Protecting the Right to Privacy: Mass Surveillance in Xinjiang

The rapid advancement of technology and biometric data collection not only is changing the way we live and interact with each other every day, but also has huge implications on how we think about privacy rights. State surveillance systems have been around since the totalitarian regimes of the early twentieth century, but the rising sophistication of technologies such as artificial intelligence, facial and voice recognition, and mobile tracking apps is making surveillance easier and more invasive than ever. Against this backdrop of a changing digital landscape, privacy rights become prone to abuse, especially by states. This raises the question: What restraints should we place on the power of states that collect and exploit personal data, and how do we ensure that states protect the privacy rights of its citizens?

In this paper, I will address this question and argue that international action is necessary in limiting the power of states that abuse privacy rights and in ensuring the universal human right of privacy to all people. Specifically, I will critique China’s state surveillance practices in Xinjiang through a human rights framework, examine how these practices constitute a violation of the right to privacy, and discuss potential remedies involving international intervention. I will first define relevant terms and evaluate existing definitions of “the right to privacy” and “surveillance.” Then, I will outline the extent of China’s violation of privacy rights in Xinjiang by providing concrete examples of the exploitation of data as a mechanism for discrimination and persecution of the ethnic Uyghur minority. Finally, I will look at insufficiencies in recent
global responses to the crisis and discuss further potential remedies that can be implemented on a national and international level to curb China in abusing privacy rights.

**Definition of Privacy and Surveillance**

Before discussing examples of violations of the right to privacy and practices of mass surveillance in Xinjiang, it is necessary to start with definitions. What is “the right to privacy?” What constitutes “surveillance?”

Article 12 of the UDHR states, “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.”

Here, the right to privacy is loosely defined and lumped together with a variety of other individual rights. This definition is a bit broad, as the meaning of “arbitrary interference” has drastically changed since the advent of new surveillance technologies.

The Office of the United Nations High Commissioner of Human Rights (OHCHR) offered a more updated and comprehensive definition in its 2018 report, titled *The Right to Privacy in the Digital Age*: “Privacy can be considered as the presumption that individuals should have an area of autonomous development, interaction and liberty, a ‘private sphere’ with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals.”

There are still several issues and points of ambiguity present in this definition. What is “excessive” intervention? While mass surveillance of an entire population such as the case in Xinjiang can certainly be considered excessive, the inclusion of this word seems to imply that

---

unsolicited intervention by other uninvited individuals that is of more limited forms is acceptable. The definition may therefore be more effective without the word “excessive.” Notably, this definition is explicit in specifying that privacy should be “free from State intervention,” which is at the center of the case study of mass surveillance in Xinjiang. But again, this definition is problematic in that it seems to be centered around the individual.

According to law professor Paul Bernal, privacy should not be portrayed as simply an individual right in opposition to a collective need for security, but as a right that relates to our functioning as a community. Especially in the context of state surveillance, the relationship between security and privacy is not a dichotomy. Surveillance impacts not just individual privacy but a broad spectrum of rights and freedoms that impact communities, such as the freedom of expression and prohibition of discrimination. Privacy acts as a gateway or guardian to these other collective human rights, and categorizing privacy as solely an individual right downplays the negative impact of surveillance on communities.

Prior Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression Frank La Rue echoed this point, stating, “States cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy. Privacy and freedom of expression are interlinked and mutually dependent; and infringement upon one can be both the cause and consequence of an infringement upon the other.” Thus, in this paper I will refrain from framing the right to privacy as solely an individual right and instead examine the impact of the violation of this right on communities.

---

I will also be using Professor of Sociology at Queen’s University David Lyon’s definition of surveillance: “The focused, systematic, and routine attention to personal details for the purposes of influence, management, protection, or direction.”4 Though the word “attention” is ambiguous, I will interpret it to mean that surveillance occurs not only when data are algorithmically analyzed, but when it is first gathered. The OHCHR stated in its report that, mass surveillance, despite some states claiming that it is a necessary tool to protect national security, is “not permissible under international human rights law,” and “the mere collection of data already affects the right to privacy.”5 The very existence of data creates the risk of abuse, and human rights efforts should focus on eliminating the mass collection of data. With these definitions in mind, we can better understand the context of ongoing mass surveillance practices in Xinjiang and their impact on the right to privacy of Uyghur communities.

