CHERI
Swiss Existential
Risk Initiative

September 2021

The Implications of EU and Chinese Regulation on AI-powered Surveillance

A brief overview

Chiara Gerosa

Table of Contents

Summary **3**

The Risks of AI Surveillance **4**

Advancing global authoritarianism 4

Authoritarianism and existential risk 5

Comparing Regulation **6**

Why compare China and the EU? 6

Comparing Chinese and EU regulation 7

AI ethics 8

Data and privacy protections 11

How Meaningful are Existing Regulatory Frameworks? **12**

AI surveillance for political control 13

Global AI surveillance technology transfers 13

International digital norm-setting 14

A weak AI Act? 14

Conclusion **15**

Acknowledgements **18**

Bibliography 19

Summary

Recent advances in artificial intelligence (AI) have created strong incentives for countries to develop governance strategies to maximize the potential benefits of AI technologies, while also mitigating their risks. At present, 60 countries have released AI policy documents.[1] Yet given its increasing development and proliferation, especially for public security purposes, issues concerning AI-powered surveillance are fairly neglected in academic literature. Think tank reports that do tackle AI surveillance tend to be extremely US-focused and center on the geopolitics of China's creeping dominance of global AI surveillance technology.[2] Some comparative literature exists on AI regulation,[3] but many articles focus on single states and there is little on the implications of AI on surveillance.

This report acts as a brief introduction for those interested in pursuing further research on AI surveillance. Regulations provide the framework to harness technological potential and enact (potentially) digitally repressive policies. The goal of this report is, therefore, to provide a broad understanding of the regulatory frameworks that shape the future trajectory AI surveillance tools; specifically, how EU and Chinese regulations may shape the global development and implementation of AI surveillance technologies.

To demonstrate the role of EU and Chinese regulations on AI surveillance applications, the report is structured as follows. The first section outlines the risks associated with AI surveillance. The following section explains the rationale behind analyzing EU and Chinese regulation, before proceeding to compare key aspects of EU and Chinese regulation. Regulations that exclusively govern AI surveillance do not currently exist, therefore, the report focuses mainly on data and privacy regulation. The final section assesses the real-life implications of the discussed regulations on the development and application of AI surveillance technologies. The conclusion summarizes the main points of the report and suggests avenues for further exploration.

The research for this report was guided by the following questions:

1. To what extent are China and the EU setting regulatory norms on the governance of AI surveillance systems?
2. What effects might Chinese and EU regulation have on the application of AI surveillance systems in the long-term?

The key findings of this report are as follows:

- Both the EU and China focus on economic growth in their AI regulations, but there is a stark difference when it comes to utilizing AI surveillance for matters of national security.
- There are large differences between *de jure* and *de facto* regulation in China, meaning that privacy protections are unlikely to apply to state surveillance.

[1] EC/OECD, 'Database of National AI Policies'.
[2] Sahin, 'The West, China, and AI Surveillance'.
[3] Roberts et al., 'The Chinese Approach to Artificial Intelligence'.

- The EU's recent AI regulation may provide too large of a scope for it to be effective at restricting the development of "high-risk" AI surveillance applications.
- The value in comparing the EU and China actors stems from their norm-setting and regulatory power.
    - We can already observe China's AI surveillance technology being exported around the world, which may have implications for how receiving countries carry out domestic surveillance practices.

The Risks of AI Surveillance

1. Advancing global authoritarianism

By allowing governments to monitor, understand, and control their citizens more closely, AI offers authoritarian countries a plausible alternative to liberal democracy, potentially sparking renewed international competition between political systems.[4] This is because AI enables more pervasive forms of surveillance by improving data processing speed, pattern recognition and prediction. The predictive power of AI allows authoritarian states to pre-empt opposition; deter specific activities or beliefs that challenge the state; and neutralize potential dissidents through targeted detentions and preventive arrests.[5] This, in turn, also fundamentally transforms citizens' behaviour and incentives.[6] An expectation of state omnipresence through surveillance could lead to citizens pre-emptively denounce other citizens out of fear.

During the COVID-19 pandemic, advanced AI surveillance systems allowed the Chinese government to provide more efficient public services: many Chinese surveillance technologies were legitimized for public health purposes, including tracking apps; surveillance by drones; cameras inside and outside houses; remote temperature scanning; and upgraded facial recognition to identify mask wearers.[7] This could, ultimately, enhance perceptions of regime performance.[8] Indeed, there was little domestic public resistance in China about technology-related privacy risks during the pandemic.[9]

China's surveillance model may gain even more legitimacy as an alternative to democracy and a vital tool beyond the pandemic. A growing number of states are deploying Chinese AI surveillance tools for public surveillance purposes. Worldwide, at least 80 countries have adopted Chinese surveillance technology platforms.[10] The surveillance platforms being exported from China integrate multiple government databases and provide analytic capabilities that can

[4] Wright.

[5] Feldstein, *The Rise of Digital Repression*.

[6] Feldstein.

[7] Peterson, 'Designing Alternatives to China's Repressive Surveillance State'.

[8] Hoffman, 'Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion'.

[9] Liu and Zhao, 'Privacy lost: Appropriating surveillance technology in China's fight against COVID-19'.

[10] Feldstein, 'The Global Expansion of AI Surveillance'.

support multiple command and control centers.[11] Such surveillance is not inherently controversial - some applications of AI surveillance are positive, used for spotting wildfires or managing traffic, for example. However, think tanks, scholars and journalists assert that China is not only exporting technology to enhance the public safety of these nations, but is also advancing censorship, disinformation and public opinion-shaping tools that support regimes with poor human rights records or illiberal forms of governance.[12]

Though the US also exports AI surveillance technology, many countries solely utilize Chinese tech. For example, Chinese telecommunications firm Huawei dominates African markets, where it has sold security tools that governments use for digital surveillance and censorship.[13] If AI-powered surveillance technologies are proven effective for social control, they may have the potential to become a model for authoritarian governments, significantly impacting power and endurance of non-democratic regimes all over the world.[14]

2. Authoritarianism and existential risk

If AI becomes increasingly more powerful and contributes to the proliferation of authoritarian governance and the decline of democratic institutions, the world could reach a point where authoritarian regimes vastly outnumber democratic ones. Through powerful surveillance and enforcement, it may become impossible for a handful of dissidents to find each other and stage mass protests or uprisings.

