Journal of Technology Law & Policy

Volume XXI – 2020-2021

ISSN 2164-800X (online)

DOI 10.5195/tlp.2021.240

http://tlp.law.pitt.edu

Big Data and "New Surveillance": Is International Regulation Feasible?

Leanne Winkels

Big Data and "New Surveillance": Is International Regulation Feasible?

Leanne Winkels*

I. INTRODUCTION

In an increasingly connected world where technology and information are easily accessible to the consumer, what, if anything, is being done to protect the information and identity of private individuals? Through the use of the internet and data that is accumulated from users' profiles, Governments and Corporations access and compile data sets on targeted groups and individuals "of interest" in an unprecedented manner.

The collection and analysis of data is a concern related to international human rights and international relations. It implicates issues of sovereignty and highlights the lack of international agreeance on how to address these issues and to protect private information.

A key area of concern is the right to privacy and how governments may be exploiting the collection of data from individuals to violate their right to privacy, and in some cases to commit serious human rights violations. I will first outline the policy and background of the use of Big Data in international human rights. Secondly, against this backdrop, I will look at the use of Big Data by Russia and by China. Third, I will analyze the proposed models for assessment and protection of human rights in conjunction with the critiques and suggestions made by scholars in this field. Finally, I will discuss the potential for an international system to be developed and implemented to both enable human rights monitoring using Big Data, while at the same time providing protections against violations of the right to privacy and other human rights laws.

II. POLICY AND BACKGROUND

In order to properly discuss and analyze the current framework, [or lack thereof], surrounding Big Data, requires a basic overview of how Big Data operates and what the current standpoints are on its use. First, how is Big Data currently understood and legislated on by governments and the international community?

* Leanne Winkels is a J.D. Candidate for the Class of 2021 at the University of Pittsburgh School of Law.

Volume XXI – 2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.240 ● http://tlp.law.pitt.edu

Big Data is a "gather in bulk, access in detail"[1] monitoring and compiling of information; it is a new surveillance system that is categorically different from traditional methods of surveillance and gathering information. As a result, a broad range of human rights are implicated in the use of Big Data as a surveillance tool.[2] Another term by which the same process is known, is "bulk communications data techniques," or "bulk data" which involves "the large-scale collection, retention and subsequent analysis of communications data . . . of which by nature, an exhaustive analysis of this highly dynamic area is problematic. Indeed, it is precisely these limitations that challenge the applicability of current human rights law tests."[3]

The understanding of Big Data can be broken down into three stages: the gathering and collecting of data; the automated analysis of data which includes algorithmic filtering; and the human examination of the results of that analysis of filtering.[4] The breakdown between these stages is where a split over semantics arises. The key question is when, or at what stage, does "surveillance" actually take place? The argument can be made that surveillance happens at the first stage—that the very act of gathering or collecting data is surveillance. Privacy advocates and some scholars will argue this point, focusing on the fact that individuals are constantly having their data collected—from cookies on websites they access or to their geolocation—which fundamentally impacts or changes the way that we behave, and this constitutes "surveillance." Others argue that surveillance does not take place until the third stage, where human involvement and analysis of the data occurs, and that it is the human element of viewing and analyzing the data that constitutes "surveillance."[5] This view enables the claim that the population is free from "mass surveillance" because the human element is introduced only after the data has been analyzed to determine, reveal, or surface, those individuals who may be of particular concern to the surveillant power.

Author Paul Bernal makes the argument that it is at the first stage, the collection or gathering of data, that the "rights-balancing exercise" should start.[6] Bernal points out that this new form of surveillance has human rights implications that surpass privacy concerns, claiming that Articles 6 the right to a fair trial, 8(1) the right to

---

[1] Paul Bernal, *Data Gathering, Surveillance and Human Rights: Recasting the Debate*, 1 J. OF CYBER POL'Y 243, 246 (2016).

[2] *Id.* at 247.

[3] Daragh Murray & Pete Fussey, *Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data*, 52 ISR. L. REV. 31, 31 (2019).

[4] Bernal, *supra* note 1, at 249.

[5] *Id.*

[6] *Id.* at 251.

