US Tapping China

Trends of Surveillance and Digital Authoritarianism in the US and China

Paula Soumaya Domit
Rebecca Leeper
Larissa Zutter

Common Good Digital Framework
September, 2020

Introduction

The United States is built upon a foundation of civil liberties including privacy and due process. Such liberties protect citizens from government overreach and promote democracy. With the advent of disruptive technology, particularly artificial intelligence (AI) and the ability to store and process big-data, surveillance methods, which fundamentally erode prized civil liberties, have been augmented. China's use of such technology is an illustration of how they can be deployed to oppress and perpetuate totalitarianism -- also known as digital authoritarianism[1]. This concerning trend is not confined to the Chinese state, but rather is an international trend. The evolution of surveillance methods and policies utilized by the US government bear a striking resemblance to the trajectory which led the Chinese government to become an authoritarian surveillance regime.

This paper will first review the existing discriminatory surveillance regime of the Chinese government, including its technical capacity and the policies which uphold it. The technologies used by the United States to advance their surveillance methods since 2001 will also be examined. In addition, a legal review of US policies related to privacy and surveillance will be outlined. Finally, we will investigate a pivotal case study of government coordination with a private company, namely Yahoo. The technologies developed, policies instituted, and actions taken by the US government all serve to expose the United States' trajectory towards digital totalitarianism, as they mirror, though more covertly, the behaviors of the Chinese government. The conclusion will then address US policy recommendations to reverse its current track and

[1] Digital authoritarianism is the use of digital information technology by authoritarian regimes to surveil, repress, and manipulate domestic and foreign populations (Alina Polyakova & Chris Meserole, 2019).

emerge as an international leader promoting its democratic values as they relate to AI and surveillance.

China

Surveillance Capacity Expansion

In the twenty years since the establishment of the Great Firewall of China, the Chinese government has continued to develop its capacities in surveillance and governance through digital technology and now boasts of the most robust and sophisticated surveillance system in the world. In 2005, the Ministry of Public Security (MPS) and the Ministry of Industry and Information Technology (MIIT) launched SkyNet, a program seeking to install a national network of CCTV feeds (Polyakova and Meserole, 2019). The project was massively successful and significantly expanded the magnitude and reach of Chinese surveillance. By 2017, China had the largest video surveillance network in the world with one CCTV camera for every 5.9 citizens (Campbell, 2019). It was expanded into Sharp Eyes, an ambitious project aimed to create an "omnipresent, fully networked, always working and fully controllable" surveillance system using a variety of technologies to produce 100% coverage of all public areas (Campbell, 2019). The Chinese state collects copious other personal data from internet usage, digital communications, fiscal information, DNA, and more. During the COVID-19 pandemic, the Chinese government has also begun utilizing a contact-tracing app through which it collects self-reported information regarding the health status, travel data, social environment and health records of an individual (Wels-Maug, 2020). This has significantly expanded the already massive quantity of data collected and controlled by the Chinese government on its citizens.

Information collected through the Chinese surveillance systems as well as personal devices is used to train facial and voice recognition technology. Databases are synchronized in order to ensure that information on each individual is traceable. At the heart of this process is the Integrated Joint Operations Platform (IJOP), a digital platform which compresses all of the data available on an individual and uses AI to flag and police behaviors that have been classified as suspicious or hostile to the state (Yang, 2019). The IJOP has "three broad functions: [it] collects data, reports on suspicious activities or circumstances, and prompts investigative missions" (Nazish Dholakia & Maya Wang, 2019). The IJOP uses data points from gas stations, CCTV feeds, police checkpoints on the street, Wi-Fi sniffers, access-controlled areas, and normal activities which now require ID checks (such as taking a bus or picking up a package), and more recently QR code scans of the contact tracing app (Xiao Qiang, 2019; Mozur, et al, 2020). It integrates the compiled information with the other data available to produce comprehensive profiles on individuals (Alexandra Ma, 2019). These profiles include highly precise details such as religious and political affiliation, blood type, the frequency at which someone pumps gas, and their electricity usage. The algorithm then scans the data to search for markers of any of the 36 "person-types" that have been denoted as suspicious. If a marker is identified, a law-enforcement investigation is automatically triggered (Nazish Dholakia & Maya Wang, 2019). The IJOP app itself prompts the investigations and law-enforcement is dispatched to further probe into the alleged suspicious behavior or, in other cases, simply apprehend the citizen in question. Often, these person-types explicitly target ethnic and religious minorities such as Uighurs and other Turkic Muslims in the province of Xinjiang, who can then be sent to ideological detention camps for their "suspicious behavior" (Campbell, 2019b). In this way, the Chinese government uses big

data to preemptively halt or punish behaviors and individuals who do not align with the interests of the Chinese Communist Party. Through the use of massive amounts of data collected through surveillance technologies, particularly furthered by the COVID-19 contact tracing application, the Chinese government has the capacity to identify and oppress certain groups of their choosing with ease. The use of surveillance technology to facilitate government oppression, such as the targeting of Turkik Muslims, has long been regarded as a dystopian possibility, but it has come to fruition through China's actions in Xinjiang.

Surveillance Policy Expansion

Chinese expansions in technical capabilities for surveillance have been enhanced by policy measures under Xi Jinping. At the beginning of his presidency in 2012, President Xi's administration implemented policies that increased the reach and capability of the surveillance systems, such as requiring internet and social media users to register their accounts under their real name and ensuring that private platforms enforce censorship measures and report offending posts to the government (Xiao Qiang, 2019). As a result of President Xi's policies, Chinese high-tech products, platforms, and enterprises, such as the popular WeChat, Alipay Health Code (new contact tracing app) and Alibaba, now work closely with the Chinese government to censor and surveil. Further, these platforms and products with their embedded surveillance systems are also exported to other countries. Consequently, this exportation expands the reach of the Chinese government's surveillance network and its capacity for technological espionage, as those products are used and implemented in other states. (Polyakova et al, 2019).