Such a descent into a totalitarian future would be an existential risk, that is, “a risk that threatens the destruction of humanity’s long-term potential”.[15] Strict totalitarian rule with pervasive surveillance, propaganda, limited freedom of thought and expression controlled through fear and violence would ensure that only a narrow range of unpleasant futures would be available to humanity. If everyone in the world lived under such rule, the regime is protected from both internal and external threats and can be maintained indefinitely.[16]

[11] Peterson, ‘Designing Alternatives to China’s Repressive Surveillance State’.
[12] Hoffman, ‘Social Credit: Technology-enhanced authoritarian control with global consequences’; Hoffman, ‘Engineering global consent: the Chinese Communist Party’s data-driven power expansion’; Lilkov, ‘Made in China’.
[13] Parkinson, Bariyo, and Chin, ‘Huawei Technicians Helped African Governments Spy on Political Opponents’.
[14] Wright, ‘How Artificial Intelligence Will Reshape the Global Order’.
[15] Ord, *The Precipice*. p.37
[16] Ord.

Comparing Regulation

1. Why compare China and the EU?

Sources of Chinese and EU regulatory power

Though China is a *country* while the EU is an *economic and political union*, the value in comparing the two actors stems from their regulatory power. While the EU is already considered to be a global regulatory power, exercising both soft[17] and market[18] power to stimulate regulatory changes abroad, China's regulatory power emanates from its role as a leading tech developer and innovator.

There is broad consensus that the EU is a trade, regulation and standard-setting superpower. The EU's international regulatory clout can be attributed to its market size and regulatory competence.[19] Generally, EU unilateral regulatory standards act as "norm catalysts", setting a baseline that creates incentives and affects the costs and benefits of third countries and international policies.[20] This is known as the *Brussels Effect.* Non-compliance with EU regulation would mean losing access to Europe's $20 trillion market.[21]

The 2018 General Data Protection Regulation (GDPR), for instance, has taken the lead in protecting privacy rights. It protects the processing of personal data of individuals within the EU and the European Economic Area (EEA), as well as the transfer of personal data outside the EU and EEA.[22] The GDPR has acted as a blueprint for other data protection regulation abroad - Brazil's *Lei Geral de Proteçao de Dados* (LGPD or General Data Protection Law) was modeled directly after GDPR and is nearly identical in terms of scope and applicability.[23]

In April 2021, the EU initiated the world's first attempt at horizontal regulation of AI systems through the European Commission's proposed Regulation on Artificial Intelligence, or the 'AI Act'.[24] Like the GDPR, the AI Act is extraterritorial in scope: the planned regulation applies not only to EU-based companies and individuals but also intends to pose legal obligations on foreign companies selling AI products or services in the EU.[25] Though the AI Act has yet to be finalized, if the EU manages to become the first actor to create an appropriate regulatory

[17] Soft power is the ability of a country to do what it wants without using force or coercion. See Ikenberry, 'Soft Power'.

[18] Market power is the ability to generate prices that diverge from what would result in a fully clearing market. See Gent and Crescenzi, 'Market Power, War, and Strategic Delay'.

[19] Bradford, 'The Brussels Effect'.

[20] Hadjiyianni, 'The European Union as a Global Regulatory Power'.

[21] Raines, 'Raise the Bar by Leveraging the EU's Regulatory Power'.

[22] Asghar et al., 'Visual Surveillance Within the EU General Data Protection Regulation'.

[23] 'How GDPR Is Shaping Global Data Protection'.

[24] Veale and Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act'.

[25] Lomas, 'Europe Lays out Plan for Risk-Based AI Rules to Boost Trust and Uptake'.

framework on AI, the Act could become the de facto regulation for how AI technology is governed globally, potentially triggering a similar effect to that of the GDPR.[26]

China's regulatory power, on the other hand, is linked to its role as a tech developer and exporter of technologies that provide useful services.[27] Officials from the Cyber Administration of China have written about the need to develop controls so that "the party's ideas always become the strongest voice in cyberspace" - this includes enhancing the "global influence of [...] companies like Alibaba, Tencent, Baidu [and] Huawei".[28] Today, China is a global leader in the development of AI technologies and China's many large technology companies are major global suppliers of AI and big-data surveillance technologies.[29]

For example, China launched one of its first AI projects in Africa in March 2018 when Chinese startup CloudWalk began to supply Zimbabwe with facial recognition technology, a means for Zimbabwe to manage its national surveillance program.[30] Assisted by a $240 million loan from China, Zimbabwe has installed a wide network of cameras and response centers.[31] Over the past several years, Ecuador has also become a heavy user of Chinese AI surveillance technology. South Africa, Bolivia, and Venezuela have also imported AI surveillance technologies from China, to varying degrees.[32]

For many, the proliferation of Chinese AI surveillance technology abroad equates to a spread of Chinese *models* of digital authoritarianism.[33] If we assume this is true, we could conclude that governments that employ Chinese AI surveillance technology may want to also adopt Chinese regulatory frameworks because of overlapping ethical stances on privacy and government control, as well as government interest to retain social order and stability. As with the GDPR, foreign companies conducting business in countries that choose to adopt Chinese regulatory frameworks would have to adhere to local regulations as well, thus would also follow Chinese regulations.

