How Do the UK and China Regulate the Use of Facial Recognition Software in Public Surveillance Systems, and What Are the Ethical and Legal Implications of Their Differing Approaches To Transparency, Privacy Protection, and State Control?

Nathalie Sofia Cooper

IE University, Segovia, Spain

Email: Ncooper.ieu2023@student.ie.edu

Published: 27th of January, 2025

**Abstract**

This paper investigates the use of Facial Recognition Technologies (FRT) in public surveillance systems in the United Kingdom and China. It assesses the respective countries’ approaches to privacy, data protection, and state control. Through the use of case law such as R (Bridges) v. South Wales Police as well as a detailed analysis of key legislation including China’s cybersecurity law, this paper draws two main conclusions: the first is that facial recognition in the UK is constricted by law through the country’s strong democratic tradition and strict data protection laws despite a strong desire to increase use of such technology by security forces. The second conclusion drawn is that FRT in China is less heavily regulated due to its authoritarian system of government that places more importance on state security rather than individuals’ right to privacy and data protection. Finally, this paper identifies the problems that may arise for the protection of individual rights with a more lenient legal approach to FRT through assessing the ethical and legal implications of the use of these technologies in public surveillance systems.

**Introduction**

This paper will discuss the legal and ethical implications of the use of facial recognition software in public spaces in the UK versus China. It will comment on the differing approaches of the two countries with regards to transparency, privacy protection, and state control. Facial recognition technology is a type of technology that uses an algorithm to both verify and identify an individual from an image or a video[[1]](#footnote-0). Its origins can be traced back as early as the 1960s, when Woodrow Wilson Bledsoe devised a mechanism to identify peoples’ faces and compare it to data points of already stored photos[[2]](#footnote-1). Initially, this system was neither fast nor efficient, but by the early 2000s and from 2010 onwards, it became more digitalised and widespread. In 2011 for example, FRT was used to identify Osama Bin Laden, while in 2014, Facebook developed the ‘tag’ feature in social media photos, which expanded the scope of the software massively[[3]](#footnote-2).

Over the course of the past decade, this technology has grown to immeasurable popularity, and has become a crucial part of identification in our daily lives; from registering at the workplace to signing into our phones, it is clear that FRT is everywhere. This has put a substantial strain on our legal systems and our personal rights related to them. While on one hand the software has improved our security measures (when it comes to, for example, the identification of criminals), as well as optimized our day-to-day administrative tasks, it has, in some countries, been subject to misuse. This misuse includes, amongst others, improper data storage, abuse of personal data, and a lack of transparency[[4]](#footnote-3). As a result of this, there have been many questions as to where this software stands with regards to our individual/human rights, as well as how it affects our right to privacy. In order to assess this criterion and see how facial recognition technology in public surveillance systems is regulated, this paper will analyse two different jurisdictions with opposing approaches to privacy, transparency, and state influence: the UK and China. It will be argued that the UK, which has a strong democratic tradition, emphasises individual privacy and regulatory transparency as opposed to robust state control. While there has not yet been specific legislation targeted at FRT in the UK, this paper will analyse the different sources from which the UK draws upon to regulate this technology. On the other hand, China, which has an authoritarian regime, places more importance on state control as opposed to privacy protection and ethical standards. Therefore, while the UK restricts facial recognition technology through stringent legal provisions, China’s state-controlled surveillance systems reflects a higher emphasis on security than privacy.

**The UK’s ‘Privacy First’ Legal Framework and Regulatory Approach**

The UK’s strict regulation of facial recognition software and its protection of privacy rights is reflected in its strong democratic tradition. As mentioned before, because of how new this technology is, there have not yet been **specific** laws to regulate it, however there are countless sources of law governing privacy rights and data protection which are directly applicable to the topic of Facial Recognition Technology (FRT). This includes, amongst others, judicial rulings and statutes. The protection of citizens from the abuse of FRT by the government and the police is reflected by robust regulatory frameworks like The Framework Convention on Artificial Intelligence (FCAI), the Data Protection Act (2018) (DPA) and the Surveillance Camera Code of Practice (2013) (SCCP).