The Chinese administration has also introduced prison sentences for internet-related offenses. In 2016, the government's first cybersecurity law went into effect, requiring internet companies to facilitate government control of data and mandating the storage of their users' personal data (Xiao Qiang, 2019). This law also prohibits individuals from establishing communication groups for anything which the government considers to be "criminal activities" or spreading rumors, particularly about the government (hrw.org, 2016). Such criminalization of online free speech through these policies is contrary to Article 19 of the Universal Declaration of Human Rights which protects freedom of expression under international law (*Universal Declaration of Human Rights*, 1948). The policies passed by the Chinese government are designed to strengthen its use of big data and surveillance for repression, not to protect the citizens or their data.

China has developed both the technical expertise and has instated the necessary legal and institutional frameworks to maintain a sophisticated, all-encompassing surveillance state. By expanding the use of digital technology, the government can control the country's massive population. Through this comprehensive surveillance system, the Chinese government promotes its interests through social media and other platforms while actively stifling any easily traceable dissent. The Chinese surveillance state is concerning as it ushers in an era of digitized totalitarianism. China is widely accepted as the most sophisticated example of absolute state control and surveillance pursued through digital means, but this phenomenon is also in its incipient stages in the United States.

United States

Surveillance Capacity Expansion

The United States has followed China's lead by massively expanding its use of surveillance in the past two decades. Following the September 11th, 2001 terrorist attacks in New York, the United States turned to increased surveillance in an effort to prevent similar attacks. After the attacks, polls showed popular support for these increased security measures for counterterrorism purposes (Yesil, 2006). Cameras were installed in airports, transport stations, monuments, and parks to deter criminals. The use of video surveillance, facial recognition, body-worn cameras, and other technologies for policing in the United States was largely accepted, as people prioritized safety over their privacy. As American society became more attached to the use of digital technologies such as social media, the US government expanded its surveillance methods to include other forms of technology, such as personal devices, like laptops, and internet usage. The US National Security Agency (NSA) has capitalized upon this modern reliance interconnected digital networks to collect information in bulk to be used against any "possible security threats". Despite the NSA's claim that the "NSA's SIGINT [Signals Intelligence] mission is specifically limited to gathering information about international terrorists and foreign powers, organizations, or persons", the Agency pursues this objective by gathering massive amounts of information on US citizens and foreign actors, and subsequently analyzing its pertinence to any security threat (nsa.gov, n.d.). The NSA tracks the whereabouts of citizens using their cellphones' connection to mobile networks and stores this location data in massive databases. The government claims that they only target and collect on specific individuals and that the bulk collection of data is purely incidental; however, target or not, all of the data is kept

("How the NSA Is Tracking People Right Now," n.d.). The NSA also uses "Co-Traveler Analytics" to develop targets by tracking and identifying devices which have been in close proximity to any known foreign intelligence target ("How the NSA Is Tracking People Right Now," n.d., April Glaser & Kurt Opsahl, n.d.). The NSA collects and stores metadata regarding digital communications (e.g. who spoke to whom, for how long, etc.) as well as the content of those communications (e.g. messages and images sent) to construct an accurate representation of existing social networks and behavioral patterns of people within the United States and abroad. In order to construct this representation effectively with the massive quantity of collected information, the NSA uses contact chaining, "a sophisticated form of analysis that looks for hidden, indirect relationships in very large data sets" (Gellman, 2020). Contact chaining has allowed the NSA to develop a comprehensive map encompassing the possible links between every person it surveils, which is constantly updated to create a live social graph of the United States (Gellman, 2020).

Though the fear following 9/11 prompted citizens to accept increased surveillance, current popular opinion opposes the US government's massive collection and usage of data. According to a report by Pew Research Center, a majority of Americans feel that the risks of data collection outweigh the benefits and are concerned about the use of their data, but feel that it is impossible to go through daily life without the government collecting more of their data (Auxier et al., 2019). Despite the disapproval of citizens, the United States continues its development of surveillance and technologies for policing. Some of these technologies, such as automation of records management or computer-aided dispatch, help increase the efficacy of existing policing strategies without major changes to the strategies themselves (Strom, 2016); however, the

integration of more surveillance and facial recognition into policing being explored by the United States could have catastrophic results. Devices such as body-worn cameras have already been widely adopted by law-enforcement. The addition of facial recognition to these devices could allow citizens' faces to be run against criminal databases in real time so they could be apprehended (Doffman, 2019). Experts and scholars warn of the ethical and practical dangers of implementing facial recognition technology in these ways. Such measures would further violate citizens' privacy and would adversely impact women and people of color, due to algorithmic biases within these technologies (McCarthy, 2018, Bass, 2018). This is an example in which irresponsible usage of data technology could lead to discrimination without necessary regulation addressing the way it could be discriminatory. The United States has not reached China's level of sophistication with these methods, but its commitment to digital surveillance and its exploration of facial recognition imply that it is following China's lead in adopting these technologies for its own uses. Moreover, the US has also instituted policies that have enabled the usage of the above surveillance technologies and have eroded foundational privacy protections found in the constitution and other legal frameworks.

Surveillance Policy Expansion

There are five primary data related laws limiting government surveillance that are fundamental to the US as a liberal democracy, including the 4th Amendment, The Privacy Act of 1974, The 1978 Right to Financial Privacy Act (RFPA), The Electronic Communications Privacy Act/Stored Communications Act of 1986 (ECPA) and The Health Insurance Portability and Accountability Act of 1996 (HIPAA). Such laws are meant to protect individuals and their

private data from undue government surveillance and differentiate a democratic state like the US from an authoritarian one like China. When examined, however, there are clear gaps in the legislation leaving room for wide interpretation, and ultimately enabling expanded surveillance. In addition, legislation such as the Patriot Act and the FISA Amendments Act are explicit steps towards China's legislative model to codify the ability to grossly surveil its citizens. In sum, though the right to privacy is included in the US Constitution and other US laws, the advent of new technologies and wide interpretation of the laws have enabled the above surveillance techniques and the latest legislation has in fact upheld it.

US Law Enabling Surveillance

The 4th Amendment, The Privacy Act of 1974, the RFPA, the ECPA, and HIPPA are often described as foundational privacy laws that protect and empower citizens in the US. However, the court's interpretation, the vague language and the exceptions included in the above listed laws has in practice enabled surveillance.