2. Comparing Chinese and EU regulation

Regulations that exclusively govern AI surveillance do not currently exist. Regulatory or legal literature relevant to AI focuses mainly on data and privacy regulation.[34] Thus, to understand how AI surveillance technology may be developed and implemented in the future, this section

[26] Hovsepyan, 'Regulating AI'.
[27] Hoffman, 'Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion'.
[28] Cave et al., 'Mapping China's Tech Giants'.
[29] Feldstein, *The Rise of Digital Repression*.
[30] Chutel, 'China Is Exporting Facial Recognition Software to Africa, Expanding Its Vast Database'.
[31] Romaniuk and Burgers, 'How China's AI Technology Exports Are Seeding Surveillance Societies Globally'.
[32] Romaniuk and Burgers.
[33] Sahin, 'The West, China, and AI Surveillance'.
[34] See e.g. Aho and Duffield, 'Beyond Surveillance Capitalism'; Pernot-Leplay, 'China's Approach on Data Privacy Law'.

provides a rapid review of existing literature on Chinese and EU AI and privacy regulation. AI regulations provide insight to understanding the *development* of AI surveillance technologies, for example, how AI will impact existing surveillance technologies and what types of AI-powered surveillance capabilities will be allowed to develop. Privacy regulations, meanwhile, are relevant to understand how AI surveillance will be *implemented:* which protections (or lack thereof) will be put in place to manage the increasingly large amounts of data that will be collected through AI surveillance tools.

a. AI ethics

This report defines AI ethics the moral principles that underpin a country's approach to AI development. For example, most governments approach AI development with the aim of improving economic and social outcomes for its population, as well as leveraging AI to maintain external security. This is also true for the EU and China – both powers place a particular focus on economic growth in their AI visions. However, the EU follows a "human-centered approach" and is eager to promote this as a global and unique selling point; this is clearly summarized by the European Commission, who state that "any AI-generated improvements need to be based on rules that safeguard the functioning of markets and the public sector, and people's safety and fundamental rights".[35] China, on the other hand, prioritizes international competitiveness and economic development.

The EU values AI as a means for economic development and prosperity, demonstrated via the promotion of AI research and development through various investment mechanisms. The Digital Europe Programme, for example, provides funding for projects in five crucial areas: supercomputing, AI, cybersecurity, advanced digital skills and ensuring the wide use of digital technologies across the economy and society.[36] InvestEU, similarly, strengthens investments in digital infrastructures, technologies, and skills and is expected to mobilize approximately €372 billion in additional investment between 2021-27.[37]

In the EU, boundaries for what constitutes the ethically acceptable development and use of AI are defined. In April 2019, the European Commission High-Level Expert Group on Artificial Intelligence released the Ethics Guidelines for Trustworthy AI, which lists the seven principles of trustworthy AI to ensure that the application of AI is ethical and that the technology is robust and reliable. According to the guidelines, trustworthy AI has two components. First, it should respect basic human rights, regulations, and core principles and values; second, it should be technologically safe and reliable to avoid unintentional harm caused by insufficient technology.[38]

[35] 'A European Approach to Artificial Intelligence | Shaping Europe's Digital Future'.
[36] 'Digital Europe Programme'.
[37] 'What Is the InvestEU Programme?'; 'InvestEU and a Europe Fit for the Digital Age'.
[38] Murphy, 'Artificial Intelligence Security Standardization White Paper'.

Another key document is the European Commission's Regulation on Artificial Intelligence, the AI Act, proposed on 24 April 2021. The proposed AI Act states that "AI should be a tool for people and be a force for good in society with the ultimate aim of increasing human well-being".[39]

Therefore, the European approach seems to be to ensure that European values remain at the core of AI development and applications. This is done by encouraging the uptake of AI by public and private sectors to advance the economy. In parallel, the EU mitigates ethical risks and ensures the development of "human-centric, trustworthy, secure, sustainable and inclusive AI"[40] through ethics guidelines and novel regulation such as the AI Plan.

China, meanwhile, is among the forerunners in the development of AI. Since 2017, China has emphasized how imperative it believes leading the AI revolution is, overtaking the US and the EU in the amount of funding provided for AI development.[41] Since 2013, China has published several national-level policy documents reflecting its intention to develop and deploy AI in a variety of sectors.[42] Among the most advanced AI policy documents globally is the 2017 New Generation Artificial Intelligence Development Plan (AIDP).[43] The AIDP's overarching aim is to make China the world center of AI innovation by 2030 and make AI "the main driving force for China's industrial upgrading and economic transformation".[44]

To some extent, China's AI approach can also be called "human-centric", but with a much larger focus on economic development to achieve benefits for society. This is clear in the AIDP's guiding ideologies:

> *"...intelligent economy development; smart society construction; protecting national security; building of knowledge clusters, technology clusters, and industry clusters mutually integrated with talent, system, and culture, for a mutually supporting ecosystem, [...]* ***Comprehensively enhance society's productive forces, [...] and national competitiveness****, in order to provide strong support to accelerate the construction of [a] global science and technology power..."*[45]

Notwithstanding, ethical frameworks also exist. However, it is unclear to what extent they are applied in practice. In March 2019, China's Ministry of Science and Technology established The National New Generation Artificial Intelligence Governance Expert Committee. This body

[39] European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts.

[40] European Commission, ANNEXES to the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Fostering a European approach to Artificial Intelligence.

[41] Jing, 'This Chinese City Plans a US$16 Billion Fund for AI Development'.

[42] Roberts et al., 'The Chinese Approach to Artificial Intelligence'.

[43] Roberts et al., 'Governing Artificial Intelligence in China and the European Union: Comparing Aims and Promoting Ethical Outcomes'.

[44] Webster et al., 'Full Translation'.

[45] Webster et al.

released eight principles for the governance of AI: above all else, AI development should begin from enhancing the common wellbeing of humanity. Respect for human rights, privacy and fairness were also underscored.[46]

Additionally, in April 2019, China's National Artificial Intelligence Standardization General Working Group published the Artificial Intelligence Ethical Risk Analysis Report, proposing two ethical guidelines for AI. The first is the principle of human fundamental interests, which means that AI should ultimately achieve human fundamental interests.[47] The second is the principle of responsibility, which refers to the establishment of a clear responsibility system in both the development and application of AI-related technologies[48].