The first regulatory framework which governs the UK’s facial recognition system in public places is the ‘Council of Europe Framework Convention on AI’. This convention is considered the first “legally binding international agreement on AI” and was signed by the UK in September 2024[[5]](#footnote-4). It includes provisions which regulate rights within the scope of Artificial Intelligence and include the widespread use of facial recognition technology, which the UK has widely been using in public surveillance systems to, for example, identify and convict people of crimes[[6]](#footnote-5). It includes regulatory frameworks and provisions to protect individuals and their data, as well as human rights and the rule of law. It also incorporates vital safeguards, such as the principle of self-determination (which allows people to “decide their own destiny in the international order”[[7]](#footnote-6)) and the principle of equality (the idea that individuals should be treated alike in the eyes of the law). These, while accepting the widespread use of AI and its effects on our day-to-day life, aim at promoting state transparency[[8]](#footnote-7). Nevertheless, the framework did not come without scrutiny. There have been concerns as to whom the treaty actually applies to, and which actors it exempts. Francesca Fanucci, one of the many drafters of the treaty as well as a legal expert at ECNL, voiced her concerns about the extent to which the treaty limits the activities of private actors[[9]](#footnote-8). Despite the Convention being one of the most progressive pieces of AI legislation, it is clear that it has some loopholes that may lead to abuse. Firstly, it provides for an insufficient regulation of private companies as opposed to the public sector, which Fanucci described as “disappointing”[[10]](#footnote-9). The Convention also allows exceptions for the use of AI in national security contexts, which could allow for states to abuse it in ways that can negatively infringe on human rights.

For the UK, this framework enhances the already-existing British legislation on privacy and data-protection, such as the DPA and the SCCP, by governing the use of AI in the use of facial recognition technology and preventing the state from abusing its discretionary power and infringing on individual rights. It also makes sure that there are harmonised efforts across Europe to control and answer for the widespread use of AI. The ‘human-centric’ design of the legislation allows for FRT to serve the wider public good without, once again, compromising personal privacy.

The Surveillance Camera Code of Practice (2013) (aka the SCCP) was issued under the Protection of Freedoms Act in 2012[[11]](#footnote-10), and is another piece of legislation that solidifies the notion that Facial Recognition Software in public places is heavily regulated in the UK. When looking at the code’s main doctrines, it is evident that state surveillance and facial recognition are guided by three main principles – firstly, there should be as much transparency as possible in surveillance. This includes a “published contact point for access to information and complaints”[[12]](#footnote-11), and all rules and policies to do with surveillance must be clear and accessible by all parties affected. Secondly, there must be a justified, legal, and legitimate claim in order to use such technologies and the data collected by them – they should not be unnecessarily stored if they have already been used, and their use must follow specified procedures that do not infringe upon the right to privacy. Thirdly, the methods of surveillance cannot be excessively intrusive – this relates to transparency, as well as who is able to access such recordings/images and making sure that they are being appropriately used. By enforcing the aforementioned standards, the code balances public safety and the duty of state agents such as the police to punish crimes and fulfil their duties while maintaining the notion of an individual’s right to privacy.

Finally, the Data Protection Act (2018) can be considered one of the biggest pieces of legislation that governs the UK’s right to privacy and the processing of data – it enshrined key provisions from the EU’s General Data Protection Regulation (GDPR) into British law, even after Brexit. Similarly to the SCCP, it also specifies that personal data (including data derived from facial recognition technology), can only be used with a legitimate and lawful purpose, and that privacy rights cannot be infringed upon. There is also an explicitly stated right to know and find out what data different organisations and the government have about you – fulfilling the requirement of transparency. You are also able to object to the way in which your data is being used[[13]](#footnote-12), and data can either be deleted (with the ‘Right to be Forgotten’) or erased completely. Therefore, this act clearly protects individuals against the unlawful processing and use of their private information by the state and related actors, including data from FRTs, which reflects the UK’s strong belief in democratic principles. Case law in the UK, such as the ruling in ***R (Bridges) v South Wales Police (2020) EWCA civ 1058*** further proves the limitations on FRT and emphasises the UK’s privacy-first approach.

