dominate the international market, and many of them developing countries and partners in China's Belt and Road Initiative (BRI).[6] US companies are also prominent exporters; however, with markedly less endorsement and fiscal support from government entities, they have struggled to keep up with China's sales. In fact, at present, the US government and numerous US FRT companies *themselves* are in the midst of evaluating the technology's implications for human rights and their roles as exporters.

Companies in other countries, including Japan, Israel, and South Korea, are also prominent exporters.[7] Due to the size and strength of these companies, and the widespread demand for surveillance technology, the imposition of any US export control on FRT may only irreversibly disrupt the global market if the United States were able to persuade allies and "global swing states" to do so as well.

THE UNITED STATES

The use of FRT by public security agencies in the United States dates back almost 20 years, in line with the emergence of the "Homeland Security era" following the September 11 attacks.[8] In the time since, numerous federal departments and several hundred state and local police agencies have developed or acquired FRT. Currently, most FRT systems are used for retrospective forensic analysis—using software to identify a person from a photo or video still after an event has occurred—but a growing number of agencies have begun to use FRT systems for real-time analysis as well.[9] This growth trend may have hit a ceiling, however, as movements have been gaining steam amongst tech companies, civil rights organizations, and facets of the government itself to curtail the reach of "intelligence-led policing."

In 2016, a report from the US Government Accountability Office (GAO) revealed that the Next Generation Interstate Photo System (NGI-IPS), operated by the Federal Bureau of Investigation (FBI), allows not only federal bureau agents but also state and local law enforcement agencies to submit identification requests against a database of nearly 30 million photos, composed primarily of booking mugshots.[10] Additionally, the report disclosed that since 2011, the FBI's internal unit called Facial Analysis, Comparison, and Evaluation (FACE) Services has been tapping into databases owned by the Department of State, Department of Defense, and at least 16 state Department of Motor Vehicles databases (containing driver's license photographs) to support active investigations.[11] This came as a surprise to government watchdogs, because, historically, access to biometric data by federal agencies had been limited to data from criminal investigations or arrests.[12] Researchers at the Center on Privacy & Technology at Georgetown Law have also found evidence of other federal agencies, including the Department of Defense, the Drug Enforcement Administration, Immigration and Customs Enforcement (ICE), and the US Marshals Service having access to one or more state or local facial recognition systems.[13]

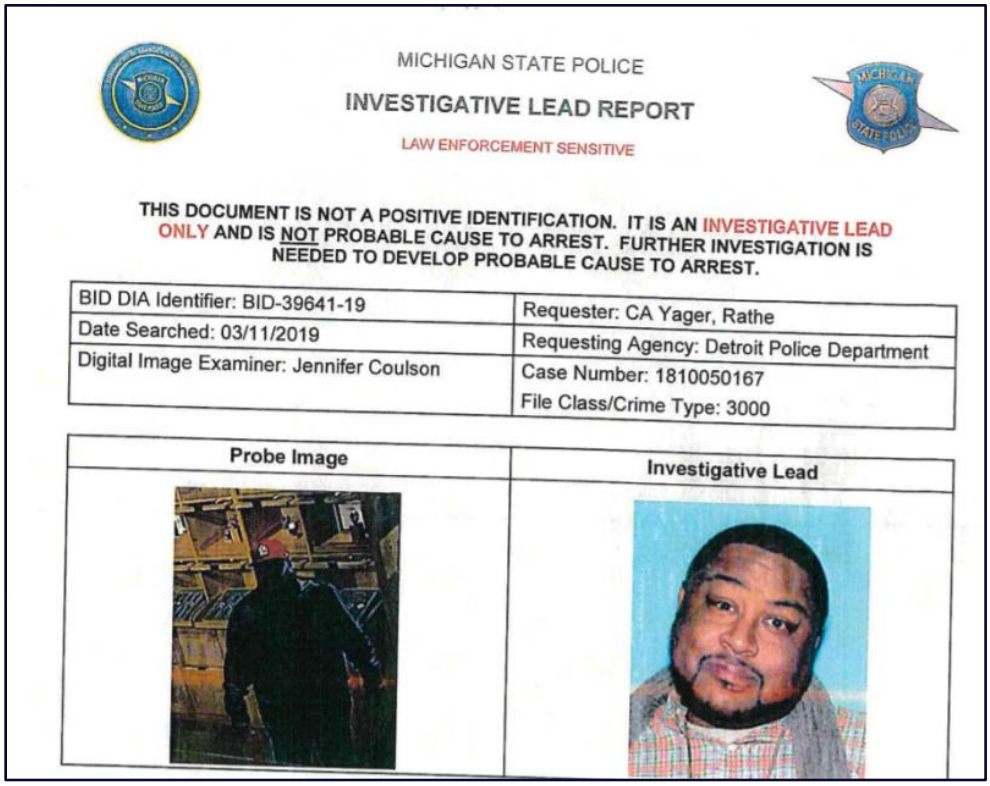
In addition to creating and maintaining their own facial recognition systems, state and local police forces are able to query the FBI to conduct searches through the NGI-IPS network of federal, state, and local databases of criminal photos. For most of the past 20 years, state and local facial image databases have been limited to booking mugshots or driver's license photographs; however, earlier this year, the *New York Times* (NYT) exposed an unsettling trend of state and local police agencies subcontracting private companies with facial recognition systems that utilize data outside of government databases.[14] In a January 2020 exposé titled, "The Secretive Company That Might End Privacy as We Know It," the NYT illuminated how a company called Clearview AI had scraped the internet—including Facebook, YouTube, and Venmo, among millions of sites—for publicly available data.[15] Clearview AI was licensing its software to more than 600 law enforcement agencies across the United States (as well as many private-sector clients) and was leveraging its political connections to further expand sales to police forces.[16] Since the expose's publication, 11 class actions and numerous other lawsuits have been filed—most of which allege a violation of individual states' biometric information privacy laws[17]—but the limited scope of these cases and the uncertainty around their outcomes highlight the need for comprehensive regulation at the federal level.

Although Clearview AI continues to peddle its technology (even having signed a contract with ICE in August 2020),[18] some of the largest tech companies in the United States have recently decided to stall or terminate their facial recognition programs. First, in June 2020, IBM's CEO Arvind Krishna, in a letter to numerous members of Congress, announced that the company

would be terminating its general purpose facial recognition and analysis software products, stating, "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."[19] Two days later, Amazon announced a one-year moratorium on police use of its Rekognition software, calling on Congress to "put in place stronger regulations to govern the ethical use of facial recognition technology."[20] The following day, Microsoft followed suit, with the company's president, Brad Smith, stating the company would wait until a national law was in place that was "grounded in human rights."[21]

These developments would likely not have occurred without the research and advocacy of numerous scholars and civil rights advocates who have brought to light FRT's shortcomings. In 2018, an MIT Media Lab team led by Joy Buolamwini published a landmark study titled "Gender Shades," which exposed disparate performances of facial analysis tools to classify gender across race and sex: algorithms from three of the world's leading software companies all performed significantly poorer with darker-skinned faces, particularly darker-skinned females.[22] Two civil advocacy groups emerged from that team to advocate for racial and social justice in AI development: Black in AI, founded by Timnit Gebru, and the Algorithmic Justice League, founded by Buolamwini. Numerous other organizations have also made the regulation or banning of FRT central to their missions, including the American Civil Liberties Union (ACLU), Fight for the Future, the Center on Privacy & Technology at Georgetown Law, and the AI Now Institute. In addition to the inconsistent performances of FRT across sex and race, these organizations decry the notably poor performance of police-acquired FRT systems, the vulnerability of data collected by FRT, and infringements of Fourth Amendment rights. The 2020 Black Lives Matter protests further garnered energy behind these movements by bringing institutional racism and police accountability into greater focus and have played an indispensable role in pushing companies to self-regulate.