Therefore, China places a clearer emphasis on international competitiveness – being a global leader of AI development. Societal improvement is advanced through economic development in China, whereas in the EU, economic development is derived from inclusive AI that protects human rights. Though there are mentions of human rights in China's AI regulations, it is the CCP that decides what societal improvement is defined. The Social Credit System, for example, is an example of the government nudging individuals' behaviour to achieve outcomes that the *government* considers societally beneficial to protect social stability.[49] Figure 1 provides a summary of the main ethical principles in China and EU AI Regulations outlined in this section.

Table 1: Summary of the main ethical principles in China and EU AI Regulations

China	EU
Artificial Intelligence Ethical Risk Analysis Report (April 2019)	**Ethics Guidelines for Trustworthy AI (April 2019)**
AI should ultimately achieve the fundamental interests of humans	AI should respect basic human rights, regulations, and core principles and values
The establishment of a clear responsibility system in both the development and application of AI-related technologies	AI should be technologically safe and reliable to avoid unintentional harm caused by insufficient technology
The National New Generation Artificial Intelligence Governance Expert Committee principles for the governance of AI (March 2019)	**EU Coordinated Plan, 2021 Review**
AI should enhance the common wellbeing of humanity and respect human rights, privacy and fairness	AI should be human-centric, trustworthy, secure, sustainable and inclusive

[46] Roberts et al., 'Governing Artificial Intelligence in China and the European Union: Comparing Aims and Promoting Ethical Outcomes'.
[47] Murphy, 'Artificial Intelligence Security Standardization White Paper'.
[48] Murphy.
[49] Roberts et al., 'The Chinese Approach to Artificial Intelligence'.

New Generation Artificial Intelligence Development Plan AKA AIDP (July 2017)	**Proposed Regulation on Artificial Intelligence, AKA the AI Act (April 2021)**
AI should enhance society's productive forces and national competitiveness	AI should be a tool for people and be a force for good in society with the ultimate aim of increasing human well-being

b. Data and privacy protections

This section compares China's Personal Information Protection Law (PIPL) with the EU's General Data Protection Regulation (GDPR). In China, privacy is mainly pursued against private-sector risks, while in the EU, privacy is a fundamental human right. Although broad consumer protections are present, these are not extended to the Chinese government - when national security or the public interest are invoked, there is lack of clear measures and boundaries to protect citizens' privacy.

In October 2020, a draft Personal Information Protection Law (PIPL) was released, a milestone in China's effort towards a comprehensive privacy and data governance regime. Modelled after the GDPR's approach to consent and individuals' rights to access and delete their information, the PIPL demonstrates the government responding to popular will and addressing the same consumer backlash against tech giants that exists around the world, but with characteristics specific to China.[50] The PIPL has been hailed "data privacy with Chinese characteristics"[51] and is a significant development in the evolving global privacy landscape, providing a "third way" between the US and EU approaches to privacy regulation.[52]

Yet progress is counterbalanced by the increase of the Chinese government's access to data, spurred by innovations such as facial recognition. Both the GDPR and the PIPL assert individual privacy and place limits on corporate uses of data. Yet the most significant difference between the two regulations lies in the provisions related to national security. Sizable exemptions exist for the government's collection and use of data when related to security, health, or the vaguely defined "significant public interests".[53]

Whereas the GDPR protects the individual from state power, human rights in China are conceived as being derived from the state itself, meaning that the state's interests remain above the individuals.[54] Therefore, though the PIPL strengthens individual protection against private entities, there is still no significant privacy protection against government intrusion.[55] No accountability or transparency mechanisms exist for China's Ministry of Public Security to

[50] Levine, '"Deeply Alarmed"'.
[51] Pernot-Leplay, 'China's Approach on Data Privacy Law'.
[52] New America, 'Personal Data, Global Effects'.
[53] Roberts et al., 'The Chinese Approach to Artificial Intelligence'.
[54] Pernot-Leplay, 'China's Approach on Data Privacy Law'.
[55] Pernot-Leplay.

publicly report any of its surveillance activities, except to the top CCP leadership.[56] Further, under China's National Intelligence Law, Chinese companies cannot plausibly refuse Chinese government requests to cooperate, whether the data involves users inside or outside China.[57]

In addition, the GDPR promotes the free flow of data across borders, providing several legal transfer mechanisms for doing so. The PIPL, on the other hand, requires the Cyberspace Administration of China to conduct security assessments before an extremely broad array of actors may transfer personal data abroad.[58] Further, the draft PIPL would allow the government to establish a blacklist of overseas data controllers banned from processing Chinese personal data if they are found to be violating China's national security or public interests, allowing the Chinese government to take reciprocal action in the name of data protection.[59]

Overall, it seems as though China intends to build privacy regulation. However, it is the Chinese consumer's data privacy protection that progresses, rather than a citizen's.[60] The persisting dichotomy between privacy from companies and privacy from the government raises questions on how AI surveillance mechanisms will continue to be implemented in China, particularly vis-à-vis the EU's value of personal data as a fundamental right.[61]

How Meaningful are Existing Regulatory Frameworks?

Implications of AI and privacy regulations for AI surveillance

The previous sections provided an overview of AI and privacy regulations that may influence the development and implementation of AI surveillance technology. Regarding AI regulation, we have observed that both China and the EU aim to leverage AI development to improve social and economic outcomes. However, China aims to advance 'societal improvement' through economic development, whereas the EU aims to advance economic development through developing inclusive AI that protects human rights. Regarding privacy, we observe that the lack of privacy from the government raises questions on how AI surveillance mechanisms will continue to be implemented in China, particularly vis-à-vis the EU's value of personal data as a fundamental right. The following section aims to assess the real-world implications of these regulatory approaches for AI surveillance technologies. How "meaningful" are these regulatory frameworks? In other words, do we observe striking differences between *de jure* and *de facto* regulation and what does this imply for the utilization of AI surveillance in China and the EU?