The case of *R (Bridges) v South Wales Police (2020) EWCA civ 1058*marked the first official scrutiny of UK courts of FRT. Ed Bridgers, a resident of Cardiff, challenged the use of facial recognition software by the South Wales Police, claiming that its use violated his privacy rights under the DPA 2018, art. 8 of the ECHR, and the Human Rights Act (1998) (HRA). This occurred after he attended a protest on March 27th, 2018. He was not made aware by the Police that they were going to utilise FRT on him. The Court of Appeal ruled in his favour, and held that the South Wales Police, through its use of FRT, violated art. 8 of the ECHR, the DPA 2018, and the Public Sector Equality Duty of the Equality Act[[14]](#footnote-13). The judgement of the Court of Appeal set an important example for the limitations of Britain’s use of FRT, proving that the UK values individuals’ right to privacy over the interests of the state. This case proved that this type of mass data collection through automatic facial recognition technology could have a disproportionate effect on individual rights, such as the freedom of expression, the right to privacy, and the freedom of assembly[[15]](#footnote-14). It also paved the way for citizens to be able to express themselves however they want without their data being captured and used against them in the context of social protests (as was the case with Mr. Bridges), as well as other circumstances.

Therefore, the UK’s privacy-first approach strongly reflects its democratic values and its belief in the principles of transparency, proportionality, and the protection of individual autonomy. Through the use of three key pieces of legislation (the DPA 2018, the SCCP, and the Framework Convention on AI), as well as the ruling in *R (Bridges) v. South Wales Police (2020)*, it is clear that the UK ensures the FRT is not being overused and that the state and its actors do not infringe upon individual rights when collecting data from such technologies. By prioritising the above-mentioned principles, as well as the relevant legal provisions, the UK ensures that there is no unchecked use of surveillance technology, guaranteeing that facial recognition software is used ethically and in a responsible manner.

**China’s Surveillance Infrastructure and State Control Priorities**

China’s approach to surveillance, facial recognition software, as well as privacy is vastly different from the UK’s – this can be accredited to its socialist-authoritarian political system, which emphasises state control and state security over all else. The fear of repression, constant surveillance, and absolute adherence to state-controlled entities are just some of the main ways through which China has nurtured its ‘Chinese Dream’ that Xi Jinping and the communist party have propagated in recent years[[16]](#footnote-15). This allows for the extensive use of FRT in public places, without legal provisions to protect individuals or their right to privacy. This is facilitated through two main legislative and policy frameworks, namely the Cybersecurity Law of 2017 and the Social Credit System. While existing legal apparatus (such as cybersecurity laws) are promising steps toward better data protection, most of them are far too general or their language is much too vague to actually establish individuals’ clear-cut rights. The 2017 Cybersecurity Law was supposedly made to protect national security, public interest, and ensure cybersecurity[[17]](#footnote-16). It does so through legally authorising the storage and collection of data from domestic servers (that companies, public organisations, and surveillance systems gather) and giving access to the government in the name of national security[[18]](#footnote-17). This gives the government access to an enormous range of personal data and information about citizens, directly infringing upon their rights. It also means that any state entity or company in China can use technologies such as surveillance systems and facial recognition software to collect information about individuals. For example, Article 29 advocates for the “cooperation between network operators in areas such as the gathering, analysis, reporting, and emergency handling of cybersecurity information”[[19]](#footnote-18). Furthermore, what often appears in the Act are vague terms such as ‘national security’ and ‘public interest’ – these give the government extensive discretion to process, store, and collect any data they see fit. There are also provisions that raise concerns over how much the Chinese government actually protects privacy rights as opposed to state interests – Articles 31 as well as 37 urges for the ‘critical protection of information infrastructure’. However, without clear definitions to do with data protection, they create centralised data repositories the government can access with great ease. Therefore, it is clear that the 2017 Cybersecurity Law grants more power to the state as opposed to having been created to protect individuals from privacy abuse – it reinforces an authoritarian approach to FRT and public surveillance. This has come under international criticism – the US, which went from openly criticising China’s Cybersecurity Law to banning certain Chinese websites from operating in America, has been at the forefront of the disapproval[[20]](#footnote-19). More criticism came when China began exporting their CCTV cameras to Europe, where the technology “Hikvision” allowed Chinese tech firms to access all the data recorded[[21]](#footnote-20). China’s approach reflects the ethical and human rights challenges associated with facial recognition software in public spaces – this has caused China to adopt an environment that lacks both privacy protections as well as democratic accountability.