Indeed, in the same month that major tech companies took stances in favor of regulating the technology, an incident took place that served as a sobering lesson as to why government accountability, independent media, and civil advocacy activity are so important: Robert Julian-Borchak Williams, a black man from Farmington Hills, Michigan, was forced to spend 30 hours in a detention center after the FRT deployed by the Detroit Police Department erroneously identified him as having carried out a robbery.[23]



MICHIGAN STATE POLICE

INVESTIGATIVE LEAD REPORT

LAW ENFORCEMENT SENSITIVE

THIS DOCUMENT IS NOT A POSITIVE IDENTIFICATION. IT IS AN INVESTIGATIVE LEAD ONLY AND IS NOT PROBABLE CAUSE TO ARREST. FURTHER INVESTIGATION IS NEEDED TO DEVELOP PROBABLE CAUSE TO ARREST.

BID DIA Identifier: BID-39641-19	Requester: CA Yager, Rathe
Date Searched: 03/11/2019	Requesting Agency: Detroit Police Department
Digital Image Examiner: Jennifer Coulson	Case Number: 1810050167
	File Class/Crime Type: 3000

Probe Image	Investigative Lead

Figure 2: The probe image used by the Detroit Police Department matched with a drivers license photo of Robert Julian-Borchak Williams, determined sufficient for an investigative lead.
Source: ACLU of Michigan, https://knpr.org/npr/2020-06/computer-got-it-wrong-how-facial-recognition-led-false-arrest-black-man [24]

In the absence of national regulation of FRT use by police forces, a patchwork of cities and states has passed their own laws. Some cities, such as San Francisco, California and Somerville, Massachusetts, have passed ordinances banning the use of FRT by public officials, and Portland, Oregon, very recently became the first city to ban FRT for security purposes in the public *and* private sectors. A few states, including Oregon, New Hampshire, and California, have banned FRT in police body cameras;[25] pending action on a bill in its State Senate, Massachusetts could become the first state to place a moratorium on, or ban outright, police use of FRT in any form or fashion.[26] With so much attention drawn towards police reform, we should expect to see numerous cities and states follow suit in the near future.

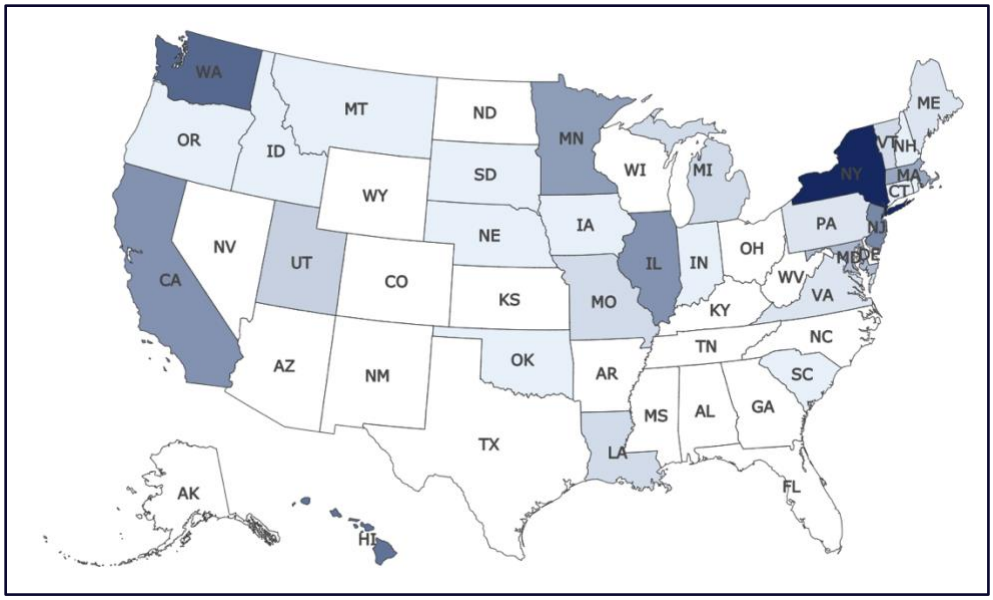


Figure 3: A patchwork of states where FRT legislation is pending; the darker the blue, the higher the number of pending bills as of September 18, 2020.

Source: Electronic Privacy Information Center.[27] https://epic.org/state-policy/facialrecognition/

On a federal level, bills have been introduced to both the House and Senate, including the Commercial Facial Recognition Privacy Act of 2019 (S.847), the National Biometric Information Privacy Act of 2020 (S.4400), and the Facial Recognition and Biometric Technology Moratorium Act of 2020 (S.4084; H.R.7356).[28] Though some of these bills have received some bipartisan support, none has made it to a vote, and they are unlikely to be passed during the current Republican-controlled congressional session or signed into law by the current presidential administration. Thus, national legislation regulating FRT likely rests on the outcome of the 2020 presidential election.

In spite of this standstill, anti-FRT sentiment is percolating in other federal government departments. In July 2020, the GAO issued a lengthy report on the privacy and accuracy issues related to commercial uses of FRT.[29] Days later, the Department of Commerce Bureau of Industry and Security decided to reconsider the export control of advanced surveillance systems—principally, FRT—to "promote human rights throughout the world," issuing a plea for public comment from academics and industry experts on its website.[30] If the United States were to impose export control on FRT designated for use by certain entities or in certain applications, it would likely try to hold its allies and "global swing states" to the same standard in order to challenge China's political and economic sphere of influence.

CHINA

As a whole, China's public security entities wield much more expansive and interoperable FRT systems than those of the United States. Real-time surveillance (as opposed to retrospective forensic analysis) is also used to a much greater degree, and even, in limited terrains, to identify and publicly denounce individuals breaking laws. (Readers may be familiar with FRT systems that have been installed at some intersections to identify and broadcast the faces and names of jaywalkers.)[31] Though there have been some public grievances about the technology's use in certain applications or locales, citizens overall approve of its use, and support has even rallied as innovative contact tracing and access control methods were rapidly rolled out earlier this year, and appeared to be effective in controlling the spread of COVID-19 within China's borders.

The degree to which FRT has been integrated into public security lends itself to a prolonged, policy-driven framework designed to utilize advanced surveillance technologies. In the early 2000s, China's MPS was in fact following the lead of the United States and United Kingdom in operationalizing "intelligence-led policing" (*qingbao zhidao jingwu* 情报指导警务). In the time since, however, China's "public security informatization" (*gong'an xinxihua* 公安信息化) pursuits have surpassed those of any other country, and large-scale domestic data collection mechanisms and interoperable sharing protocols have streamlined the integration of FRT.

A key component in this endeavor has been China's "Golden Shield Project" (*jindun gongcheng* 金盾工程), launched in 2003, which systematized public security information sharing by creating a nationwide "public security trunk network" (*gong'an wang* 公安网), permeating every province, municipality, city, prefecture, and police unit.[32] Another component of the Golden Shield was to create information command centers (*zhihui zhongxin* 指挥中心) at the ministerial, provincial, and municipal tiers, responsible for coordinating information transfers across departments or jurisdictions.[33] Together, these steps connected MPS networks once scattered or siloed, and granted every police officer the capability of sending and receiving information through the network.

Another keystone initiative of China's intelligence-led policing has been the "SkyNet" (*tianwang* 天网) project, initiated in 2005 by the MPS and the Ministry of Industry and Information Technology, aiming to fight crime and prevent possible disasters via the widespread installation of CCTV cameras in public spaces.[34] The project aimed to provide "100 percent coverage" in certain trafficked areas—including public spaces in residential communities (*xiaoqu* 小区)—by

2020.[35] In 2017, China Central Television Network reported that the SkyNet project was complete, suggesting that the roughly 176 million surveillance cameras in China had been connected, and plans had been drawn to increase that number to 626 million by 2020.[36] The government has yet to confirm whether this latter benchmark has been achieved.