[56] Peterson, 'Designing Alternatives to China's Repressive Surveillance State'.
[57] Peterson.
[58] New America, 'Personal Data, Global Effects'.
[59] New America.
[60] Pernot-Leplay, 'China's Approach on Data Privacy Law'.
[61] Pernot-Leplay.

AI surveillance for political control

Certain authors believe that the CCP's interests are prioritized over the Chinese people's interests.[62] According to a translation from Stanford's DigiChina Cyber Policy Center, there are exceptions in the PIPL for situations that "will impede State organs' fulfilment of their statutory duties and responsibilities".[63] Thus, privacy protections written by the Chinese government are unlikely to apply to state surveillance.

No accountability or transparency mechanisms exist for the Chinese government to publicly report any of its surveillance activities. Though the Governance Principles of the AIDP state that AI should promote fairness and justice, protect the rights and interests of all stakeholders and promote equal opportunities,[64] this seems to conflict substantially with national security and emphasis on ensuring political stability.[65] For example, a vast network of advanced AI facial recognition technology is used to track and control the Uyghurs, a large Muslim minority in China. The technologies look exclusively for Uyghurs based on their appearance and keeps records of their activities.[66] Police documents show demand for such capabilities is spreading – since 2017, Chinese technology giants have registered patents for tools that can detect, track and monitor Uyghurs[67] and almost two dozen police departments in 16 different provinces and regions across China sought such technology beginning in 2018.[68]

Due to the lack of oversight and *de facto* regulation in China over the government's collection and use of private data, domestic companies working with the government on AI technologies involving privacy issues such as live facial recognition may be able to develop solutions within a less restrictive context than those working with the EU governments, such as Megvii, a Beijing-based facial recognition company.[69]

Global AI surveillance technology transfers

The extent of China's surveillance seems to have impacts outside of China. As aforementioned, at least 80 countries from Latin America, Africa, and Asia have adopted Huawei's Safe City solutions or other Chinese surveillance and security technology platforms.[70] This raises the question: is China is creating a future of tech-driven authoritarianism as a competing model

[62] Hoffman, 'Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion'.
[63] Levine, '"Deeply Alarmed"'.
[64] 'Governance Principles for the New Generation Artificial Intelligence--Developing Responsible Artificial Intelligence'.
[65] Roberts et al., 'The Chinese Approach to Artificial Intelligence: An Analysis of Policy and Regulation'.
[66] Mozur, 'One Month, 500,000 Face Scans'.
[67] 'Chinese Tech Patents Tools That Can Detect, Track Uighurs'.
[68] Mozur, 'One Month, 500,000 Face Scans'.
[69] Pernot-Leplay, 'China's Approach on Data Privacy Law'.
[70] Khalil, 'Digital Authoritarianism, China and COVID'.

against emerging democracy?[71] It is difficult to fully grasp China's motives from the outside, but many reports purport that China is aggressively marketing the transfer of advanced AI technology around the globe.[72] The worry is based on the fear that China is creating a future of tech-driven authoritarianism, where its technology transfers are purposely being deployed so as to limit the organic expression and development of nascent democratic movements.[73] In Uganda, for example, Huawei has not only sold surveillance tools, but technicians from the Chinese powerhouse have supposedly also helped the government governments spy on their political opponents.[74]

International digital norm-setting

Through such technology exports, China also attempts to set new norms in digital rights, privacy and data collection as other countries importing Chinese AI surveillance solutions may lead to a growing acceptance of mass surveillance, habituation to restrictions on liberties, and fewer checks on the collection and use of personal data by the state.[75] If China can prove the effectiveness of its AI-powered surveillance technologies, it will become an attractive model and provider of cutting-edge technology for other authoritarian governments.[76] This will have significant impact on the power and endurance of non-democratic regimes all over the world. Such systems will undoubtedly strengthen surveillance and investigative capabilities of the Chinese state. However, will successful surveillance succeed in shaping people's behaviour in ways predictable to the authorities?[77]

What role might EU regulations play to counteract expanding Chinese technological power? The Chinese Belt and Road Initiative (BRI) seems to encourage countries to take on large Chinese loans that can then be leveraged by Beijing for political purposes, such as exporting AI-powered surveillance technology. The European Council has agreed on an ambitious global infrastructure plan to rival the BRI and the European Commission is set to spend nine months producing a list of "high impact and visible projects".[78]

A weak AI Act?

In the EU, the proposed AI Act explicitly regulates AI-enabled surveillance tools, whereas there is no comparable regulation for AI surveillance in China. The AI Act adopts a risk-based and sector-specific approach to set boundaries for AI systems, stating that AI-based indiscriminate

[71] Khalil.

[72] Lilkov, 'Tackling Digital Authoritarianism'; Crosston, 'Cyber Colonization: The Dangerous Fusion of Artificial Intelligence and Authoritarian Regimes'.

[73] Crosston, 'Cyber Colonization: The Dangerous Fusion of Artificial Intelligence and Authoritarian Regimes'.

[74] Parkinson, Bariyo, and Chin, 'Huawei Technicians Helped African Governments Spy on Political Opponents'.

[75] Khalil, 'Digital Authoritarianism, China and COVID'.

[76] Meissner et al., 'Is Big Data Increasing Beijing's Capacity for Control?'

[77] Meissner et al.