China’s attitude towards facial recognition software and privacy is also reflected in its development of the Social Credit System –a government-led initiative that monitors and assesses the behaviour of all citizens and enterprises in the country. According to a publication by Princeton University[[22]](#footnote-21), the System uses FRT to track individuals across all sectors, from public transportation and the workplace to residential neighbourhoods and crowds – it then analyses their behaviour and gives them social credit scores according to how they act. This either penalises or rewards citizens, nurturing a culture of compliance and strict adherence to rules due to the feeling of constant state surveillance. The system is available and published online for anyone to see, alongside the name and the social credit score of the individual – it provides details on the deeds done, the legal status of the person, and their full profile. Some experts[[23]](#footnote-22) have even speculated that the system goes so far as to give you a higher social credit score if you purchase items such as diapers but lower if you buy alcohol or video games. Eating on trains is also punished, as is spreading false rumours about other people, or cheating in online games[[24]](#footnote-23). The impact on individual lives is wide-ranging – with a good social credit score, citizens get preferential treatment when interacting with the government[[25]](#footnote-24). This can, for example, lead to the government giving you priority in granting subsidies. Nevertheless, there are also negative implications for citizens with a ‘bad’ score. They can be restricted from sending their children to private school or travelling to places by plane[[26]](#footnote-25). The System, powered by FRT, makes citizens subject to continuous surveillance and awareness that they are being watched, judged, and controlled at all times. This encourages conformity to state-outlined social values, restricting diversity and the accountability of the government. Compared to the UK, it is clear that China prioritises state surveillance over individual privacy, and that there is no clear regulatory framework that protects your individual freedom. The ethical implications of the Social Credit System in China is therefore profound – not only can the state access nearly all aspects of an individual’s life through facial recognition software, but the public can access the name, photo, and social credit number of any individual in China. The System, powered by FRT, makes citizens subject to continuous surveillance and awareness that they are being watched, judged, and controlled at all times. This encourages conformity to state-outlined social values, restricting diversity and the accountability of the government.

**Conclusion**

In conclusion, the UK and China’s regulatory approaches differ fundamentally. The UK has a transparency and privacy-focused approach due to its democratic tradition – acts such as the DPA, the SCCP, and the Framework Convention on AI all protect the individual’s right to privacy and freedom – the abuse of FRT is also heavily limited by the judiciary. While both models prioritise national security in some sense, it is clear that China has rather included this as a vague term that allows for more state interference in private life. It is therefore evident that the country has a more security-oriented and opaque practice, that allows it to easily monitor and control citizens through FRTs. While both models reflect different political systems, and it is necessary to take the political reality of the time in each country into account, it seems that democratic frameworks work better to safeguard human rights and individual rights than authoritarian ones. In the future, it will be necessary for China to start prioritising individuals, and developing clear laws with specific provisions that protect people from state control and abuse.

The real question, however, remains – is there any hope for the protection of individual rights in a world of ever-expanding facial recognition technology? Whether it’s in the UK or in China, it is clear that each individual system will have its own peculiarities, given their respective histories. The UK’s regulatory framework, while having made substantial steps towards granting individuals’ privacy rights, could improve by creating more specific legislation that targets private companies as opposed to purely the public sector. This would ensure that human rights are protected even in private scenarios of FRT. China must take more urgent and extensive measures. Firstly, it should implement comprehensive privacy laws. Independent bodies could monitor compliance with these legal frameworks, free from the government’s control. China should also aim at promoting transparency and accountability and adhere to international standards of facial recognition software use. Overall, the battle for privacy in the modern technological sphere is not only about law or technology – it is a test of how well we can safeguard individual freedoms and privacy in the face of the state and ever-evolving technologies.

**BIBLIOGRAPHY**

Babická, Karolína. “Understanding the Scope of the Council of Europe Framework Convention on AI.” Opinio Juris, October 31, 2024. <https://opiniojuris.org/2024/11/05/understanding-the-scope-of-the-council-of-europe-framework-convention-on-ai/>.

BBC News. “What does Xi Jinping’s China Dream mean?,” June 5, 2013. <https://www.bbc.com/news/world-asia-china-22726375>.

Civil Liberties Union for Europe. “Civil Liberties Union for Europe | liberties.eu,” November 29, 2024. <https://www.liberties.eu/en>.