Building on the foundation of the SkyNet project, in 2015, China's National Resource and Development Commission (NRDC) announced the "Sharp Eyes Project" (*xueliang gongcheng* 雪亮工程) with the goal of incorporating public surveillance cameras into the "informatization" architecture at the county, township, and village levels, with an emphasis on rural areas where coverage had been sparser. Receiving its name from a Chinese idiom, "the eyes of the masses are sharp" (*qunzhong de yanjing shi xueliang de* 群众的眼睛是雪亮的), often attributed to Mao Zedong, the project was initially established through a January 2018 policy memo by the Central Committee and State Council, entitled "Opinions of the Central Committee of the Communist Party of China and the State Council on the Implementation of the Strategy of Rural Revitalization."[37]

In addition to policies aimed at policing and surveillance, FRT development and deployment have been aided by mutually-reinforcing policies issued by the Central Government, such as Made in China 2025,[38] a component of China's Thirteenth Five-Year Plan (2016–2020), and the 2017 State Council's Next Generation Artificial Intelligence Plan.[39] Another policy initiative, introduced in 2018 by the Chinese Communist Party (CCP) General Office, requires all government offices and public institutions to rely entirely on domestic suppliers by 2021.[40] As a whole, these policies are in line with China's long-term transition into an "innovation-oriented society," marked by increased spending in domestic research and development, and have provided massive capital flows towards domestic technology by creating subsidies and tax incentives for technology startups (particularly in Smart City environments).

China has also sought to reinforce its prominence in FRT and video surveillance by undertaking leading roles in international standards-setting bodies. In December 2019, Dahua Technology, China Telecom, and ZTE proposed new international standards to the UN's International Telecommunications Union (ITU).[41] Proposals included recommendations for proper technological applications, which data should be collected, and how the data should be stored. Proposals were also put forward that included technological features: in some cases, features that the telecommunications companies themselves develop and employ.[42] The benefits of this current approach are twofold: Chinese companies are able to set technological requirements that match the proprietary features of their products, thereby bolstering their market; China is also able to influence foreign attitudes and governance by determining the "proper use" of facial recognition, video monitoring, city and vehicle surveillance for the more than 200 member states of the ITU.

It is important to note here the large role that robust standards plays in cultivating societal trust in the technology—when technology performs as expected, the risk of societal backlash is reduced.[43]

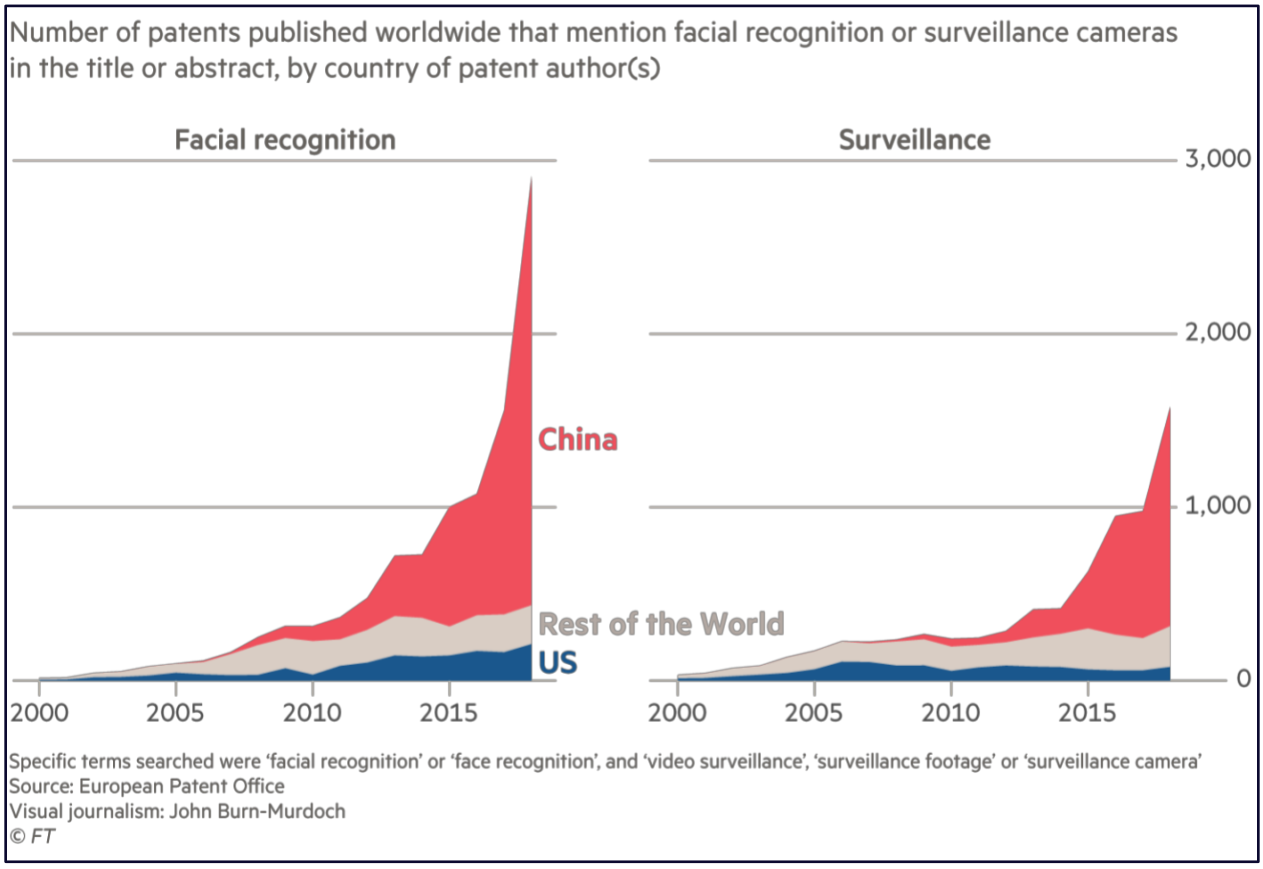


Figure 3A: Number of patents published that mention facial recognition or surveillance cameras in title or abstract, by country of patent author(s)

Source: Ten Charts That Tell the Story of 2019. Financial Times, https://www.ft.com/content/62fbf660-2651-11ea-9a4f-963f0ec7e134 [44]