Case Study: State Surveillance in Xinjiang

I. Evidence of Mass Surveillance

Since 2016, the Chinese government has subjected 13 million ethnic Uyghurs and other Turkic Muslims in Xinjiang to heightened repression in its “Strike Hard Against Violent Terrorism” campaign. Residents are kept under constant surveillance, often using advanced technology such as facial recognition, iris scanners, voice pattern analyzers, and license-plate cameras that track vehicles.6

The surveillance state pervades the daily lives of minority communities in the region, collecting biometric data and tracking behavior with the purported goal of targeting people who

---

display “terrorist elements.” In May of 2019, Human Rights Watch (HRW) released a report about the inner workings of a mass surveillance phone app used by police and officials in Xinjiang. The app allows authorities to sort and analyze data collected on residents and is a part of a larger system for collecting mass surveillance data in the region, called Integrated Joint Operations Platform (IJOP). HRW found that the data collected included residents’ religious atmosphere, political affiliations, and biodata. The app flags people who fit one of 36 suspicious “Person Types,” prompting officials to further investigate any deviances from normal behavior. It tracks data about residents by monitoring their phones, vehicles, and ID cards, even recording their use of electricity and gas stations. Officials are alerted when a phone goes off-grid, and those who are flagged as threatening may be questioned or detained in re-education camps. As HRW researcher Maya Wang put it, “Xinjiang police are using illegally gathered information about people’s completely lawful behavior – and using it against them.”

Further evidence of mass surveillance can be found in Xinjiang’s system of “grid-style social management,” which divides neighborhoods into zones overlooked by grid-captains and security officials who are responsible for ensuring stability. Xinjiang's capital Ürümqi has been divided into roughly 6,300 grids, and over a third of them have digital surveillance systems. As of March 2017, Xinjiang authorities have built 7,300 “convenience police stations” to monitor grids. This type of systematic monitoring of civilian communities is undoubtedly a breach of privacy rights facilitated by the Chinese state.

These practices have been confirmed by the more than 400 pages of internal government papers recently leaked to The New York Times by a party insider in mid-November 2019. Of

7 Ibid.
this includes 96 pages of President Xi Jinping’s internal speeches to officials calling for
“absolutely no mercy” against the Uyghurs and 161 pages containing directives and reports on
the surveillance and control of the Uyghur population in Xinjiang. These documents provide
confirmation of officials’ orders in monitoring residents in the region and evidence of the mass
violation of the right to privacy by the state.

Given that there are growing amounts of evidence of an expanding surveillance state in
Xinjiang, the international community has responded with concern, but current actions have had
muted impact as China refuses to acknowledge their human rights violations.

II. Violating Privacy Perpetuates Violations of Other Human Rights

Inherent in this system of mass data collection and the violation of privacy rights is the
discrimination against and persecution of minority ethnic communities. Of the “Person Types”
tracked by the IJOP app, targets include “those who did not socialize with neighbors, collected
money or materials for mosques with enthusiasm, or failed to participate in activities organized
by the local government or the Party.” Targeting and persecuting people on the basis of religion
runs contrary to Article 7 of the UDHR, which states that “all are equal before the law and are
entitled without any discrimination to equal protection of the law.” Thus, the violation of
privacy rights has made possible the State’s discrimination against the Uyghur population and
the violation of other basic rights.

---

10 Roth, Kenneth, and Maya Wang. “Data Leviathan.”
Mass surveillance has further facilitated systems of mass detentions in Xinjiang, as an 660,000 Uyghurs are estimated to be detained in re-education camps.\textsuperscript{12} In this sense, the state has weaponized personal data of the Uyghurs and has used it as a social control tool. According to Professor James Leibold at La Trobe University in Melbourne, mass surveillance in Xinjiang undermines social trust and enables the State to administer social sorting. Social sorting categorizes residents for the purposes of control management, entitlement, punishment, and protection.\textsuperscript{13} In Xinjiang, surveillance is being used as a tool to evaluate appropriate behavior and thought among citizens and to ultimately get them to follow state-defined norms. Implications of social sorting include reduced social mobilization by Uyghurs and other minorities and the rooting out of non-normative Chinese cultural and religious practices.