[78] Lau, 'EU Starts Work on Rival to China's Belt and Road Initiative'.

surveillance and social scoring systems will not be permitted.[79] Simply put, the AI Plan bans the most “concerning” forms of AI surveillance, such as social credit systems and biometric surveillance and these regulations will cover both EU citizens and companies doing business in the EU.[80]

Though many seem to agree that the AI Act makes notable strides towards regulating AI systems, further work is required, as there are many loopholes in the draft. The different rules put forward in the AI Act for different risk-levels of AI is reasonable, but the dichotomic distinction between high- and low-risk AI is problematic. The regulation allows too wide a scope for self-regulation in some cases; and may even contribute to deregulation in others, for example by the prevention of applying use restrictions to systems the Act does not consider high-risk.[81]

Certain regulations in the AI Act only apply to “high-risk” AI, yet determining the nature of AI risk, particularly during the early development stages, may be near impossible.[82] Fusing AI with existing mass surveillance capabilities, could be permitted where authorized by law, meaning this could be used in law enforcement. The draft AI Act does not prohibit the full extent of unacceptable uses of AI, in particular concerning biometric mass surveillance, leaving a gap for discriminatory and surveillance technologies used by governments and companies.[83]

Conclusion

The fusion of AI with surveillance comes with many risks. Not only does it have the potential to advance authoritarianism and cause instability through competition between political systems, but if taken to the extreme, the proliferation of authoritarian – or totalitarian – regimes, can pose an existential threat to humanity.

This report has provided a brief comparison of existing AI and privacy regulations in China and the EU to understand the implications on the development and implementation of AI-powered surveillance technology. In the realm of AI regulation, the EU follows a "human-centered approach", focusing on mitigating ethical risks, as well as protecting people’s safety and fundamental rights”. China, on the other hand, prioritizes international competitiveness, where even societal wellbeing improvement is achieved through an economic development framework. With regards to privacy regulation, although broad consumer privacy protections are present in China, these are not extended to the Chinese government. When national security or the public

[79] European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts.

[80] Stahl, ‘EU Is Cracking down on AI, but Leaves a Loophole for Mass Surveillance’.

[81] Veale and Borgesius, ‘Demystifying the Draft EU Artificial Intelligence Act’.

[82] Stahl, ‘EU Is Cracking down on AI, but Leaves a Loophole for Mass Surveillance’.

[83] EDRi, ‘EU’s AI Proposal Must Go Further to Prevent Surveillance and Discrimination’.

interest are invoked, there are a lack of clear measures and boundaries to protect citizens' privacy. This clashes largely with the EU's value of personal data as a fundamental right.

Such regulations have profound implications on AI surveillance and raises questions regarding how AI surveillance will continue to develop and be utilized in the future. Worryingly, it seems as though digital technologies are indeed becoming increasingly tied with divergent political models. Data collection and surveillance may, therefore, only continue to grow as a substantial component of ideological clashes.[84]

A few issues merit further attention - due to time constraints, this report was unable to explore them fully. Firstly, based on the observation that China's AI surveillance technologies are being exported successfully abroad, we may wonder why China's AI surveillance systems appeal to adopting countries and whether this does in fact correlate with other countries also adopting more pervasive models of social surveillance. In China, a perceived deficit of social trust has contributed to the expansion of Chinese surveillance capacities, meaning that public support for the China's Social Credit System and its surveillance imperatives remains high, as it is broadly regarded as a means to bringing about a more honest and harmonious society.[85] Given the Social Credit System's ability to be monitored and adjusted in real-time, the system will provide the Chinese state with the ability to roll out new policies and programs at speeds unparalleled in any other country. Government agencies can thus quickly observe the effects of their policies and interventions and adjust accordingly to maximize effect, enabling a process of rapid regulatory learning.[86] Can we say the same for other countries? What are the factors that incline countries to adopt AI surveillance technologies? Moreover, will AI surveillance succeed in shaping people's behaviour in ways predictable to the authorities?

Secondly, it is not permitted to sell certain AI surveillance systems on the EU market, yet it is permitted to sell them abroad to countries with a reputation for using technology to aid state repression.[87] For example, French company Idemia/Morpho sells facial recognition tech to the Shanghai Public Security Bureau and Dutch company Noldus sells facial expression analysis technology 'FaceReader' to the Chinese Ministry of Public Security.[88] Such an outcome may not have been intentional. It would be fruitful, however, to understand how such an outcome transpired. Interviewing those involved in the drafting of the relevant laws is a potential way forward. More generally, however, what role might EU regulations play to counteract expanding Chinese technological power? Relatedly, what shape might an alternative, human- and democracy-friendly model of AI surveillance take?

Some uncertainties nonetheless remain. Specifically, how big of a threat is AI surveillance to international security? If we develop AI that can precipitate a transition comparable to the

[84] Aho and Duffield, 'Beyond Surveillance Capitalism'.
[85] Aho and Duffield, 'Beyond Surveillance Capitalism'.
[86] Aho and Duffield.
[87] Veale and Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act'.
[88] Veale and Borgesius.

industrial revolution,[89] surveillance might only be a secondary issue in related to other AI-related security issues that have the potential to pose more immediate existential risks.

[89] Karnofsky, ‘Potential Risks from Advanced Artificial Intelligence’.

Acknowledgements

This report was written during the Swiss Existential Risk Initiative (CHERI) Summer Research Program. CHERI is a six-week research program for bachelor, master and PhD students to develop projects on the mitigation of global catastrophic risks - events that could curtail the future of humanity.

Views and mistakes are solely that of the author.

Bibliography

European Commission. ‘A European Approach to Artificial Intelligence | Shaping Europe’s Digital Future’. Accessed 9 August 2021. https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence.

Aho, Brett, and Roberta Duffield. ‘Beyond Surveillance Capitalism: Privacy, Regulation and Big Data in Europe and China’. *Economy and Society* 49, no. 2 (2 April 2020): 187–212. https://doi.org/10.1080/03085147.2019.1690275.

Asghar, Mamoona N., Nadia Kanwal, Brian Lee, Martin Fleury, Marco Herbst, and Yuansong Qiao. ‘Visual Surveillance Within the EU General Data Protection Regulation: A Technology Perspective’. *IEEE Access* 7 (2019): 111709–26. https://doi.org/10.1109/ACCESS.2019.2934226.

Bradford, Anu. ‘The Brussels Effect’. In *The Brussels Effect*. New York: Oxford University Press, 2020. https://doi.org/10.1093/oso/9780190088583.003.0003.