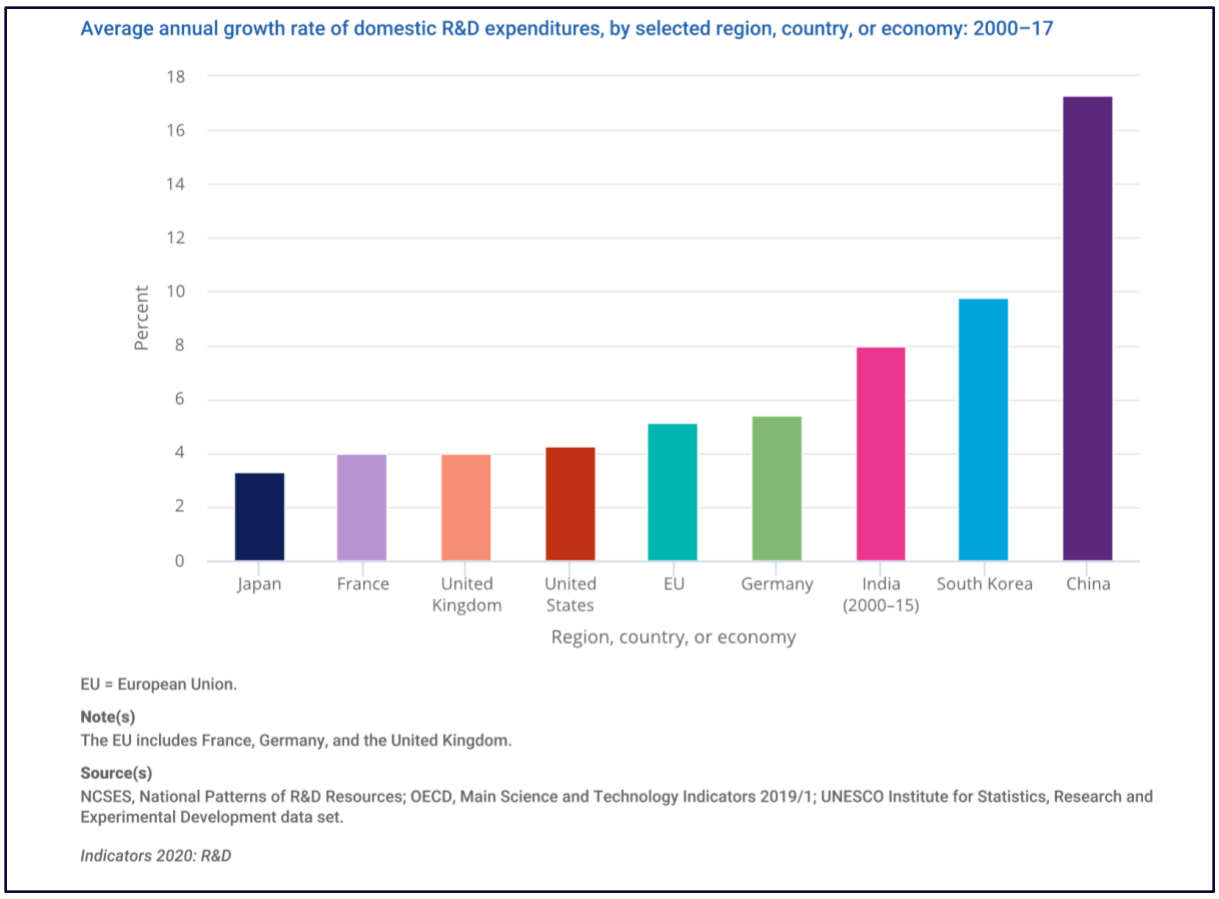


Figure 3B: Average annual growth rate of domestic R&D expenditures: 2000–2017

Source: "The State of U.S. Science and Engineering 2020." National Science Foundation, https://ncses.nsf.gov/pubs/nsb20201. [45]

With these policies and standards in place, Chinese FRT companies have experienced a surge in growth, driven by domestic and foreign demand and increased Chinese expenditures in research and development. In 2019, SenseTime experienced a revenue increase of 200%, amounting to around USD 750 million,[46] Dahua Technology's revenue increased 10.5% to USD 3.73 billion,[47] and Hikvision's revenue increased 16% to USD 8.15 billion, year on year.[48] Megvii faced losses in the second half of 2019 but experienced a big boost during the COVID-19 pandemic and is racing another quickly-rising biometrics firm, CloudWalk, to enter the Shanghai Stock Exchanges.[49] This growth has taken place *in spite* of the United States blacklisting all of these (and more than 50 other) companies—most since October 2019.

To clarify: due to the aforementioned policies, security camera coverage may be ubiquitous, but it is difficult to know the *true extent* to which facial recognition software has been integrated into physical networks. These figures are highly confidential. FRT use assuredly differs across municipalities and provinces, all of which adhere to State Council planning but operate within the

means of their respective budgets. Connectivity would also depend on the production date and model of the hardware. Heavily trafficked areas have most likely been retrofitted with new technology, but some less active areas may contain outdated or lower-resolution hardware incompatible with FRT protocols.

But we can deduce from the rapid growth of Chinese FRT companies that network integration is occurring quickly. To illustrate how effective these networks can be, in December 2017, one BBC news anchor was invited to Guiyang, a city of approximately 3.5 million people, to see how long he could avoid being identified by the city's network of cameras and detained by police. It took all of seven minutes after his arrival.[50] Was this staged? Perhaps. In any case, it delivered a clear message: in many locales, real-time FRT surveillance has been fully operationalized.

Domestic academics, think tanks, and non-governmental organizations (NGOs) play an important role in shaping tech policy; however, they function differently from their US counterparts. While they retain a degree of operational autonomy, they face a great risk in positioning themselves in abject opposition to the Communist Party, as it would label their organizations and members—many of whom may have public sector occupations—as national security risks.[51] It would also be ineffective, from an advocacy perspective, as their message may be condemned or censored by state-controlled media. Thus, they spend a significant part of their resources gauging and delicately steering public opinion, which is arguably more effective toward achieving policy goals. This also explains why these groups avoid sensitive topics, such as human rights, and focus more on the environment, public health, and education.[52] With these conditions in mind, the Beijing Academy of AI (BAAI), for example, has begun publishing papers on responsible FRT development[53] and has also begun a series of surveys to determine citizens' attitudes toward a range of FRT use cases that emerged in the COVID-19 pandemic.[54]

FRT companies seem to be entering agenda-setting roles as well. In November 2019, SenseTime announced that it would be leading a National Facial Recognition Working Group, along with 26 other Chinese FRT companies, to draft national standards and specifications to ensure "function, performance and safety requirements of [FRT], the accuracy of algorithms and applications, [and] to guide the healthy and rapid development of technology."[55] In January 2020, Megvii established an AI Governance Institute and, in its WeChat announcement, surveyed users for their feedback on the ethicality of the use of surveillance technologies in a range of scenarios[56] and later publicly shared and analyzed the responses.[57] This was the first major poll of its kind by an FRT company in China.

And indeed, state media plays a significant part in supporting intelligence-led policing efforts. As the Chinese government has rolled out its SkyNet and Sharp Eyes initiatives, state-sponsored media has incorporated the technology into its "harmonious society" narrative by highlighting its capability to assist local-level anti-corruption efforts, and publishing stories of long-lost criminals located instantaneously with FRT.[58] Subsequent interviews with Chinese citizens suggest that the general public adheres to this narrative—one 2020 survey by Kostka *et al.* found that 51% of respondents approved and 22% opposed the public use of FRT in China.[59] Another survey, conducted by the BAAI, found respondents overwhelmingly supportive of the use of FRT to support public health security during public health crises, though retained concerns about data privacy.[60]

Figure 4A: A cartoon depicting SkyNet.

Source: Wang Duo Zou, China Discipline Inspection and Supervision News Agency. "中国纪检监察报 – '花式'逃亡终难逃法网." [61]

"This set-top box is installed with a program that has multiple functions. You can watch TV or press one key to alarm."

In Group 7 of Guangzhao Village, Jin'e Street, Longchang County, Sichuan Province, villager Yanping watches TV while doing manual work. She put her hands down and pressed the remote control, and the TV screen showed the security control screen. "Now I'm relieved to go out. I go dancing dam dance after dinner every day, and the door doesn't have to be closed," Yan Ping said.

Figure 4B: Translated Excerpt from "Xueliang Project Keeps Peace-Rule of Law"

Source: "Xueliang Project' Keeps Peace-Rule of Law", Peoples Net. "雪亮工程'保平安——法治——人民网."[62]

The past year, however, there have been numerous notable instances of Chinese academics speaking out against the widespread rollout of FRT. In November of 2019, Zhejiang Sci-Tech University law professor Gou Bing filed a lawsuit against the Hangzhou Safari Park for denying

him entrance after he refused to register for their newly-implemented facial recognition registration system.[63] (In response to the lawsuit, the park agreed to allow visitors entry via a fingerprint registration system, if they wish.)[64] Then, in December, Tsinghua University's Professor of Law Lao Dongyan published a lengthy denunciation of the implementation of FRT on her public WeChat blog, igniting conversations on both English- and Chinese-language media.[65] And lately, throughout the COVID-19 pandemic, Peking University Professor of Journalism and Communication Hu Yong has published a series of WeChat posts for his over 800,000 followers, in which he has criticized the unrestrained collection of personal identifying information (without naming FRT explicitly) during the pandemic.[66] That the Chinese government, ever sensitive to dissent, did not censor such discussion is notable. The responsible entities must have felt that there was benefit in allowing discussions to take place, perhaps in tracking the flow of information to contain threats before they materialize, or perhaps in the ability to gauge, and thus better guide, public opinion.[67]

However, in general, support for the public use of FRT from the central government, local governments, and crucially, the general public, remains high. Its development stimulates economic growth and helps the government achieve its goal of securing China as a leader in AI technologies. It will likely remain a prominent fixture in state security and economic growth, and may become an inlet to more abstract forms of computation, such as *affect recognition*, which is explored further in Sébastian Krier's piece in this series.[68]

ANALYSIS

This section explores the differences and similarities between the use of FRT by public security entities in the United States and China. It analyzes FRT within the Asia Society's Green-Yellow-Red Framework, suggests possible means of collaboration between the two countries, amongst other global stakeholders, and elaborates as to why alignment on the ethics and legality of FRT applications may be urgent.