Columbia Global Freedom of Expression. “R v. the Chief Constable of South Wales Police - Global Freedom of Expression.” Global Freedom of Expression, July 12, 2023. <https://globalfreedomofexpression.columbia.edu/cases/r-v-the-chief-constable-of-south-wales-police/#:~:text=The%20judgment%20of%20the%20Court,Article%208%20of%20the%20European>.

DigiChina. “Translation: Cybersecurity Law of the People’s Republic of China (Effective June 1, 2017) - DigiChina,” August 16, 2022. <https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/>.

DigiChina. “Translation: Cybersecurity Law of the People’s Republic of China (Effective June 1, 2017) - DigiChina,” August 16, 2022. <https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/>.

EEAS. “The European Commission signs historic Council of Europe Framework Convention on Artificial Intelligence and Human Rights,” n.d. <https://www.eeas.europa.eu/delegations/council-europe/european-commission-signs-historic-council-europe-framework-convention-artificial-intelligence-and_en?s=51>.

GOV.UK. “Amended Surveillance Camera Code of Practice (accessible version),” March 3, 2022. <https://www.gov.uk/government/publications/update-to-surveillance-camera-code/amended-surveillance-camera-code-of-practice-accessible-version>

GOV.UK. “Amended Surveillance Camera Code of Practice (accessible version),” March 3, 2022. <https://www.gov.uk/government/publications/update-to-surveillance-camera-code/amended-surveillance-camera-code-of-practice-accessible-version>

GOV.UK. “Amended Surveillance Camera Code of Practice (accessible version),” March 3, 2022. <https://www.gov.uk/government/publications/update-to-surveillance-camera-code/amended-surveillance-camera-code-of-practice-accessible-version>

Government Digital Service. “Data protection.” GOV.UK, September 16, 2015. <https://www.gov.uk/data-protection>

Journal of Public and International Affairs. “The Social Credit System: Not Just Another Chinese Idiosyncrasy,” n.d. <https://jpia.princeton.edu/news/social-credit-system-not-just-another-chinese-idiosyncrasy>.

Klingert, Liv. “China’s cameras face fresh scrutiny in Europe.” *POLITICO*, October 10, 2021. <https://www.politico.eu/article/hikvision-china-surveillance-chinese-tech-europe/>.

Klosowski, Thorin. “Facial Recognition Is Everywhere. Here’s What We Can Do About It.” *Wirecutter: Reviews for the Real World*, July 15, 2020. <https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/>.

Lamb, Naiyie. “Is China’s Social Credit System Really Orwell’s Big Brother?” PIA VPN Blog, January 30, 2024. <https://www.privateinternetaccess.com/blog/in-china-your-credit-score-is-now-affected-by-your-political-opinions-and-your-friends-political-opinions/>.

LII / Legal Information Institute. “self determination (international law),” n.d. <https://www.law.cornell.edu/wex/self_determination_(international_law)#:~:text=Self%Determination%20%20denotes%20the%20%20legal,a%20number%20of%20international%20%20treaties>

Mitchell, Anna, and Larry Diamond. “China's Surveillance State Should Scare Everyone.” *The Atlantic*, February 5, 2018. <https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/>.

Pearson, James, Raphael Satter, and Christopher Bing. “US, UK accuse China of cyberespionage that hit millions of people.” Reuters, March 25, 2024. <https://www.reuters.com/technology/cybersecurity/us-sanctions-chinese-cyberespionage-firm-saying-it-hacked-us-energy-industry-2024-03-25/>.

Reuters. “US, Britain, EU to Sign First International AI Treaty,” September 5, 2024. <https://www.reuters.com/technology/artificial-intelligence/us-britain-eu-sign-agreement-ai-standards-ft-reports-2024-09-05/>

Reuters. “US, Britain, EU to Sign First International AI Treaty,” September 5, 2024. <https://www.reuters.com/technology/artificial-intelligence/us-britain-eu-sign-agreement-ai-standards-ft-reports-2024-09-05/>

Sample, Ian. “What is facial recognition - and how sinister is it?” *The Guardian*, July 29, 2019. <https://www.theguardian.com/technology/2019/jul/29/what-is-facial-recognition-and-how-sinister-is-it>.