The 4th Amendment of the American Constitution protects US citizens from unreasonable search and seizure by the government. There has been significant legal debate about how the 4th Amendment applies to digital communications. *Smith v. Maryland* determined that phone records can be obtained by the police without a warrant, while *Carpenter v. United States* in 2018 determined that law enforcement cannot access historical location data from cellphone towers without a warrant (Carpenter v. United States, 2018). Further, in the 2010 US Court of Appeals case *United States v. Warshak*, the 6th circuit explicitly determined that the 4th Amendment does apply to email contents, meaning that individuals have a reasonable

expectation of privacy in their email communications, and law enforcement cannot access them without a warrant (United States v. Warshak, 2010). However, though the content of emails is protected, general information about with whom one is corresponding is not and can be accessed without a warrant (Kim, 2017). This is a gaping hole in the interpretation of the 4th Amendment and is not reconciled in the ECPA, which is discussed later, allowing for warrantless inquiry into whom individuals are communicating with.

The Privacy Act of 1974 was passed after the Watergate Scandal to address and curb illegal surveillance (ASPE, 2015). The act restricts the disclosure of personal information maintained by government agencies to individuals or other agencies. It also provides individuals access to what records are stored on them, and grants individuals the right to amend false records (justice.gov, 2020). Notably, however, the act exempts all law enforcement agencies, including the FBI, NSA, Justice Department, and the CIA. In this way, the Privacy Act does little to actually curb government surveillance by actual law enforcement agencies.

The RFPA is meant to provide protection against government surveillance on individual's banking records. The RFPA states that “no government authority may have access to or obtain copies of, or the information contained in the financial records of any customer from a financial institution unless the financial records are reasonably described” and either the customer authorizes the access or there is a subpoena, search warrant, or an appropriate written request from an authorized government authority. It also requires that a requesting federal government agency give the customer advance notice so that the customer can challenge the request before it takes place (justice.gov, 2020). And yet, the level of documentation that is required (i.e. a warrant, court order, or subpoena) to request information is often open to interpretation.

Moreover this law only governs disclosure to federal governments and does not apply to state or local governments. Further, another exception to required documentation is if the customer is a suspected terrorist or there is an emergency situation (justice.gov, 2016). Therefore, despite the seemingly tight restrictions on government access to financial records, the exceptions and gaps often leave financial information accessible by law enforcement without a warrant.

Arguably the most comprehensive piece of legislation intended to limit government access to private data is ECPA. When it was passed in 1986 it updated the Federal Wiretap Act of 1968 and included the Stored Communications Act (Justice Information Sharing, 2019). The act is meant to protect wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers by requiring warrants to access. It explicitly applies to email, telephone and locally stored data. The Supreme Court has also ruled that warrants are necessary to access physical phones (Riley v. California, 2015). In terms of wiretapping, the ECPA mandates a warrant or consent of at least one of the parties to listen in (Electronic Privacy Information Center). For email correspondences, warrants are usually required to access email *content* of an individual; The 4th amendment protects emails stored in a home computer, and the ECPA protects email content in transit and emails in remote locations. Upon examination, though, there are many exceptions where warrants are not required, and only court orders or subpoenas are needed.[2] Unopened emails stored for 180 days and opened emails stored in remote locations can actually be accessed with a subpoena (Electronic Privacy Information Center, n.d.). Additionally, draft emails can be accessed with only a court

[2] Court orders and subpoenas are far more accessible than warrants, with court orders only requiring that there are "specific and particular facts showing that there are reasonable grounds to believe" that the records requested are "relevant and material to an ongoing criminal investigation." (Cornell University, n.d., Georgia College, 2018).

order or a subpoena (Electronic Privacy Information Center, n.d.). If a government agency wants to access text messages from a cell-provider or social media content from the site itself, the same restrictions and exceptions for email apply (Myer, 2014). Lastly, Real time data phone data, such as correspondents, length of phone calls, and IP addresses, websites visited, cloud stored data that is not considered "communication" can be collected with a court order and historical data can be accessed with a subpoena (Myer, 2014, Electronic Privacy Information Center, n.d).

Lastly, HIPPA is a federal law that is meant to protect sensitive and private patient health information from being shared without the patient's knowledge or consent (CDC, 2018). However, this legislation does little to prevent government access to the data. Health entities may release information without a warrant to identify or locate a suspect; when a law enforcement official *requests* information about a victim; and if a health entity *believes* that protected health information is evidence of a crime (OCR, 2013). As the ACLU puts it, "law enforcement is entitled to your records simply by asserting that you are a suspect or the victim of a crime" (ACLU, n.d.).

The 4th Amendment, The Privacy Act of 1974, the RFPA, the ECPA, and HIPPA are often acclaimed for their privacy protections. Yet, under examination, they all provide significant leeway for law enforcement to practice surveillance with limited regulation. This leeway has set the groundwork for more explicit legislation that protects and incentivizes surveillance, in a striking comparison to the Chinese model.

US Law Explicitly Protecting Surveillance Methods

Similarly to China, the United States has also institutionalized protections for their use of their surveillance methods. Under the 4th Amendment, electronic surveillance (such as wiretapping, bugging, videotaping, or geolocation tracking) qualifies as a search and would require a warrant. However, legislation such as the Patriot Act and the FISA Amendments Act significantly expanded the NSA and FBI's ability to conduct large-scale warrantless digital surveillance, particularly on foreigners, but also on US citizens. Among other terrorism prevention measures, the Patriot Act allowed the US government to follow and digitally surveil suspected individuals without informing them of the investigation and facilitate the sharing of information between different government agencies (US Department of Justice, n.d.). Section 702 of FISA allows the US government to covertly collect internet and telephone communications of people both in the US and abroad for the gathering of "foreign intelligence information" ("Electronic Surveillance," n.d.). Though these legal measures only allow the collection of data on specified targets with probable cause, the government claims that doing this requires taking large quantities of data which may incidentally include that of unsuspected individuals (Human Rights Watch, 2017).