Differences

As this report has demonstrated, US and Chinese public security entities use FRT in widely different capacities and receive varying degrees of support from their respective governments,

institutions, and the general public. As such, the development, use, and export of FRT by both countries now seem to be on divergent trajectories.

A prominent underlying cause may be the prevailing values of each country. A comparison is commonly drawn between the cultural values of individual liberty in the United States and that of a "harmonious society" (*hexie shehui* 和谐社会) in China. Jessica Cussins Newman touched upon how this applies to AI principle alignment in her piece in this series, pointing out that Chinese scholars tend to focus on "harmonious design" as opposed to "human-centered design."[69] Danit Gal and Rogier Creemers also provide intriguing investigations into how these values manifest in discussions, guiding documents, and practices in the AI sphere in the recent Nesta publication "The AI Powered State: China's Approach to Public Sector Innovation."[70]

FRT sits at the nexus of these divergent ideologies. In places where values of individual liberty prevail, the use of FRT can be perceived as unduly dispossessing people of their privacy. Unlike conventional geolocation methods, such as smartphone software, FRT does not require a person's knowledge or consent: whereas mobile devices can be left at home, faces cannot.

On the other hand, among populations where "harmony" (*he* 和) is a preeminent value, FRT is viewed as an effective tool to marshal behavior. Assuming criminals are rational actors, an increased likelihood of getting caught should deter criminal behavior; thus, the real appeal of FRT is not its superior capability to identify criminals or find missing persons, but the downstream benefit of deterring unlawful activity in the first place. This is not to say that the Chinese people do not value their privacy of their facial data (in fact, surveys indicate that they do),[71] but that other factors are comparatively more expendable to maintain "harmony." With these societal values and characteristics of FRT in mind, it is understandable why the technology has been received differently in each environment.

Interestingly, the ethos behind these ideologies is analogous to competing arguments of contemporary AI thought leaders. In one corner, the civil rights advocates and whistleblowing academics, previously mentioned in this report, urge a retrenchment from automated decision making that infringes on individual liberties. In the other, existential-risk thought leaders, such as Zhao Tingyang[72] and Nick Bostrom,[73] give merit to global surveillance mechanisms to curb massively destructive behaviors. To their credit, both Zhao and Bostrom both have acknowledged that mass surveillance mechanisms are fraught with risks, and navigating these challenges would require effective interstate global governance.

Similarities

The present similarities between the United States and China with respect to the use and acceptance of FRT are few. However, regardless of the course that FRT development takes in the next few years, both countries will need to navigate similar challenges, such as those of data privacy, misaligned economic incentives, and the meta-level hazards of predictive policing.

Coinciding with the spread of FRT are the growing repositories of data—images, vectors, and other personally identifiable information—that governments have a responsibility to handle data appropriately. Unfortunately, both governments have a troubled history of mishandling personal information. For example, in January 2020, a database for a school surveillance system that covered 23 schools and companies in Sichuan and Gansu provinces was found open and unencrypted, leaving 1.3 million data points, including facial data, available to the public.[74] In the United States, police departments put their communities at risk by subcontracting private FRT companies: in April 2020, Clearview AI, the company that more than 600 US police forces have subcontracted, announced that a hacker had gained unauthorized access to its entire client list.[75] Such events expose the general public to the risk that any entity—foreign government or private company—could access and use their data for nefarious purposes. It should be in the general interest of both countries to securely handle their people's data. China has as of late made progress towards this end with the enactment of the Personal Information Security Specification in February 2019,[76] but without provisions for biometric information in particular, the law is insufficient at addressing the ramifications of pervasive biometric surveillance.[77]

Another challenge facing both the United States and China are the ways in which misaligned economic incentives may lead to adverse security, human rights, or public health outcomes. In a period of global economic decline, countries are keen to foster their innovative sectors and sell advanced, in-demand technologies. FRT fits the bill remarkably, with desirable value propositions, subscription models that secure long-term passive income, and many prospective clients over large swaths of geography yet to be covered. But at some point, to maximize profits, companies may begin to offer products or services that are underdeveloped, inadvertently counterproductive, or even fraudulent. Likewise, in order to spur growth in their innovative sectors, governments may spend more on the technology than the value it provides to taxpayers.

One extreme example of a nefarious profit-seeking practice has been the sale of rigged fever-sensing cameras during the COVID-19 pandemic. As the outbreak began to unfold, numerous

Chinese surveillance camera retailers sold cameras that they claimed to be capable of accurately identifying faces and measuring temperatures. Later on, it was uncovered that some of these cameras were fraudulent—designed not to conduct any temperature measurement, but only to display a normal human body temperature, as if one had been measured, whenever they recognized a face.[78] Purchases of this equipment not only wasted a tremendous of money, but also exposed consumers to a false sense of security that might have exacerbated health risks.

Misaligned economic incentives may also result in issues further down the road, as technology shifts metrics of job performance away from those that reflect real security to another, sometimes insidious, proxy measurement. An example of this from predictive policing's past is the CompStat system, which was first deployed in New York City in the mid-1990s. The system boasted a statistics-driven approach to crime mapping, but it ultimately resulted in a disproportionate allocation of police in minority neighborhoods, where police "[ratcheted] up the numbers" of tickets and arrests to boost their personal job performance figures and to give the appearance that the system had been a worthwhile investment.

Economic incentives and targets play a pronounced role in securitization across China. This is evidenced in Xinjiang, where domestic FRT companies have vied for over USD 1 billion in government contracts.[79] It is also the case in developing Smart Cities, which aim to utilize robust digital infrastructure in the fields of public security, transport, and medicine.[80] As such, from the outset, the task of decoupling malign surveillance from security or growth would appear to present a greater challenge in China.

Both the United States and China must also weigh the "meta-level" issues facing police use of FRT. In the early 2000s, while predictive policing was in its infancy, criminologists forewarned the shortcomings of advanced video surveillance technologies. Rather than "just another tool" to help police officers conduct their work more efficiently, FRT, among other technologies, would transform the role of police officers: it requires them to act on *risk factors that they themselves define*, rather than prosecute crimes or misdemeanors ascribed by law.[81] Furthermore, when mistakes are made, such as a person being misidentified and unduly arrested, it is attributed to being a flaw of the algorithm, not a liability of any person or institution. And finally, and perhaps most perilous of all, is a risk that the algorithms that fuel predictive policing contain—and thus amplify—preexisting biases.

With respect to FRT, we can observe how preexisting biases have manifested in the real world. In some Chinese provinces, for example, FRT is used to detect and label ethnic minorities to surveil them more closely. In the United States, police agencies have deployed FRT systems before

demonstrating that they perform fairly across race and ethnicity, even though every major FRT developer showed deficient performance at identifying darker-skinned faces. In both contexts, we see technology falling short of the goal of enhancing security by causing undue arrest and harm to innocent people. To prevent these sorts of outcomes in the future, there is a need for broader dialogue between policymakers and multi-domain experts from humanities and social sciences to weigh in on the technology's implications.

What we can observe at this time is that the United States and China are unlikely to reach any semblance of high-level goal alignment in the near term, as that requires a degree of multilevel value alignment that at present does not exist. The two countries' governments, institutions, and general publics have starkly different attitudes toward FRT and predictive policing. Current events seem to be pushing them further apart—the United States is, at the moment, reevaluating the role of the police force, while China's relatively effective domestic response to the novel coronavirus outbreak has bolstered support for surveillance technologies. Relative to other issues covered in this series (such as principle alignment, deepfakes, and drug modeling), substantial barriers need to be overcome to reach bilateral cooperation on this issue. Thus, FRT could be considered a **"Red Light"** issue in the Asia Society's Green-Yellow-Red Framework.