Cave, Danielle, Samantha Hoffman, Alex Joske, Fergus Ryan, and Elise Thomas. ‘Mapping China’s Tech Giants’. Australian Strategic Policy Institute, 18 April 2019. https://www.aspi.org.au/report/mapping-chinas-tech-giants.

‘Chinese Tech Patents Tools That Can Detect, Track Uighurs’. *Reuters*, 13 January 2021, sec. China. https://www.reuters.com/article/us-china-tech-uighurs-idUSKBN29I300.

Chutel, Lynsey. ‘China Is Exporting Facial Recognition Software to Africa, Expanding Its Vast Database’. Quartz, ay 2018. https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity/.

Crosston, Matthew. ‘Cyber Colonization: The Dangerous Fusion of Artificial Intelligence and Authoritarian Regimes’. *Cyber, Intelligence, and Security* 4, no. 1 (2020): 23.

Devanesan, Joe. ‘AI-Powered Traffic Management Is Slashing Asia’s Congestion Problem’. Tech Wire Asia, 28 August 2020. https://techwireasia.com/2020/08/ai-powered-traffic-management-is-slashing-asias-congestion-problem/.

European Commission. ‘Digital Europe Programme’. Text. Accessed 9 August 2021. https://ec.europa.eu/info/funding-tenders/find-funding/eu-funding-programmes/digital-europe-programme_en.

EC/OECD. ‘Database of National AI Policies’. OECD.AI, 2021. https://www.oecd.ai.

EDRi. ‘EU’s AI Proposal Must Go Further to Prevent Surveillance and Discrimination’. European Digital Rights (EDRi). Accessed 12 July 2021. https://edri.org/our-work/eus-ai-proposal-must-go-further-to-prevent-surveillance-and-discrimination/.

European Commission. ANNEXES to the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Fostering a European approach to Artificial Intelligence, Pub. L. No. COM(2021) 205 final (2021). https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review.

———. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, Pub. L. No. COM(2021) 206 final (2021). https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206.

European Commission. ‘InvestEU and a Europe Fit for the Digital Age’. Accessed 9 August 2021. https://europa.eu/investeu/about-investeu/what-investeu-programme/investeu-and-europe-fit-digital-age_en.

Feldstein, Steven. ‘The Global Expansion of AI Surveillance’. Working Paper. Carnegie Endowment for International Peace, 2019. https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf.

———. *The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance*. Oxford University Press, 2021.

Gent, Stephen E., and Mark J. C. Crescenzi. ‘Market Power, War, and Strategic Delay’. In *Market Power Politics*. Oxford University Press, 2021. https://doi.org/10.1093/oso/9780197529805.003.0003.

‘Governance Principles for the New Generation Artificial Intelligence--Developing Responsible Artificial Intelligence’. Accessed 7 August 2021. https://www.chinadaily.com.cn/a/201906/17/WS5d07486ba3103dbf14328ab7.html.

Haciyakupoglu, Gulizar, and Wu Shang-Su. ‘China’s Social Credit System: The Black Market and Inequalities’. the interpreter, 18 March 2019. https://www.lowyinstitute.org/the-interpreter/china-social-credit-system-black-market-and-inequalities.

Hadjiyianni, Ioanna. ‘The European Union as a Global Regulatory Power’. *Oxford Journal of Legal Studies* 41, no. 1 (1 March 2021): 243–64. https://doi.org/10.1093/ojls/gqaa042.

Hoffman, S. (2018) Social Credit: Technology-enhanced authoritarian control with global consequences. Policy Brief 6. Australian Strategic Policy Institute. Available at: https://www.aspi.org.au/report/social-credit (Accessed: 7 July 2021).

Hoffman, Samantha. ‘Engineering Global Consent: The Chinese Communist Party’s Data-Driven Power Expansion’. Policy Brief. Australian Strategic Policy Institute, 2019. https://www.aspi.org.au/report/engineering-global-consent-chinese-communist-partys-data-driven-power-expansion.

Hovsepyan, Eduard. ‘Regulating AI: A Success Story for the European Union?’ *E-International Relations* (blog), 13 July 2020. https://www.e-ir.info/2020/07/13/regulating-ai-a-success-story-for-the-european-union/.

GRC World Forums. ‘How GDPR Is Shaping Global Data Protection’, August 2018. https://www.grcworldforums.com/global/how-gdpr-is-shaping-global-data-protection/355.article.

Ikenberry, G. John. ‘Soft Power: The Means to Success in World Politics’. *Foreign Affairs*, June 2004. https://www.foreignaffairs.com/reviews/capsule-review/2004-05-01/soft-power-means-success-world-politics.

Jing, Meng. ‘This Chinese City Plans a US$16 Billion Fund for AI Development’. South China Morning Post, 16 May 2018. https://www.scmp.com/tech/innovation/article/2146428/tianjin-city-china-eyes-us16-billion-fund-ai-work-dwarfing-eus-plan.

Karnofsky, Holden. ‘Potential Risks from Advanced Artificial Intelligence: The Philanthropic Opportunity’. Open Philanthropy, 6 May 2016. https://www.openphilanthropy.org/blog/potential-risks-advanced-artificial-intelligence-philanthropic-opportunity.

Khalil, Lydia. ‘Digital Authoritarianism, China and COVID’. Lowy Institute, 2 November 2020. https://www.lowyinstitute.org/publications/digital-authoritarianism-china-and-covid.

Lau, Stuart. ‘EU Starts Work on Rival to China’s Belt and Road Initiative’. POLITICO, 6 July 2021. https://www.politico.eu/article/eu-starts-work-on-rival-to-chinas-belt-and-road-project-network/.

Levine, Alexandra S. ‘“Deeply Alarmed”: China Now Ahead of U.S. on Privacy Law’. POLITICO, 8 July 2021. https://www.politico.com/newsletters/politico-china-watcher/2021/07/08/deeply-alarmed-china-now-ahead-of-us-on-privacy-law-493497.