Singh, Shilpi, and Prasad. “Techniques and Challenges of Face Recognition: A Critical Review.” *Procedia Computer Science* 143 (2018): 536–43. <https://www.sciencedirect.com/science/article/pii/S1877050918321252>.

Squires, Dan, QC, Aidan Wills, Liberty, Jason Beer QC, Francesca Whitelaw, Richard O’Brien, Thomas Yarrow, et al. “R (Bridges) -v- CC South Wales & ors.” *Court of Appeal (Civil Division) Case No: C1/2019/2670*, August 11, 2020. <https://www.libertyhumanrights.org.uk/wp-content/uploads/2020/02/Bridges-Court-of-Appeal-judgment.pdf>.

Wang, Zhizheng. “Systematic Government Access to Private-Sector Data in China.” In *Oxford University Press eBooks*, 241–58, 2017. <https://doi.org/10.1093/oso/9780190685515.003.0011>.

Yang, Zeyi. “China just announced a new social credit law. Here’s what it means.” *MIT Technology Review*, August 4, 2024. <https://www.technologyreview.com/2022/11/22/1063605/china-announced-a-new-social-credit-law-what-does-it-mean/>

Yang, Zeyi. “China just announced a new social credit law. Here’s what it means.” *MIT Technology Review*, August 4, 2024. <https://www.technologyreview.com/2022/11/22/1063605/china-announced-a-new-social-credit-law-what-does-it-mean/>.