Although tensions are high between the countries, constructive confidence-building measures still exist and are worth pursuing. In fact, FRT would be a positive outlet for AI researchers to apply the emerging mantra of "alignment beyond principles." One such pursuit may be for US and Chinese think tanks to collaborate on a taxonomy of FRT applications, and evaluate each use case with respect to some mutually agreed-upon framework, such as the G20's principles towards "Human-Centered Artificial Intelligence." Stemming from this preliminary work, this sphere of research would stand to benefit from a document akin to Electronic Frontier Foundation's "International Principles on the Application of Human Rights to Communications Surveillance" [82] —cited by the UN Office of the High Commissioner for Human Rights (UNHCR)[83]—that outlines the necessity and proportionality of FRT applications or applications of biometric surveillance technologies as a whole.

The most instrumental work will likely come about through Track 1.5, 2 and 3 diplomacy. Engagement at this level may require a degree of political maneuvering, not to mention cultural humility. In spite of these challenges, in the long term, it will be important for dialogues to expand further into multi-stakeholder arrangements, to incorporate more the voices of those representing the geographies where this technology is securing a foothold. Furthermore, consequential research

and decision making should not be left to a charmed circle of technical experts. Instead, they should involve experts in associated fields, including law, criminology, sociology, intersectionality, and ethnography. This is not only the case for FRT but for all matters pertaining to surveillance technologies and human rights.

Researchers and policymakers should make haste to establish and nurture these channels for technological diplomacy. Unfortunately, an accelerated decline of higher educational exchange, technological decoupling, and the balkanization of critical internet infrastructure (i.e. the US's Clean Network and China's Global Data-Security Rules) portend a lower-bandwidth exchange of ideas in the near term.

In addition to dwindling capacities for dialogue, there are empirical reasons to believe that collaborative work is urgent. Studies on public attitudes toward biometric surveillance have shown that people become more accepting of the technology the more they interact with it in day-to-day life.[84] This may result in people becoming complacent with FRT through extended exposure of relatively innocuous applications (face ID, filters on social media apps, mobile banking access, etc.) without appropriate scrutiny of its implications across applications or populations in the hands of government entities. Furthermore, over time, public security entities will become less likely to stifle their use of FRT as they become more financially invested in the infrastructure and more adjusted to using it. Lest we enable a world with restricted privacy in public spaces, we should deliberate, now, whether or not that is the future that we want.

CONCLUSION

The use of FRT by public security entities is at inflection points in both the United States and China. In the United States, the near-term trajectory seems to be highly dependent on the outcome of the 2020 presidential election. With a change of administration, we may see public security entities follow the Democratic Party's pressure for stronger guardrails on FRT and surveillance technologies. With a Republican incumbency, we may expect to see the government double-down—to a myopic degree—on "law and order" messaging. Meanwhile, in China, we can expect the use of FRT to swell, especially as the COVID-19 pandemic persists, in line with support of public health surveillance. As Yuval Noah Harari has aptly commented, referring to the recent surge of biometric surveillance, "temporary measures have a nasty habit of outlasting emergencies, especially as there is always a new emergency lurking on the horizon."[85]

Though the US in China may have little in common with respect to FRT presently, they are confronting similar governance challenges, including data privacy, misaligned economic incentives, and the "meta-level" hazards of predictive policing. What is needed at the present time is a common assessment of the ethics and legality of all FRT applications, among those of other biometric surveillance technologies. This report has demonstrated some of the hazards that arise when such technology is in the hands of public security entities, but indeed, risks run the gamut of use cases and end users.

Collaboration towards this end is essential for preserving privacy and the freedom of movement, among other universal human rights. In spite of rising communication barriers, this is an urgent and tractable issue for which AI researchers and ethicists should seek to build upon common principle frameworks, pursue avenues of dialogue, and explore unconventional forms of diplomacy and governance.

KEY TAKEAWAYS

- **The United States and China are on divergent trajectories with respect to their use of facial recognition technology (FRT).** In spite of some vocal resistance in specific circumstances, FRT use by security entities is overall supported by the government, institutions, and general public in China, and the pandemic reinforced support of surveillance technology. Meanwhile, in the US, FRT and predictive policing are facing a wide-spread reckoning, and its development or curtailment likely rests on the outcome of the 2020 Presidential election.

- **Decisions made by both the United States and China in the near term will dictate global deployment in the long term.** The two countries dominate the global market for FRT. And while the US may soon impose export controls on FRT on "human rights" grounds, it may only irreversibly disrupt the market as a whole if the United States were able to persuade allies and "global swing states" to do so as well.

- **Despite being on divergent trajectories, both countries are confronting similar FRT governance challenges, which present opportunities for alignment.** Challenges include those of data privacy, misaligned economic incentives, and the "meta-level" hazards of policing.

- **Bilateral and multilateral dialogue is a priority to align on FRT applications, not just principles.** In spite of growing tensions and diminishing avenues for dialogue between the United States and China, alignment should be sought on applications of FRT and other surveillance technologies. Representative voices of those from regions where the technology is securing a foothold, and those from associated academic fields, deserve a seat at the table.

ENDNOTES

[1] "Commerce Department to Add Nine Chinese Entities Related to Human Rights Abuses in the Xinjiang Uighur Autonomous Region to the Entity List," U.S. Department of Commerce, accessed September 8, 2020, https://www.commerce.gov/news/press-releases/2020/05/commerce-department-add-nine-chinese-entities-related-human-rights.
[2] Larry Magid, "IBM, Microsoft And Amazon Not Letting Police Use Their FRT," Forbes, accessed September 8, 2020, https://www.forbes.com/sites/larrymagid/2020/06/12/ibm-microsoft-and-amazon-not-letting-police-use-their-facial-recognition-technology/.
[3] Steven Fieldstein, "The Global Expansion of AI Surveillance," September 2019, https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf.
[4] Dave Gershgorn, "Facial Recognition Companies See the Coronavirus as a Business Opportunity," Medium, March 19, 2020, https://onezero.medium.com/facial-recognition-companies-see-the-coronavirus-as-a-business-opportunity-6c9b99d60649.
[5] James Vincent, "Face Masks Are Breaking Facial Recognition Algorithms, Says New Government Study," The Verge, July 28, 2020, https://www.theverge.com/2020/7/28/21344751/facial-recognition-face-masks-accuracy-nist-study; ipvideomarket, "Beware Rigged China Fever Cameras," IPVM, 18:43 400AD, https://ipvm.com/reports/china-fever-comp.
[6] Fieldstein, "The Global Expansion of AI Surveillance."
[7] Fieldstein.
[8] Fred Wilson and Jessie Lee, "Intelligence-Led Policing: The New Intelligence Architecture," n.d., 52; Jerry Ratcliffe, "Intelligence-Led Policing," n.d., 280.
[9] "America Under Watch - Real-Time Facial Recognition in America," America Under Watch - Real-Time Facial Recognition in America, accessed September 22, 2020, https://www.americaunderwatch.com.
[10] "FACE Recognition Technology: FBI Should Better Ensure Privacy and Accuracy [Reissued on August 3, 2016]" (U. S. Government Accountability Office, August 3, 2016), https://www.gao.gov/products/GAO-16-267.
[11] U. S. Government Accountability Office, "Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses," no. GAO-20-522 (August 11, 2020), https://www.gao.gov/products/GAO-20-522.
[12] "The Perpetual Line-Up," Perpetual Line Up, https://www.perpetuallineup.org/.
[13] "The Perpetual Line-Up," Perpetual Line Up, https://www.perpetuallineup.org/.
[14] S. Z. Li and Anil K. Jain, eds., *Handbook of Face Recognition*, 2nd ed (London : New York: Springer, 2011).
[15] Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," *The New York Times*, January 18, 2020, sec. Technology, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[16] Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," *The New York Times*, January 18, 2020, sec. Technology, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.
[17] Amanda Bronstad | September 10, and 2020 at 03:36 PM, "NY-Based Facial Recognition Tech Company Wrangles With Judges in Two States Over Privacy Class Actions," New York Law Journal, https://www.law.com/newyorklawjournal/2020/09/10/ny-based-facial-recognition-tech-company-wrangles-with-judges-in-two-states-over-privacy-class-actions/.
[18] "Clearview AI Landed a New Facial Recognition Contract with ICE | TechCrunch," https://techcrunch.com/2020/08/14/clearview-ai-ice-hsi-contract-2020/.
[19] "IBM CEO's Letter to Congress on Racial Justice Reform," THINKPolicy Blog, June 8, 2020, https://www.ibm.com/blogs/policy/facial-recognition-sunset-racial-justice-reforms/.
[20] "We Are Implementing a One-Year Moratorium on Police Use of Rekognition," https://blog.aboutamazon.com/policy/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition.
[21] Jay Greene, "Microsoft Won't Sell Police Its Facial-Recognition Technology, Following Similar Moves by Amazon and IBM," *Washington Post*, https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/.
[22] Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," n.d., 15.
[23] Kashmir Hill, "Wrongfully Accused by an Algorithm," *The New York Times*, June 24, 2020, sec. Technology, https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.
[24] "'The Computer Got It Wrong': How Facial Recognition Led To False Arrest Of Black Man," Nevada Public Radio, https://knpr.org/npr/2020-06/computer-got-it-wrong-how-facial-recognition-led-false-arrest-black-man.
[25] "California to Ban Facial Recognition in Police Body Cameras - The Washington Post," https://www.washingtonpost.com/technology/2019/09/12/california-could-become-largest-state-ban-facial-recognition-body-cameras/.
[26] "Massachusetts Could Become First State to Ban Facial Recognition," https://news.bloomberglaw.com/tech-and-telecom-law/facial-recognition-ban-in-massachusetts-set-for-senate-approval.
[27] Electronic Privacy Information Center, "EPIC - State Facial Recognition Policy," https://epic.org/state-policy/facialrecognition/.
[28] Roy Blunt, "S.847 — 116th Congress (2019–2020): Commercial Facial Recognition Privacy Act of 2019," webpage, March 14, 2019, 2019/2020, https://www.congress.gov/bill/116th-congress/senate-bill/847; Jeff Merkley, "Text — S.4400 – 116th Congress (2019-2020): National Biometric Information Privacy Act of 2020," legislation, August 3, 2020, 2019/2020, https://www.congress.gov/bill/116th-congress/senate-bill/4400/text; Edward J. Markey, "S.4084 — 116th Congress (2019–2020): Facial Recognition and Biometric Technology Moratorium Act of 2020," webpage, June 25, 2020, 2019/2020, https://www.congress.gov/bill/116th-congress/senate-bill/4084; Pramila Jayapal, "H.R.7356 — 116th Congress (2019–2020): Facial Recognition and