Like China, the US government also expands its surveillance methods by partnering with private companies, like internet service providers or digital platforms, such as AT&T and Facebook. In 2008, the Electronic Frontier Foundation, a non-profit defending digital privacy and free speech, filed a federal lawsuit against the US National Security Agency (NSA) on behalf of Carolyn Jewel and other AT&T users after an AT&T technician revealed that "AT&T was routing fiber optic cable communications into a secret room in its San Francisco facility

controlled by the NSA, allowing the government to gather the public's communications without court authorization" (PoKempner, 2019). This claim was further corroborated by many whistleblowers who confirmed that the NSA illegally collects digital communications of its own citizens. The US government has consistently blocked the lawsuit claiming that the charges cannot be confirmed without revealing state secrets, therefore, they should be dropped (Electronic Frontier Foundation, n.d.). The US government's evasive response to this lawsuit sets a dangerous legal precedent which is analogous to China's creation of policy to expand state control and decrease its accountability for illegal digital surveillance.

When examining the US government's use of and coordination with private company's data databases, the US government's current trajectory in regards to surveillance is exposed. The US government uses National Security Letters (NSL) to retrieve information on citizens from companies in the financial, technology and internet services industry among others (Electronic Privacy Information Center, n.d.). NSLs are a tool used in investigations related to national security and allow agencies like the FBI to receive data on corporate companies' customers' use of their services "such as banking, telephone, and internet usage records" (Electronic Frontier Foundation, 2014). NSLs usually contain a gag order which prohibits the recipient of the NSL, the private company, from disclosing to their user that they have received one. Further, an NSL and the included gag order are only reviewed by a judge if the recipient files a legal challenge (Electronic Frontier Foundation, 2014; Electronic Privacy Information Center, n.d.). In other words, they are warrantless requests for personal data. Since the introduction of the Patriot Act in 2001 the use of NSLs has been largely expanded as the FBI was also granted the right to issue

them (Electronic Frontier Foundation, 2014; Electronic Privacy Information Center, n.d.; Timberg & Barrett, 2019).

The practice of issuing NLSs poses a risk to civil liberties as well as the liberal democratic principles of the US. The most common critique is that NSLs are unconstitutional and unlawful. The Electronic Frontier Foundation argues that NSLs infringe on the First Amendment (right to free speech) by prohibiting companies to disclose when they have received an NSL (Electronic Frontier Foundation, 2014; Whittaker, 2017). Several challenges have been brought against NSLs and the enclosed gag orders, and courts are not consistent in their ruling. In 2013, a federal judge declared the gag orders and NSLs unconstitutional due to the infringement of free speech and the violation of the separation of powers (Zetter, 2013). However, a different court found that the NSLs in this case were issued in accord with the procedures and substantive requirements for constitutional use of NSLs (*NATIONAL SECURITY LETTER, UNDER SEAL, Petitioner-Appellant, v. JEFFERSON B. SESSIONS III, Attorney General, Respondent-Appellee*, 2017).

The way agencies like the FBI are issuing NSLs is also controversial and has raised concerns. Per the FISA Amendments Act, agencies submitting NSLs are only allowed to request information on the *usage* of services by users, not the content of usage itself. This only includes, as advised by the Office of Legal Council under President George W. Bush, "basic subscriber information, including name, address, and toll billing records — information the phone companies compile in their everyday business" (McLaughlin, 2016). However, in 2014 in a report issued by the inspector general, it was found that the FBI had expanded what it was requesting from companies in NSLs, and that the FBI had underreported the use of NSLs to

congress (Zetter, 2012). The report described that the FBI had expanded the use of NSLs to include requesting content of emails and other communications and other personal information. According to Chris Soghoian, chief technologist at the American Civil Liberties Union, the FBI requests more information than permitted in the hope that smaller companies will comply due to their lack of resources or knowledge of the laws involved (McLaughlin, 2016). The misuse of investigative tools by the FBI in combination with the lack of transparency and judicial oversight has left citizens vulnerable to surveillance that violates liberal democratic principles like the 1st and 4th Amendment. In 2016, a case involving the web services provider Yahoo exposed this vulnerability.

2016 Yahoo Surveillance Case

In 2016, after having received a classified government directive, Yahoo conducted a sweeping search of customers' email accounts looking for a set of characters (Menn, 2016). Yahoo built a custom software program to scan emails in real time in transmission. This was the first known time a US internet company, under the direction of the US government, had done a non-targeted search in real time instead of scanning stored messages or limiting the search to a small number of accounts in real time (Wolf, 2016). Andrew Crocker, staff attorney with the Electronic Frontier Foundation, commented, "[it is] hard to see how the government justifies requiring Yahoo to search emails like that; there is no warrant that could possibly justify scanning all emails." (Wolf, 2016). Privacy activists were not the only ones who condemned the decision to comply with the request. Even Yahoo's Chief Information Officer resigned, explaining that the company made decisions that he found undermined users' security. Critique

was also directed at Yahoo because they chose not to fight the directive, which according to some FISA experts would have been possible. After further investigation, it was found that Yahoo executives chose to comply because they doubted the system in place to dispute the directive (Menn, 2016; Wolf, 2016). Though one of the most egregious examples of the abuse of NSLs, this is just one case among many where consumers' privacy was exploited for the advancement of the US government's surveillance agenda.

The Chinese government's coordination with private companies to surveil its citizens has led to its classification as a 'digital totalitarian state.' Moreover, as described, the Chinese government uses their surveillance system to target and persecute ethnic and religious minorities, such as Uighurs and other Turkic Muslims in the province of Xinjiang. This is perhaps the greatest misuse of surveillance that is furthered by government and corporate collaboration -- discriminatory targeting and human rights violation by means of coordinated excessive privacy exploitation.

The Yahoo case, with the breadth and controversial nature of the directive, the development of a custom surveillance software by a private company coordinating with the government, and the doubt in a system to dispute the directive, illustrates the US's dangerous trajectory towards Chinese surveillance practices. This case mirrors the coordination between China's government and WeChat, for example. US citizens rely not only on the government to protect their rights, to institute transparent policies, and to grant due process, but also rely on technology companies to follow those policies and protect them from unlawful surveillance by law enforcement. Both of these institutions are in a delicate balance to protect citizens and ensure

their rights. The Yahoo case is a complete breakdown of the balance and an erosion of basic privacy rights and due process.