1. Singh, Shilpi, and Prasad. “Techniques and Challenges of Face Recognition: A Critical Review.” *Procedia Computer Science* 143 (2018): 536–43. https://www.sciencedirect.com/science/article/pii/S1877050918321252. [↑](#footnote-ref-0)
2. Klosowski, Thorin. “Facial Recognition Is Everywhere. Here’s What We Can Do About It.” *Wirecutter: Reviews for the Real World*, July 15, 2020. https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/. [↑](#footnote-ref-1)
3. Sample, Ian. “What is facial recognition - and how sinister is it?” *The Guardian*, July 29, 2019. https://www.theguardian.com/technology/2019/jul/29/what-is-facial-recognition-and-how-sinister-is-it. [↑](#footnote-ref-2)
4. Civil Liberties Union for Europe. “Civil Liberties Union for Europe | liberties.eu,” November 29, 2024. https://www.liberties.eu/en. [↑](#footnote-ref-3)
5. EEAS. “The European Commission signs historic Council of Europe Framework Convention on Artificial Intelligence and Human Rights,” n.d. https://www.eeas.europa.eu/delegations/council-europe/european-commission-signs-historic-council-europe-framework-convention-artificial-intelligence-and\_en?s=51. [↑](#footnote-ref-4)
6. GOV.UK. “Amended Surveillance Camera Code of Practice (accessible version),” March 3, 2022. https://www.gov.uk/government/publications/update-to-surveillance-camera-code/amended-surveillance-camera-code-of-practice-accessible-version. [↑](#footnote-ref-5)
7. LII / Legal Information Institute. “self determination (international law),” n.d. https://www.law.cornell.edu/wex/self\_determination\_(international\_law)#:~:text=Self%Determination%20 denotes%20the%20 legal,a%20number%20of%20international%20 treaties. [↑](#footnote-ref-6)
8. Babická, Karolína. “Understanding the Scope of the Council of Europe Framework Convention on AI.” Opinio Juris, October 31, 2024. https://opiniojuris.org/2024/11/05/understanding-the-scope-of-the-council-of-europe-framework-convention-on-ai/. [↑](#footnote-ref-7)
9. Reuters. “US, Britain, EU to Sign First International AI Treaty,” September 5, 2024. <https://www.reuters.com/technology/artificial-intelligence/us-britain-eu-sign-agreement-ai-standards-ft-reports-2024-09-05/>. [↑](#footnote-ref-8)
10. Reuters. “US, Britain, EU to Sign First International AI Treaty,” September 5, 2024. <https://www.reuters.com/technology/artificial-intelligence/us-britain-eu-sign-agreement-ai-standards-ft-reports-2024-09-05/>. [↑](#footnote-ref-9)
11. GOV.UK. “Amended Surveillance Camera Code of Practice (accessible version),” March 3, 2022. <https://www.gov.uk/government/publications/update-to-surveillance-camera-code/amended-surveillance-camera-code-of-practice-accessible-version>. [↑](#footnote-ref-10)
12. GOV.UK. “Amended Surveillance Camera Code of Practice (accessible version),” March 3, 2022. https://www.gov.uk/government/publications/update-to-surveillance-camera-code/amended-surveillance-camera-code-of-practice-accessible-version. [↑](#footnote-ref-11)
13. Government Digital Service. “Data protection.” GOV.UK, September 16, 2015. https://www.gov.uk/data-protection. [↑](#footnote-ref-12)
14. Squires, Dan, QC, Aidan Wills, Liberty, Jason Beer QC, Francesca Whitelaw, Richard O’Brien, Thomas Yarrow, et al. “R (Bridges) -v- CC South Wales & ors.” *Court of Appeal (Civil Division) Case No: C1/2019/2670*, August 11, 2020. https://www.libertyhumanrights.org.uk/wp-content/uploads/2020/02/Bridges-Court-of-Appeal-judgment.pdf. [↑](#footnote-ref-13)
15. Columbia Global Freedom of Expression. “R v. the Chief Constable of South Wales Police - Global Freedom of Expression.” Global Freedom of Expression, July 12, 2023. https://globalfreedomofexpression.columbia.edu/cases/r-v-the-chief-constable-of-south-wales-police/#:~:text=The%20judgment%20of%20the%20Court,Article%208%20of%20the%20European. [↑](#footnote-ref-14)
16. BBC News. “What does Xi Jinping’s China Dream mean?,” June 5, 2013. https://www.bbc.com/news/world-asia-china-22726375. [↑](#footnote-ref-15)
17. DigiChina. “Translation: Cybersecurity Law of the People’s Republic of China (Effective June 1, 2017) - DigiChina,” August 16, 2022. https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/. [↑](#footnote-ref-16)
18. Wang, Zhizheng. “Systematic Government Access to Private-Sector Data in China.” In *Oxford University Press eBooks*, 241–58, 2017. https://doi.org/10.1093/oso/9780190685515.003.0011. [↑](#footnote-ref-17)
19. DigiChina. “Translation: Cybersecurity Law of the People’s Republic of China (Effective June 1, 2017) - DigiChina,” August 16, 2022. https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/. [↑](#footnote-ref-18)
20. Pearson, James, Raphael Satter, and Christopher Bing. “US, UK accuse China of cyberespionage that hit millions of people.” Reuters, March 25, 2024. https://www.reuters.com/technology/cybersecurity/us-sanctions-chinese-cyberespionage-firm-saying-it-hacked-us-energy-industry-2024-03-25/. [↑](#footnote-ref-19)
21. Klingert, Liv. “China’s cameras face fresh scrutiny in Europe.” *POLITICO*, October 10, 2021. https://www.politico.eu/article/hikvision-china-surveillance-chinese-tech-europe/. [↑](#footnote-ref-20)
22. Journal of Public and International Affairs. “The Social Credit System: Not Just Another Chinese Idiosyncrasy,” n.d. https://jpia.princeton.edu/news/social-credit-system-not-just-another-chinese-idiosyncrasy. [↑](#footnote-ref-21)
23. Mitchell, Anna, and Larry Diamond. “China's Surveillance State Should Scare Everyone.” *The Atlantic*, February 5, 2018. https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/. [↑](#footnote-ref-22)
24. Lamb, Naiyie. “Is China’s Social Credit System Really Orwell’s Big Brother?” PIA VPN Blog, January 30, 2024. https://www.privateinternetaccess.com/blog/in-china-your-credit-score-is-now-affected-by-your-political-opinions-and-your-friends-political-opinions/. [↑](#footnote-ref-23)
25. Yang, Zeyi. “China just announced a new social credit law. Here’s what it means.” *MIT Technology Review*, August 4, 2024. [↑](#footnote-ref-24)
26. Yang, Zeyi. “China just announced a new social credit law. Here’s what it means.” *MIT Technology Review*, August 4, 2024. https://www.technologyreview.com/2022/11/22/1063605/china-announced-a-new-social-credit-law-what-does-it-mean/. [↑](#footnote-ref-25)