It becomes more evident than ever that the people of Xinjiang are in dire need of international intervention and protection, and the violation of the right to privacy is at the center of the Xinjiang crisis. In order to reduce discrimination and other human rights violations in Xinjiang, it is crucial to first ensure that mass surveillance and privacy rights violations come to an end. Surveillance and arbitrary data collection are tools that the State uses for social sorting, and the elimination of these tools is necessary for a resolution to the broader Xinjiang conflict.

\section*{III. National Security and the Right to Privacy}

According to the leaked internal Chinese documents, the Chinese State’s crackdown on Xinjiang can be traced back to 2014, when Uyghur militants stabbed more than 150 people at a train station in an organized terrorist attack. The documents compared the Chinese government’s

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{13}Leibold, James. “Surveillance in China’s Xinjiang Region.”
\end{itemize}
\end{footnotesize}
response to the attack to 9/11 in America, and President Xi said that a sweeping campaign of surveillance and intelligence was needed to ensure stability in Xinjiang and root out resistance in the Uyghur society. Xi insisted that new technology must be part of the solution, and collection of biometric data began in February of 2017.14

When the international community expressed concern about the issue at the UN in September, the Chinese delegation pushed back, claiming the policies were intended to fight terrorism and separatism, despite the lack of evidence of the existence of an organized terrorist movement in Xinjiang. The state initially went so far as to cover up its practices of mass surveillance and detention, denying that its re-education camps existed. When questioned by the UN in August 2018, China presented a positive image of the situation, claiming that residents of Xinjiang were very happy and even forcing them to sing national songs when under foreign investigation.15 China is unlikely to voluntarily acquiesce to international demands to eliminate its surveillance system in Xinjiang on its own, so it is evident that some form of international intervention is needed.

Inherent in the root of this issue is a conflict between national sovereignty and human rights. Is national security in any way a valid argument for justifying human rights violations? Counter-terrorism has long been used as political justification to suppress the Uyghur population, and officials cite “social stability and long-term security” as the local government’s bottom-line goals.16 While these intentions are legitimate, their delivery is extreme and has led to the violation of the human rights of an entire community.

---

Again, privacy should not be framed as an individual right that is dichotomous to security. In practice, surveillance can do harm to both privacy and security. In his book *Data and Goliath*, Bruce Schneier found, “Terrorist plots are different from the kind of commercial fraud that data mining has worked well in detecting, mostly because whereas fraud is common, terrorist attacks are very rare. This means that even highly accurate terrorism prediction systems will be so flooded with false alarms that they will be useless.”17 History also shows that excessive security measures can lower the level of trust and cooperation with authorities, which could damage rather than help security.18

Mass surveillance does not need to be the solution to countering terrorism. In order to arrive at more rights-respecting ways to counter terrorism than mass surveillance, China could perhaps benefit from the expertise and advising of UN Special Rapporteur on the promotion of human rights while countering terrorism. What may have started out as a measure to protect the safety of citizens has grown into a much larger problem that is doing far more harm than providing help to individuals in Xinjiang. When state regimes overstep in implementing national security systems that violate a multitude of rights, international human rights laws should take precedence, especially in the case of the crisis in Xinjiang. If states like China refuse to acknowledge any wrongdoing, international and humanitarian intervention is needed to resolve the issue.

**Global Response and Potential Remedies**

I. **Global Response to the Xinjiang Human Rights Crisis**

---

To stop violating the privacy rights of the Uyghur community, the Chinese government must immediately shut down surveillance systems and delete all existing data. Though privacy rights do not seem like a priority compared to other rights violations in Xinjiang, data on residents gives the state power to control people and carry out other rights violations.