Policy Recommendations

The US is on a clear trajectory towards the Chinese model of digital authoritarianism. In order to reverse this trajectory and instead secure and promote a stable counterpart to the Chinese paradigm of surveillance and control of citizens, the US needs to emerge as a leader in privacy protection and limit AI-enhanced government surveillance. Domestic policy must be bolstered and international advocacy and cooperation are required.

Domestic Policy

The two domestic policy recommendations we make in support of other established privacy advocates to this end are:

- To increase transparency
- To raise digital literacy

More transparency in government surveillance would empower citizens and help the US. gain credibility as an opposite digital leader to China on the international stage. There are two primary issues to address in regard to transparency: data collection and classification.

First is the issue of data collection. Several organizations like Human Rights Watch, the Brennan Center for Justice, and the Global Network Initiative have already called on the US. to be more transparent about and held accountable for how they are surveilling citizens (Sullivan,

2019; Toh, 2019; *Transparency & Oversight*, n.d.). Furthermore, many international organizations and committees, the OECD and the European Commission have likewise stated transparency as one of their key pillars and established principles to this end (High-Level Expert Group on Artificial Intelligence, 2019; OECD, 2019). In regards to domestic policy, the US should establish policy that ensures citizens have access to the personal data that is being collected, stored and analyzed by the government and are knowledgeable about what the algorithms are searching for, who is building the systems, and how their output is being used.

Second, government classification of information has also greatly hindered a more informed debate and limited the public's oversight over the government's use of surveillance technologies. Overclassification impedes accountability and transparency that reaches far into the private sector (Sullivan, 2019). Policy recommendations to this end include greater declassification and stricter rules on documenting why something is being classified, accompanied by regular audits to hold the respective actors accountable (Sullivan, 2019; *Transparency & Oversight*, n.d.).

Increasing transparency not only protects individuals' rights but also allows for assessment of the government's surveillance methods, aiding in upholding accountability. Further, transparency will help strengthen privacy-oriented legislation by exposing egregious oversteps of the fundamental right of privacy as described in the constitution. Finally, enacting more legislation prioritizing transparency could also differentiate the United States from the repression and secrecy sustained by the Chinese government.

The empowerment and protection of citizens should also be pursued through digital literacy. A 2019 study by the Pew Research Center found that 78% of Americans say that they understand very little or nothing about what the government does with the personal data it collects. It further found that only 3% of American adults say "they have 'a lot' of understanding of the current laws and regulations in place to protect their data privacy, with 63% saying they understand very little or not at all" (Auxier et al., 2019; Auxier & Rainie, 2019). To this end education and information dissemination plays a key role in giving the general public the tools to interact securely and consciously with technology. Gaining technical knowledge should be integrated into required curriculums (Heck et al., n.d.). The US government should invest money in education to ensure that citizens are informed enough to critically evaluate AI policy and usagee developments. It should be further promoted by government, corporations, and civil society through awareness campaigns funded by the government.

New domestic surveillance policy will be a comprehensive and long undertaking and citizens would benefit from a federal moratorium on the use of certain AI technologies; The idea being, so long as there is not a full understanding of a technology and how it works, it's implementation and use on citizens should not be allowed. Several calls on the US government to do this have been made, especially in the area of facial recognition and data collection (Chen, 2020; Vincent, 2020). The Electronic Privacy Information Center drafted a letter that was signed by 40 consumer, privacy and civil liberties organizations calling on the "Privacy and Civil Liberties Board ("PCLOB") to recommend to the President and the Secretary of Homeland Security the suspension of facial recognition systems, pending further review" (Chen, 2020; Electronic Privacy Information Center, 2020, p. 1). Further, the Facial Recognition and

Biometric Technology Moratorium Act of 2020 was recently proposed by US lawmakers. This act would "halt government use of facial recognition technology and other biometric surveillance tools at the federal level, and ban federal funds from being used by state and local law enforcement to purchase the technology" (Ng, 2020; *OTI Endorses Facial Recognition Technology Moratorium Bill*, 2020). Opponents of this bill argue that such blanket regulations will undermine its usage in areas where it is of utmost importance for national security (*Security Industry Association Strongly Opposes the Facial Recognition and Biometric Technology Moratorium Act Citing Immeasurable Benefits of the Proven Technology*, 2020). However, in spite of the strong opposition by organizations like the Security Industry association, several private companies, like IBM and Amazon have decided to put a temporary halt to the sale of their facial recognition software (Johnson, 2020). This reaction from such large and powerful private sector stakeholders is evidence that there exists a possibility and desire for regulation of this technology and highlights the need for such measures to be carried out at the federal level.

At the federal level, these calls have fallen on deaf ears. At the state level, however, some states, including California, New Hampshire, and Oregon as well as the city of Boston, have imposed bans on the use of facial recognition by police (Brooks, 2020; Jarmanning, 2020; Lee, 2019; Samsel, 2019). Despite progress on a state and municipal level, there are no federal laws on limiting the use of facial recognition (Ng, 2020).

International Advocacy and Cooperation

When considering international policy, it is of great importance that the US focuses on international cooperation by creating international regulatory and ethics frameworks in this policy area, in cooperation with other countries that are stakeholders in this area. The Chinese government has emerged as a leader in AI. It has set goals to expand their influence in the international political realm by exporting their technology and ideologies and participating in the shaping of international AI norms (Steckman, 2019). The Trump administration has shown a radically different position and has tumultuously navigated the creation of norms in this area with its characteristic distaste for international cooperation and organizations. The United States' disinterest in leading the creation of AI norms directly conflicts with American interests. If the US wants their values to be prominent on the international stage, participation in the forming of new policy norms is essential. The ubiquity of these technologies is only growing. American negligence to participate in its regulation will indubitably result in other stakeholders' interests taking priority in deciding how to use a technology that will change the most fundamental aspects of life. Furthermore, due to the international flow of data, international norms must be negotiated to ensure that when data is transferred to a different country, it is not misused. As one of the most influential and defining powers on the international stage, and a dominant player in the technology market, the US has the power to promote and create new norms as they relate to surveillance methods. Furthermore, US-based companies hold large amounts of data on foreign citizens, showing that their surveillance reach goes far beyond the United States (Lewis, 2019). Therefore, the US must take action to ensure that liberal democratic values are upheld, as it has done many times over. If the US chooses not to be part of the formation of international

frameworks, they will either have to adopt norms they themselves had no part in establishing or they will be isolated.