Biometric Technology Moratorium Act of 2020," webpage, June 25, 2020, 2019/2020, https://www.congress.gov/bill/116th-congress/house-bill/7356.

[29] U. S. Government Accountability Office, "Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses," no. GAO-20-522 (August 11, 2020), https://www.gao.gov/products/GAO-20-522.

[30] "Advanced Surveillance Systems and Other Items of Human Rights Concern," Federal Register, July 17, 2020, https://www.federalregister.gov/documents/2020/07/17/2020-15416/advanced-surveillance-systems-and-other-items-of-human-rights-concern.

[31] "Chinese City Uses Facial Recognition to Tackle Jaywalking - China - Chinadaily.Com.Cn," https://www.chinadaily.com.cn/china/2017-09/25/content_32466168.htm.

[32] Edward Schwarck, "Intelligence and Informatization: The Rise of the Ministry of Public Security in Intelligence Work in China," *The China Journal* 80 (July 2018): 1–23, https://doi.org/10.1086/697089.

[33] Edward Schwarck, "Intelligence and Informatization: The Rise of the Ministry of Public Security in Intelligence Work in China," *The China Journal* 80 (July 2018): 1–23, https://doi.org/10.1086/697089.

[34] "Beijing's Guardian Angels? - Global Times," http://www.globaltimes.cn/content/737491.shtml.

[35] Xiao Qiang, "The Road to Digital Unfreedom: President Xi's Surveillance State," *Journal of Democracy* 30, no. 1 (January 9, 2019): 53–67, https://doi.org/10.1353/jod.2019.0004.

[36] "China to Have 626 Million Surveillance Cameras within 3 Years · TechNode," TechNode, November 22, 2017, https://technode.com/2017/11/22/china-to-have-626-million-surveillance-cameras-within-3-years/.

[37] "（受权发布）中共中央 国务院关于实施乡村振兴战略的意见-新华网," accessed April 23, 2020, http://www.xinhuanet.com/politics/2018-02/04/c_1122366449.htm.

[38] Elsa B. Kania,"Made in China 2025, Explained," https://thediplomat.com/2019/02/made-in-china-2025-explained/.

[39] "Full Translation: China's 'New Generation Artificial Intelligence Development Plan' (2017)," New America, accessed September 27, 2020, http://newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/.

[40] Yuan Yang and Nian Liu, "Beijing Orders State Offices to Replace Foreign PCs and Software," December 8, 2019, https://www.ft.com/content/b55fc6ee-1787-11ea-8d73-6303645ac406.

[41] Madhumita Murgia, Yuan Yang, and Anna Gross, "Chinese Tech Groups Shaping UN Facial Recognition Standards," December 1, 2019, https://www.ft.com/content/c3555a3c-0d3e-11ea-b2d6-9bf4d1957a67.

[42] Madhumita Murgia, Yuan Yang, and Anna Gross, "Chinese Tech Groups Shaping UN Facial Recognition Standards," December 1, 2019, https://www.ft.com/content/c3555a3c-0d3e-11ea-b2d6-9bf4d1957a67.

[43] "Chinese Interests Take a Big Seat at the AI Governance Table," New America, accessed March 13, 2020, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinese-interests-take-big-seat-ai-governance-table/.
[44] Billy Ehrenberg-Shannon et al., "Ten Charts That Tell the Story of 2019," December 29, 2019, https://www.ft.com/content/62fbf660-2651-11ea-9a4f-963f0ec7e134.
[45] "The State of U.S. Science and Engineering 2020 | NSF - National Science Foundation," accessed April 26, 2020, https://ncses.nsf.gov/pubs/nsb20201.
[46] "Exclusive: China's SenseTime Expects $750 Mln 2019 Revenue despite U.S. Ban - Sources," *Reuters*, December 6, 2019, https://www.reuters.com/article/us-china-sensetime-exclusive-idUSKBN1YA1IV.
[47] "Dahua Releases 2019 Annual Report," *ISJ International Security Journal* (blog), April 6, 2020, https://internationalsecurityjournal.com/dahua-technology-releases-annual-report-for-2019/.
[48] "Hikvision 2019 Annual Report," *Annual Report*, 2019, 312.
[49] May 15 and 2020 | Chris Burt, "CloudWalk Raises $250M and Plans IPO as Biometrics Firms Flourish in China during Pandemic Response," Biometric Update, May 15, 2020, https://www.biometricupdate.com/202005/cloudwalk-raises-250m-and-plans-ipo-as-biometrics-firms-flourish-in-china-during-pandemic-response.
[50] "In Your Face: China's All-Seeing State," BBC News, accessed May 10, 2020, https://www.bbc.com/news/av/world-asia-china-42248056/in-your-face-china-s-all-seeing-state.
[51] Emina Popović, "Lobbying Practices of Citizens' Groups in China," *SAGE Open*, n.d., 9.
[52] Popović.
[53] Yi Zeng et al., "Responsible Facial Recognition and Beyond," *ArXiv:1909.12935 [Cs]*, September 19, 2019, http://arxiv.org/abs/1909.12935.
[54] Yi Zeng et al., "Facial Recognition and Public Heath" (Research Center for AI Ethics and Safety, Beijing Academy of Artificial Intelligence, May 4, 2020), https://attachment.baai.ac.cn/share/aies/facial-recognition-and-public-health-en-2020-05-17.pdf.
[55] 商汤君, "商汤当选国家人脸识别工作组组长单位，促进 AI 安全应用," 微信公众平台, accessed March 13, 2020, http://mp.weixin.qq.com/s?__biz=MzIwNTcyNzYwMA==&mid=2247490663&idx=1&sn=49a850be5b5d5b168af6171c464f7eb6&chksm=972d2e78a05aa76eaea678312bb59b9792bb1c4a49942aaffa9a231053ce44b00dad85d813d1#rd.
[56] 旷视 MEGVII, "旷视成立 AI 治理研究院 回溯全球十大 AI 治理事件," WeChat Official Accounts Platform, accessed April 21, 2020, http://mp.weixin.qq.com/s?__biz=MzA3NjIzMTk0NA==&mid=2651650765&idx=1&sn=edf2a65e279648e320d86c7f4b929b41&chksm=849c3eaab3ebb7bc9b2a274b6cc57de7de8af8f4939990e95ff938b43189cbb3e48d5b333401#rd.
[57] "关注 AI 治理 | 十大热点事件大众观," WeChat Official Accounts Platform, http://mp.weixin.qq.com/s?__biz=MzA3NjIzMTk0NA==&mid=2651650806&idx=1&sn=183d4c29aaad2689a411f3fbd132a695&chksm=849c3e91b3ebb787ee399bb3fa81e1c812518e940a5886c7115bfcbbccb3a44f147cfaf7ac86#rd.