So far, China has been unwilling to voluntarily remove its mass surveillance systems in Xinjiang, and international efforts have resulted in minimal progress. In July 2019, 22 countries – including France, Germany, and Japan – at the UN issued a joint statement urging China to end human rights violations against Uyghurs in Xinjiang, calling on China to cooperate with the UN high commissioner for human rights and allow UN experts access to the region. In retaliation, China presented a letter signed by 49 countries – including Cambodia, Pakistan, Saudi Arabia, and Cuba – supporting its actions in the region.19

The conflict is very much at a standstill on the international level, with evident divisiveness among nations; democratic nations are more inclined to be on the side of human rights, while nations heavily relying on economic and political relationships with China support its surveillance systems. In order for real progress for human rights on the international front to be made, the entire international community should be on the same page.

The U.S. has also acted in trying to resolve the human rights conflict, and in October 2019, the Senate passed the bipartisan Uygur Human Rights Policy Act, calling for sanctions targeting Chinese officials responsible for crackdowns in Xinjiang. The U.S. imposed visa restrictions on these Chinese officials and blacklisted two dozen Chinese companies linked to the abuses, including surveillance technology manufacturers and Xinjiang's public security bureau.20

---

By blocking Chinese companies from selling Chinese products in the U.S., the U.S. has sent a clear message to China about its stance on the Xinjiang issue, but it is still uncertain whether the economic impact in this single action is enough in resolving the conflict. For example, Hikvision and Dahua Technology are the world’s two largest security camera manufacturers, together supplying a third of the global market for surveillance equipment.\textsuperscript{21} With the Chinese government offering them $1.2 billion contracts for 11 large-scale surveillance projects across Xinjiang, the U.S.’s sanctions have limited effects since they only impact a handful of large companies. Therefore, while international statements by the UN and initial economic sanctions imposed by the U.S. are steps in the right direction, there is more to be done in resolving the crisis.

II. Proposed Strategies

a. Tightening Economic Sanctions

Tightening sanctions may add stress on China and serve the goal of creating a united front against China’s human rights violations, in turn sending a signal to other nations that the U.S. does not condone these human rights violations. By expanding the blacklist of Chinese companies involved in the violations and denying them access to U.S. markets, the U.S. can target smaller players economically. It can also update export control restrictions so that dual-use U.S. technology is not integrated into repressive technology abroad.\textsuperscript{22}

Furthermore, the current administration could come forward and call for U.S. companies and investors to agree to not purchase or invest in any technology involved in surveillance in

\textsuperscript{21} Ibid.
Xinjiang. Specifically, the U.S. government could develop some form of human rights due diligence guidance for these companies to eliminate investments in companies involved in repression in Xinjiang.

Beyond temporary restrictions that the U.S. government has already enacted, other activists call for passing a new U.S. law that completely prohibits the export of technology that can be used for surveillance to government end-users in China. The proposed law also includes legally banning the financing of, investing in or research and development for Chinese surveillance companies by U.S. citizens or corporation. The implications of creating such a law would strengthen the U.S.’s signal that it opposes the Xinjiang violations and administer tangible legal consequences for individuals and corporations who do not abide by it. To extend the effectiveness of economic sanctions, other countries around the world can follow in the U.S.’s footsteps and refuse to export and import repressive technology involved in surveillance in Xinjiang.

b. Supporting Human Rights Advocacy in Regional Bodies

Other calls to action include using the media on an international scale to publicly denounce China’s violations by collecting, declassifying, and publicizing intelligence about surveillance in Xinjiang. The stakes of the issue at hand are higher than ever as China grows in international influence. In fact, recent reports suggest China is exporting its surveillance technology to other countries. As there remains divisiveness among nations in support and in opposition of China, continuing to publicize China’s human rights violations in Xinjiang may

---


24 Lehr, Amy. “Responding to the Xinjiang Surveillance State-and Its Likely Progeny.”
pressure nations that initially sided with China, like Cambodia, to join a united effort in criticizing China’s surveillance systems.

As senior fellow at the Hudson Institute John Lee put it, “Although the U.S. and other countries are not able to directly affect developments in Xinjiang, the highlighting of the harsh treatment of Uyghurs by the U.S. will strengthen the resolve of countries to counter Beijing’s attempts to redefine ‘human rights’ as those rights held by a state or government rather than those residing in the individual.” Public pressure could thus encourage a united international front against China’s violations.