Conclusion

The evolution of surveillance methods and policies utilized by the US government bear a striking resemblance to the trajectory which led the Chinese government to become a discriminatory and oppressive surveillance regime. This road toward digital authoritarianism, though, is still in its incipient stages for the United States and can be corrected by new US legislation (or strengthening of existing laws) to increase transparency and promote digital literacy. Such legislation could differentiate the US from the Chinese state, allowing them to emerge as a credible actor when advocating for international frameworks. Without an unambiguous change in direction, however, the fundamental values of privacy and due process, upon which the American Constitution and other liberal democracies rest, will be gradually eroded and erased to a point of no return.

Sources

ACLU. (n.d.). FAQ on Government Access to Medical Records. https://www.aclu.org/other/faq-government-access-medical-records

ASPE. (2015, December 03). 1. The Privacy Act of 1974. https://aspe.hhs.gov/report/options-promoting-privacy-national-information-infrastructure/1-privacy-act-1974

Auxier, Brooke, and Lee Rainie. "Key Takeaways on Americans' Views about Privacy, Surveillance and Data-Sharing." *Pew Research Center* (blog), November 15, 2019. https://www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/.

Auxier, Brooke, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner. "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information." Pew Research Center, 2019.

Bass, Dina . (2018, December 12). Almost Everyone Involved in Facial Recognition Sees Problems. Bloomberg. https://www.bloomberg.com/news/articles/2018-12-12/almost-everyone-involved-in-facial-recognition-sees-problems

Brooks, Ryan. "Data Privacy Laws by State: The U.S. Approach to Privacy Protection." *Https://Blog.Netwrix.Com/* (blog), April 24, 2020. https://blog.netwrix.com/2019/08/27/data-privacy-laws-by-state-the-u-s-approach-to-privacy-protection/.

Campbell, Charlie. (2019a, November 21). What the Chinese Surveillance State Means for the Rest of the World. Time. https://time.com/5735411/china-surveillance-privacy-issues/

Campbell, Charlie. (2019b, November 25). Leaked Documents Claim to Reveal Internal Protocols for China's Muslim Detention Camps. Time. https://time.com/5738401/xinjiang-uighur-muslim-camps-china-cables/

Carpenter v. United States, 585 U.S. (2018)

CDC. (2018, September 14). Health Insurance Portability and Accountability Act of 1996 (HIPAA). https://www.cdc.gov/phlp/publications/topic/hipaa.html

Chen, Angela. "40 Groups Have Called for a US Moratorium on Facial Recognition Technology | MIT Technology Review," January 27, 2020. https://www.technologyreview.com/2020/01/27/276067/facial-recognition-clearview-ai-epic-privacy-moratorium-surveillance/.

China: Abusive Cybersecurity Law Set to be Passed. (2016, November 6). Human Rights Watch. https://www.hrw.org/news/2016/11/06/china-abusive-cybersecurity-law-set-be-passed#

China: Big Data Fuels Crackdown in Minority Region. (2018, February 26). Human Rights Watch. https://www.hrw.org/news/2018/02/26/china-big-data-fuels-crackdown-minority-region

Cornell University. (n.d.). 18 U.S. Code § 2703 - Required disclosure of customer communications or records. https://www.law.cornell.edu/uscode/text/18/2703

Court of Justice of the European Union. "The Court of Justice Invalidates Decision 2016/1250 on the Adequacy of the Protection Provided by the EU-US Data Protection Shield," July 16, 2020, 3.

Dholakia, Nazish , and Wang, Maya. (2019, May 1). China's "Big Brother" App [Interview]. https://www.hrw.org/news/2019/05/01/interview-chinas-big-brother-app

Doffman, Zac . (2019, January 10). Facial Recognition is Coming to Police Body-Worn Cameras in 2019. Forbes. https://www.forbes.com/sites/zakdoffman/2019/01/10/body-worn-2-0-how-iot-facial-recognition-is-set-to-change-frontline-policing/#25fd56731ff3

Electronic Frontier Foundation. "National Security Letters." Electronic Frontier Foundation. Accessed August 22, 2020. https://www.eff.org/issues/national-security-letters.

———. "National Security Letters: FAQ." Electronic Frontier Foundation, March 5, 2014. https://www.eff.org/issues/national-security-letters/faq.

Electronic Frontier Foundation. (n.d.). Jewel v. NSA. Eff.Org. https://www.eff.org/cases/jewel

Electronic Surveillance. (n.d.). Legal Information Institute. Cornell Law School. https://www.law.cornell.edu/wex/electronic_surveillance

Electronic Privacy Information Center. (n.d.). EPIC - Electronic Communications Privacy Act (ECPA). https://epic.org/privacy/ecpa/

Electronic Privacy Information Center. "EPIC - Max Schrems v. Data Protection Commissioner (CJEU - 'Safe Harbor')." Accessed August 6, 2020. https://epic.org/privacy/intl/schrems/.

———. "EPIC - National Security Letters." Accessed August 22, 2020. https://epic.org/privacy/nsl/.

———. "Letter to the Privacy and Civil Liberties Board ('PCLOB') to Recommend to the President and the Secretary of Homeland Security the Suspension of Facial Recognition Systems, Pending Further Review," January 27, 2020. https://epic.org/privacy/facerecognition/PCLOB-Letter-FRT-Suspension.pdf.

European Commission. "Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition - Two Years of Application of the General Data Protection Regulation." Communication from the Commission to the European Parliament and the Council. European Commission, June 24, 2020. https://ec.europa.eu/info/sites/info/files/1_en_act_part1_v6_1.pdf.