[58] "中国纪检监察报 - '花式'逃亡终难逃法网," http://www.jjjcb.cn/content/2018-09/30/content_68514.htm; "'雪亮工程'保平安--法治--人民网," November 18, 2018, https://web.archive.org/web/20181118195610/http://legal.people.com.cn/n1/2017/0614/c42510-29337488.html.

[59] Genia Kostka, Léa Steinacker, and Miriam Meckel, "Between Privacy and Convenience: Facial Recognition Technology in the Eyes of Citizens in China, Germany, the UK and the US," *SSRN Electronic Journal*, 2020, https://doi.org/10.2139/ssrn.3518857.

[60] Zeng et al., "Facial Recognition and Public Health."

[61] "中国纪检监察报 - '花式'逃亡终难逃法网."

[62] "'雪亮工程'保平安--法治--人民网."

[63] "Chinese Man Sues Wildlife Park over Use of Facial Recognition System," South China Morning Post, November 3, 2019, https://www.scmp.com/news/china/society/article/3036126/chinese-professor-sues-wildlife-park-after-it-introduces-facial.

[64] 江巍, "Park Alters Entry Rules Following Facial Recognition Tech Lawsuit - Chinadaily.Com.Cn," https://www.chinadaily.com.cn/a/201911/07/WS5dc38381a310cf3e35575f3a.html.

[65] "清华教授劳东燕：人脸识别技术的隐忧," WeChat Official Accounts Platform, accessed April 9, 2020, http://mp.weixin.qq.com/s?__biz=MzU2MTYyMjA2Nw==&mid=2247493201&idx=2&sn=3a5916ad3ca2ea7d6a405877ef7d87c6&chksm=fc775b0dcb00d21b8a82afe4a6a5cdc6d8e93b4252c828235d5916ed23306d2997eefdd774b3#rd.

[66] 胡泳, "胡泳 | 危机时刻的公共利益与个人隐私（下）," WeChat Official Accounts Platform, accessed April 9, 2020, http://mp.weixin.qq.com/s?__biz=MjM5MzA1MTQ4MQ==&mid=2650145467&idx=1&sn=ac33a87b1efc876a92f2dbd85f7ebaa7&chksm=be9e448d89e9cd9b8fbbcd713dcf3e526c99b8ce886980acfab7f6b3493075348263b5f70f89#rd.

[67] Qiuqing Tai, "China's Media Censorship: A Dynamic and Diversified Regime," *Journal of East Asian Studies* 14, no. 2 (August 2014): 185–210, https://doi.org/10.1017/S1598240800008900.

[68] Sébastien Krier, "Facing Affect Recognition" (Asia Society, September 18, 2020), https://asiasociety.org/sites/default/files/inline-files/Affect%20Final.pdf.

[69] Jessica Cussins Newman, "AI PRINCIPLES IN CONTEXT: Tensions and Opportunities for the United States and China" (Asia Society, n.d.), https://asiasociety.org/sites/default/files/inline-files/Cussins_Principles_Final.pdf.

[70] "The AI Powered State: China's Approach to Public Sector Innovation" (Nesta, n.d.), https://media.nesta.org.uk/documents/Nesta_TheAIPoweredState_2020.pdf.

[71] Yi Zeng et al., "Facial Recognition and Public Health" (Research Center for AI Ethics and Safety, Beijing Academy of Artificial Intelligence, May 4, 2020), https://attachment.baai.ac.cn/share/aies/facial-recognition-and-public-health-en-2020-05-17.pdf.

[72] 赵汀阳, "赵汀阳 | 人工智能'革命'的'近忧'和'远虑'——一种伦理学和存在论的分析," WeChat Official Accounts Platform, http://mp.weixin.qq.com/s?__biz=MzAwNDYzNDI2Ng==&mid=2651908570&idx=1&sn=1af4

39bb4f763581dbafbc9f999e12d1&chksm=80ccaa2fb7bb23393ac527c1f25576c8b050df112147028824eb408b537b167d9b9d40519f51#rd.

[73] Nick Bostrom, "The Vulnerable World Hypothesis," *Global Policy* 10, no. 4 (November 2019): 455–76, https://doi.org/10.1111/1758-5899.12718.

[74] Liza Lin, "Thousands of Chinese Students' Data Exposed on Internet," *Wall Street Journal*, January 17, 2020, sec. World, https://www.wsj.com/articles/thousands-of-chinese-students-data-exposed-on-internet-11579283410.

[75] Kate O'Flaherty, "Clearview AI, The Company Whose Database Has Amassed 3 Billion Photos, Hacked," Forbes, accessed September 22, 2020, https://www.forbes.com/sites/kateoflahertyuk/2020/02/26/clearview-ai-the-company-whose-database-has-amassed-3-billion-photos-hacked/.

[76] "Translation: China's Personal Information Security Specification," New America, 2020, http://newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-personal-information-security-specification/.

[77] "Coming into Focus: China's Facial Recognition Regulations," https://www.csis.org/blogs/trustee-china-hand/coming-focus-chinas-facial-recognition-regulations.

[78] ipvideomarket, "Beware Rigged China Fever Cameras," IPVM, 18:43 400AD, https://ipvm.com/reports/china-fever-comp.

[79] ipvideomarket, "Dahua and Hikvision Win Over $1 Billion In Government-Backed Projects In Xinjiang," IPVM, 53:29 400AD, https://ipvm.com/reports/xinjiang-dahua-hikvision.

[80] "Shenzhen's 'Maslow Model' for Smart Cities," *GovInsider* (blog), September 6, 2019, https://govinsider.asia/connected-gov/shenzhens-maslow-model-for-smart-cities/.

[81] Stéphane Leman-Langlois, "The Myopic Panopticon: The Social Consequences of Policing Through the Lens," *Policing and Society* 13, no. 1 (January 2002): 43–58, https://doi.org/10.1080/1043946022000005617.

[82] "NECESSARY & PROPORTIONATE: INTERNATIONAL PRINCIPLES ON THE APPLICATION OF HUMAN RIGHTS TO COMMUNICATIONS SURVEILLANCE," https://necessaryandproportionate.org/files/en_principles_2014.pdf.

[83] "The Right to Privacy in the Digital Age :," June 30, 2014, http://digitallibrary.un.org/record/777869.

[84] Oliver Buckley and Jason R.C. Nurse, "The Language of Biometrics: Analysing Public Perceptions," *Journal of Information Security and Applications* 47 (August 2019): 112–19, https://doi.org/10.1016/j.jisa.2019.05.001.

[85] Yuval Noah Harari, "Yuval Noah Harari: The World after Coronavirus | Free to Read," March 20, 2020, https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75.

Author's Note: I would thank my friends and colleagues, in the US, China, and elsewhere, that provided feedback on this piece. I would also like to express my sincere gratitude to the academics, journalists, and activists that contribute their energy, intellect, and empathy to this field.

Series Edited and Overseen by Heather Evans and Benjamin Cedric Larsen
Cover Artwork Designed by Kisara Moore and Anya Lassila
Traffic Light Design by Anya Lassila

Thank you to the Asia Society Northern California Team for supporting this publication.