While faraway democratic nations like the U.S. have been vocal about opposing mass surveillance and human rights abuses in China, China has received very little pressure or public condemnation from its Central Asian neighbors, Muslim countries, or its other trading partners. Especially important in presenting a united international front in opposition to abuses in Xinjiang is pressing regional human rights organizations such as the Association of Southeast Asian Nations (ASEAN) to urge Southeast Asian nations to condemn China’s human rights abuses.

Southeast Asian countries have been reluctant to take a strong stance on China’s abuses due to economic ties. Moreover, the principle of non-interference in ASEAN holds that countries should respect the sovereignty of other countries and not interfere in their domestic affairs.25 However, in order to fully deal with regional problems such as the Xinjiang crisis, it is necessary for the organization speak out. ASEAN Parliamentarians for Human Rights Chairperson Charles Santiago said, “Indonesia and Malaysia, as Muslim-majority nations in the region, have the responsibility to be vocal in their condemnation of China's human rights abuses.” Thus,

---

neighboring countries, especially Muslim-majority countries, have the duty to uphold the rights of the Uyghur community and condemn China publicly.

c. Creating a New Agency to Implement Guidelines for Privacy Rights

Much of current strategy in addressing human rights violations in Xinjiang involve economic approaches administered by individual nations like the U.S. While sanctions such as visa restrictions and company blacklists can be effective on a macroeconomic scale, increased international and humanitarian efforts are also needed to hold China accountable. For more of the international sphere to be on the same page about privacy rights in Xinjiang, the creation of a new international advocacy organization is needed.

A longer-term strategy to combat practices of mass surveillance and violations of privacy rights in Xinjiang and beyond is to create an entirely new United Nations agency dedicated to protecting privacy rights in the digital age. While the UN appointed a Special Rapporteur on the Right to Privacy in 2015 and has demonstrated interest in this issue, there is a lack of an official agency dedicated to protecting and defining these rights. According to Privacy International, which was an initial advocate of the appointment of the Special Rapporteur, “There is an urgent need for authoritative interpretations of existing human rights laws as the gap between the recommendations of human rights bodies and the laws and practices of states is growing.” Privacy International has reported that UN human rights mechanisms have yet to develop comprehensive recommendations and guidelines on the right to privacy and that the Special Rapporteur has thus far offered little concrete guidance on the crisis in Xinjiang.26

---

This new agency can write and publish international guidelines and offer recommendations about privacy rights and surveillance, incorporating suggestions by international and regional bodies and experts. While the UN published guidelines in its 2018 report, *The Right to Privacy in the Digital Age*, this single set of recommendations is insufficient as digital rights are constantly changing as new technologies are being developed. A new agency focusing its efforts on promoting best practices for protecting privacy rights as the digital world changes would resolve this issue and create soft law for countries and corporations to follow.

In the case of Xinjiang, the creation of this agency would send a strong message to China and its supporting countries that mass surveillance is not acceptable. In this regard, this agency could specialize in assessing the situation in Xinjiang and offer guidelines for China to phase out mass surveillance systems and turn toward other methods of providing security. Providing a frequently revised, up-to-date legal toolkit for the international community surrounding privacy rights and condemning practices of mass surveillance would help in changing norms and increasing discourse surrounding privacy rights.

**Conclusion**

As technology advances, arguments over surveillance and privacy rights will remain critical for the foreseeable future. States must adapt in ensuring that the right to privacy is recognized, and international action is necessary in limiting the power of states that violate this right by collecting and exploiting personal data. While there is no perfect solution for correcting the human rights abuses involved in systems of mass surveillance in Xinjiang, several steps can

---

be made by the international community toward pressuring China into eliminating these systems; a few of these potential remedies include tightening sanctions, pressing regional bodies to speak out, and creating a new international agency to promote privacy rights. While a combination of these strategies would be most effective, tightening sanctions and pressuring neighboring countries would yield the most immediate results; a new international agency may take longer to establish but would create more lasting long-term benefits to protecting privacy rights. The stakes are high, and the international community must come together to react and respond to the situation in Xinjiang, as its implications on privacy rights and surveillance are important and far-reaching.
Bibliography