Feldstein, Steven . (2019). *The Road to Digital Unfreedom: How Artificial Intelligence is Reshaping Repression*. Journal of Democracy, 30(1), 40–52. https://doi.org/10.135

Georgia College. (2018, July 31). Subpoenas, Court Orders and Search Warrants. https://www.gcsu.edu/legalaffairs/subpoenas

Gellman, Barton. (2020, May 24). Inside the NSA's Secret Tool for Mapping Your Social Network. Wired. https://www.wired.com/story/inside-the-nsas-secret-tool-for-mapping-your-social-network/

Getchell, Michelle. "The United States and the United Nations." In *Oxford Research Encyclopedia of American History*, by Michelle Getchell. Oxford University Press, 2017. https://doi.org/10.1093/acrefore/9780199329175.013.497.

Glaser, April , and Opsahl, Kurt . (n.d.). Meet CO-TRAVELER: The NSA's Cell Phone Location Tracking Program. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2013/12/meet-co-traveler-nsas-cell-phone-location-tracking-program

Heck, Tamara, Sylvia Kullmann, and Luzian Weisel. "Information Literacy and Its Interplay with AI," n.d., 3.

High-Level Expert Group on Artificial Intelligence. "Ethics Guidelines for Trustworthy AI." European Commission, 2019. https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

How the NSA is Tracking People Right Now. (n.d.). The Washington Post. https://www.washingtonpost.com/apps/g/page/world/how-the-nsa-is-tracking-people-right-now/634/

Jarmanning, Ally. "Boston Lawmakers Vote To Ban Use Of Facial Recognition Technology By The City." NPR.org, June 24, 2020. https://www.npr.org/sections/live-updates-protests-for-racial-justice/2020/06/24/883107627/boston-lawmakers-vote-to-ban-use-of-facial-recognition-technology-by-the-city.

Johnson, Khari. "Amazon Imposes One-Year Moratorium on Police Use of Its Facial Recognition Technology." *VentureBeat* (blog), June 10, 2020. https://venturebeat.com/2020/06/10/amazon-imposes-one-year-moratorium-on-police-use-of-its-facial-recognition-technology/.

Justice Information Sharing. (2019, April 23). Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510-2523. https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285

Justice.org (2020, January 15). Privacy Act of 1974. https://www.justice.gov/opcl/privacy-act-1974

Justice.gov. (2016, December 20). DOJ Privacy Act Regulations. https://www.justice.gov/opcl/doj-privacy-act-regulations

Kim, J. (2017, June). Fourth Amendment. https://www.law.cornell.edu/wex/fourth_amendment

Kimber, Richard. "On Democracy." *Scandinavian Political Studies* 12, no. 3 (September 1989): 199–219. https://doi.org/10.1111/j.1467-9477.1989.tb00090.x.

Lee, Dave. "San Francisco Bans Facial Recognition in US First." *BBC News*, May 15, 2019, sec. Technology. https://www.bbc.com/news/technology-48276660.

Leibold, J. (2020). Surveillance in China's Xinjiang Region: Ethnic Sorting, Coercion, and Inducement. Journal of Contemporary China, 29(121), 46–60. https://doi.org/10.1080/10670564.2019.1621529

Lewis, James A. "Artificial Intelligence and China's Unstoppable Global Rise: A Skeptical Look." In *Artificial Intelligence, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives*, edited by Nicholas D. Wright, 98–105. Maxwell Air Force Base, Alabama: Air University Press, 2019.

Ma, Alexandra. (2019, May 11). China uses an intrusive surveillance app to track its Muslim minority, with technology that could be exported to the rest of the world. Here's how it works. Business Insider. https://www.businessinsider.com/how-ijop-works-china-surveillance-app-for-muslim-uighurs-2019-5

Mathews, Kristen J., and Courtney M. Bowman. "The California Consumer Privacy Act of 2018." Privacy Law Blog, July 13, 2018. https://privacylaw.proskauer.com/2018/07/articles/data-privacy-laws/the-california-consumer-privacy-act-of-2018/.

McCarthy, Kieren. (2018, August). America's Top-Maker of Cop Body Cameras Says Facial-Recog AI isn't Safe. The Register. https://www.theregister.co.uk/2018/08/09/body_cameras_face_recognition/

McLaughlin, Jenna. "FBI Kept Demanding Email Records Despite DOJ Saying It Needed a Warrant." *The Intercept* (blog), June 2, 2016. https://theintercept.com/2016/06/02/fbi-kept-demanding-email-records-despite-doj-saying-it-needed-a-warrant/.

———. "Tech Companies Fight Back After Years of Being Deluged With Secret FBI Requests." *The Intercept* (blog), June 21, 2016. https://theintercept.com/2016/06/21/tech-companies-fight-back-after-years-of-being-deluged-with-secret-fbi-requests/.

Menn, Joseph. "Exclusive: Yahoo Secretly Scanned Customer Emails for U.S. Intelligence - Sources." *Reuters*, October 5, 2016. https://www.reuters.com/article/us-yahoo-nsa-exclusive-idUSKCN1241YT.

Meyer, T. (2014, June 27). No Warrant, No Problem: How the Government Can Get Your Digital Data. https://www.propublica.org/article/no-warrant-no-problem-how-the-government-can-still-get-your-digital-data

NATIONAL SECURITY LETTER, UNDER SEAL, Petitioner-Appellant, v. JEFFERSON B. SESSIONS III, Attorney General, Respondent-Appellee (United States Court of Appeals, Ninth Circuit July 17, 2017).

Ng, Alfred. "Lawmakers Propose Indefinite Nationwide Ban on Police Use of Facial Recognition." CNET, June 25, 2020. https://www.cnet.com/news/lawmakers-propose-indefinite-nationwide-ban-on-police-use-of-facial-recognition/.

New America. "OTI Endorses Facial Recognition Technology Moratorium Bill," June 26, 2020. http://newamerica.org/oti/press-releases/oti-endorses-facial-recognition-technology-moratorium-bill/.