Lilkov, Dimitar. ‘Tackling Digital Authoritarianism’. Made in China. Brussels: Wilfred Martens Centre for European Studies, 2020. https://www.martenscentre.eu/wp-content/uploads/2020/06/paper_made-in-china-webversion.pdf.

Little, Jane Braxton. ‘AI Could Spot Wildfires Faster Than Humans’. Scientific American, 17 June 2021. https://www.scientificamerican.com/article/ai-could-spot-wildfires-faster-than-humans/.

Liu, J. and Zhao, H. (2021) ‘Privacy lost: Appropriating surveillance technology in China’s fight against COVID-19’, Business Horizons [Preprint]. doi:10.1016/j.bushor.2021.07.004.

Lomas, Natasha. ‘Europe Lays out Plan for Risk-Based AI Rules to Boost Trust and Uptake’. *TechCrunch* (blog), 21 April 2021. https://social.techcrunch.com/2021/04/21/europe-lays-out-plan-for-risk-based-ai-rules-to-boost-trust-and-uptake/.

Meissner, Mirjam, Rogier Creemers, Pamela K. Crossley, Peter Mattis, and Samantha Hoffman. ‘Is Big Data Increasing Beijing’s Capacity for Control?’ ChinaFile, 10 August 2016. https://www.chinafile.com/conversation/Is-Big-Data-Increasing-Beijing-Capacity-Control%3F.

Mozur, Paul. ‘One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority’. *The New York Times*, 14 April 2019, sec. Technology. https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html.

Murphy, Ben, ed. ‘Artificial Intelligence Security Standardization White Paper’. CSET, 14 May 2020. https://cset.georgetown.edu/publication/artificial-intelligence-security-standardization-white-paper-2019-edition/.

New America. ‘Personal Data, Global Effects: China’s Draft Privacy Law in the International Context’. New America. Accessed 6 July 2021. http://newamerica.org/cybersecurity-initiative/digichina/blog/personal-data-global-effects-chinas-draft-privacy-law-in-the-international-context/.

Nilsen, Ella, and Alex Ward. ‘Biden Is Using His Economic Plan to Challenge China’. Vox, 26 April 2021. https://www.vox.com/22350402/biden-infrastructure-plan-foreign-policy-china.

Ord, Toby. *The Precipice*. Bloomsbury Publishing, 2020.

Parkinson, Joe, Nicholas Bariyo, and Josh Chin. ‘Huawei Technicians Helped African Governments Spy on Political Opponents’. *Wall Street Journal*, 15 August 2019, sec. Tech. https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017.

Pernot-Leplay, Emmanuel. ‘China’s Approach on Data Privacy Law: A Third Way Between the U.S. and the EU?’ SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, 2020. https://papers.ssrn.com/abstract=3542820.

Peterson, Dahlia. ‘Designing Alternatives to China’s Repressive Surveillance State’. Center for Security and Emerging Technology, October 2020. https://cset.georgetown.edu/publication/designing-alternatives-to-chinas-repressive-surveillance-state/.

Raines, Thomas. ‘Raise the Bar by Leveraging the EU’s Regulatory Power’. Chatham House – International Affairs Think Tank, 12 June 2019. https://www.chathamhouse.org/2019/06/raise-bar-leveraging-eus-regulatory-power.

The White House. ‘Remarks by President Biden in Press Conference’, 25 March 2021. https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/03/25/remarks-by-president-biden-in-press-conference/.

Roberts, Huw, Josh Cowls, Emmie Hine, Jessica Morley, Mariarosaria Taddeo, Vincent Wang, and Luciano Floridi. ‘Governing Artificial Intelligence in China and the European Union: Comparing Aims and Promoting Ethical Outcomes’. SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, 1 March 2021. https://papers.ssrn.com/abstract=3811034.

Roberts, Huw, Josh Cowls, Jessica Morley, Mariarosaria Taddeo, Vincent Wang, and Luciano Floridi. ‘The Chinese Approach to Artificial Intelligence: An Analysis of Policy, Ethics, and Regulation’. *AI & SOCIETY* 36, no. 1 (1 March 2021): 59–77. https://doi.org/10.1007/s00146-020-00992-2.

Romaniuk, Scott N., and Tobias Burgers. ‘How China’s AI Technology Exports Are Seeding Surveillance Societies Globally’. *The Diplomat*, 18 October 2018. https://thediplomat.com/2018/10/how-chinas-ai-technology-exports-are-seeding-surveillance-societies-globally/.

Sahin, Kaan. ‘The West, China, and AI Surveillance’. *Atlantic Council* (blog), 18 December 2020. https://www.atlanticcouncil.org/blogs/geotech-cues/the-west-china-and-ai-surveillance/.

Stahl, Bernd Carsten. ‘EU Is Cracking down on AI, but Leaves a Loophole for Mass Surveillance’. The Conversation, 21 April 2021. http://theconversation.com/eu-is-cracking-down-on-ai-but-leaves-a-loophole-for-mass-surveillance-159421.

Veale, Michael, and Frederik Zuiderveen Borgesius. ‘Demystifying the Draft EU Artificial Intelligence Act’. SocArXiv, 5 July 2021. https://doi.org/10.31235/osf.io/38p5f.

Ward, Alex. ‘Joe Biden Wants to Prove Democracy Works — before It’s Too Late’. Vox, 28 April 2021. https://www.vox.com/2021/4/28/22408735/joe-biden-congress-speech-democracy-autocracy.

Webster, Graham, Rogier Creemers, Paul Triolo, and Elsa Kania. ‘Full Translation: China’s “New Generation Artificial Intelligence Development Plan” (2017)’. *New America* (blog), 1 August 2017. http://newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/.

European Commission. ‘What Is the InvestEU Programme?’ Accessed 9 August 2021. https://europa.eu/investeu/about-investeu/what-investeu-programme_en.

Wright, Nicholas. ‘How Artificial Intelligence Will Reshape the Global Order’, 11 October 2019. https://www.foreignaffairs.com/articles/world/2018-07-10/how-artificial-intelligence-will-reshape-global-order.