NSA.gov. (n.d.). What We Do- Signals Intelligence. National Security Agency Central Security Service. https://www.nsa.gov/what-we-do/signals-intelligence/

OECD. "Recommendation of the Council on Artificial Intelligence." OECD Legal Instruments. OECD Legal Instruments. OECD, May 22, 2019. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

OCR (2013, July 26). Summary of the HIPAA Privacy Rule. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

Pieke, F. N. (2012). The Communist Party and social management in China. China Information, 26(2), 149–165. https://doi.org/10.1177/0920203X12442864

PoKempner, Dinah . (2019, September 18). US Government Mass Surveillance Isn't 'Secret.' Human Rights Watch. https://www.hrw.org/news/2019/09/18/us-government-mass-surveillance-isnt-secret

Polyakova, Alina and Meserole, Chris. (2019). Exporting Digital Authoritarianism: The Russian and Chinese Models. The Brookings Institution. https://www.brookings.edu/research/exporting-digital-authoritarianism/

PRWeb. "Security Industry Association Strongly Opposes the Facial Recognition and Biometric Technology Moratorium Act Citing Immeasurable Benefits of the Proven Technology," June 26, 2020. https://www.prweb.com/releases/security_industry_association_strongly_opposes_the_facia

l_recognition_and_biometric_technology_moratorium_act_citing_immeasurable_benefits_of_the_proven_technology/prweb17223201.htm.

Q & A: US Warrantless Surveillance Under Section 702 of the Foreign Intelligence Surveillance Act. (2017, September 14). Human Rights Watch. https://www.hrw.org/news/2017/09/14/q-us-warrantless-surveillance-under-section-702-foreign-intelligence-surveillance

Qiang, Xiao. (2019). The Road to Digital Unfreedom: President Xi's Surveillance State. Journal of Democracy, 30(1), 53–67. https://doi.org/10.1353

Riley v. California, 573 US 373 (2014)

Roth, Kenneth , and Wang, Maya. (2019, August 16). *Data Leviathan: China's Burgeoning Surveillance State*. Human Rights Watch.

Samsel, Haley. "California Becomes Third State to Ban Facial Recognition Software in Police Body Cameras." Security Today, October 10, 2019. https://securitytoday.com/articles/2019/10/10/california-to-become-third-state-to-ban-facial-recognition-software-in-police-body-cameras.aspx.

Senate Committee on Foreign Relations. (2020). *The New Big Brother: China and Digital Authoritarianism*. US Senate.

Smith v. Maryland, 442 U.S. 735 (1979)

Steckman, Laura. "Pathways to Lead in Artificial Intelligence." In *Artificial Intelligence, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives*, edited by Nicholas D. Wright, 81–88. Maxwell Air Force Base, Alabama: Air University Press, 2019.

Strom, Kevin . (2016). *Research on the Impact of Technology on Policing Strategy in the 21st Century.* RTI International Police Executive Research Forum.

Sullivan, David. "Transparency, National Security, and Protecting Rights Online." *Global Network Initiative* (blog), January 29, 2019. https://globalnetworkinitiative.org/transparency-national-security-and-protecting-rights-online/.

Timberg, Craig, and Devlin Barrett. "Secretive FBI Demands for Information Go Far beyond Tech Companies, New Documents Reveal." *Washington Post*, September 20, 2019.

https://www.washingtonpost.com/technology/2019/09/20/secretive-fbi-demands-information-go-far-beyond-tech-companies-new-documents-reveal/.

Toh, Amos. "Rules for a New Surveillance Reality." Human Rights Watch, November 18, 2019. https://www.hrw.org/news/2019/11/18/rules-new-surveillance-reality.

United States v. Warshak - 631 F.3d 266 (6th Cir. 2010)

Universal Declaration of Human Rights. (1948). United Nations. https://www.un.org/en/universal-declaration-human-rights/#:~:text=Article%2019.,media%20and%20regardless%20of%20frontiers.

US Department of Justice. (n.d.). The USA Patriot Act:Preserving Life and Liberty. https://www.justice.gov/archive/ll/highlights.htm

Brennan Center for Justice. "Transparency & Oversight." Accessed June 29, 2020. https://www.brennancenter.org/issues/protect-liberty-security/transparency-oversight.

VanGrasstek, Craig. *The History and Future of the World Trade Organization*. World Trade Organisation, 2013. https://www.wto.org/english/res_e/booksp_e/historywto_e.pdf.

Vincent, Brandy. "Senators Call for a Moratorium on Government's Use of Facial Recognition." Nextgov.com, February 14, 2020. https://www.nextgov.com/emerging-tech/2020/02/senators-call-moratorium-governments-use-facial-recognition/163131/.

Walch, Kathleen. "AI Laws Are Coming." Forbes, February 20, 2020. https://www.forbes.com/sites/cognitiveworld/2020/02/20/ai-laws-are-coming/.

Walton, Greg . (2001). *China's golden shield: Corporations and the development of surveillance technology in the People's Republic of China.* https://books.google.com/books?hl=en&lr=&id=S9rP0A2q14UC&oi=fnd&pg=PA3&dq=chinese+government+surveillance&ots=LK4IntHI_l&sig=7b3zACZ_w9KUz6ofdZXkBCLNbdg#v=onepage&q&f=false

Whittaker, Zack. "FBI Uses 'National Security Letters' All the Time — but What Are They?" ZDNet, June 24, 2017. https://www.zdnet.com/article/national-security-letters-everything-you-need-to-know/.

Wolf, Nicky. "Yahoo 'Secretly Monitored Emails on Behalf of the US Government.'" the Guardian, October 5, 2016. http://www.theguardian.com/technology/2016/oct/04/yahoo-secret-email-program-nsa-fbi.

Yesil, B. (2006). WATCHING OURSELVES. Cultural Studies, 20(4–5), 400–416. https://doi.org/10.1080/09502380600708770

Yang, Yingshi , and Zhu, Julie. (2020, February 7). Coronavirus brings China's surveillance state out of the shadows. Reuters. https://www.reuters.com/article/us-china-health-surveillance/coronavirus-brings-chinas-surveillance-state-out-of-the-shadows-idUSKBN2011HO

Yuan Yang. (2019, December 10). The role of AI in China's crackdown on Uighurs. Financial Times.

Zetter, Kim. "Federal Judge Finds National Security Letters Unconstitutional, Bans Them | WIRED." Wired, March 15, 2013. https://www.wired.com/2013/03/nsl-found-unconstitutional/.

———. "Unknown Tech Company Defies FBI In Mystery Surveillance Case." *Wired*, March 14, 2012. https://www.wired.com/2012/03/mystery-nsl/.