Volume XXI – 2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.240 ● http://tlp.law.pitt.edu

respect for private and family life—which extends to protection of "his correspondence," 9 the right to freedom of thought, conscience and religion, 10 the right to freedom of expression, 11 the right to freedom of assembly and association, and 14 the prohibition against discrimination, of the European Convention on Human Rights (ECHR) are implicated by this new system.[7]

This new method of surveillance can uncover habits, preferences, and "to a reasonable probability religion, sexual preferences, political leanings and more . . . data gathering can therefore impact upon any aspect of a private life" and can expose those personal characteristics.[8] According to Bernal, this kind of profiling, through analysis of data collected, can bring Article 9 of the ECHR into play.[9] Article 9 implicates the right to freedom of thought, conscience, and religion, and may only be subject to limitations which are "prescribed by law and are necessary in a democratic society in the interests of public safety etc."[10] This right may be undermined by the use of the profiles compiled through the new surveillance system under Big Data. Additionally, the ability to analyse individual users' data, in the context of all of the data collected, facilitates the identification of "anonymous" users who may use software or practices to hide their identity. By analyzing their activity in the context of the larger pool of activity, patterns or overlaps can be identified.[11] While this may be beneficial to determining the network within which a potential threat to national security may come from, there is ample opportunity for this type of system to be abused to identify vulnerable members of minority groups, such as LGBTQ+ or members of marginalized or persecuted religious or ethnic groups.

As previously noted, an awareness of surveillance can affect one's behavior—"knowing one's online activities are subject to government interception and believing these surveillance practices are necessary for national security play important roles in influencing conformist behavior."[12] That influence, Stoycheff concludes, "is in effect a chilling of speech, particularly of minority opinion."[13] Surveillance can be used to identify those with a minority opinion (cultural, political, religious, etc.) and can be used to prevent them from accessing information. When

---

[7] *Id.* at 252; *see also* European Convention on Human Rights, arts. 6, 8–11, 14, Mar. 9, 1953, E.T.S. No. 005.

[8] Bernal, *supra* note 1, at 253.

[9] *Id.*

[10] European Convention on Human Rights, arts. 6, 8–11, 14, Mar. 9, 1953, E.T.S. No. 005 [hereinafter ECHR].

[11] Murray & Fussey, *supra* note 3, at 39.

[12] Elizabeth Stoycheff, *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, 93 JOURNALISM & MASS COMMC'N. Q. 296, 297 (2016).

[13] *Id.* at 297–98.

Volume XXI – 2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.240 ● http://tlp.law.pitt.edu

considered in conjunction with geolocation data—which enables authorities to physically locate individuals and potentially those wishing to assemble—this chilling effect on speech and minority opinion becomes that much more severe. Put simply:

> In the context of surveillance, a chilling effect is said to arise when individuals refrain from engaging in certain forms of activity because of the perceived consequences if that activity is observed. Any chilling effect immediately brings into play rights such as freedom of expression, freedom of association and freedom of assembly, as it will impact upon the ability of individuals to freely access information, to develop their understanding of specific issues, to engage in communication—or meet—with particular individuals or organisations, and so on.[14]

According to the International Lesbian, Gay, Bisexual, Trans and Intersex Association (ILGA), 72 countries prohibit same-sex relations.[15] Surveillance technologies give governments the ability to "out" individuals. They know where people sleep at night, and with whom. The potential for lives to be destroyed is very great, indeed.[16]

The new surveillance can not only enable discrimination, it may also automate it by controlling decisions and options available to a person on the basis of the profile built through collecting that person's data. The person involved, whose decisions and options are being controlled, may never know what is happening.[17] As noted above, this implicates most clearly, Article 10, and 14 of ECHR, by impeding an individual's ability to "receive and impart information and ideas without interference" (Art. 10), and the prohibition against discrimination "on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, etc." (Art. 14).[18] A dangerous system may be created where individuals who belong to a minority group may be unintentionally exposing themselves to the risk of being targeted via surveillance, simply by accessing the internet. There is a large opportunity for this information to

[14] Murray & Fussey, *supra* note 3, at 43–44.

[15] Aengus Carroll & Lucas Ramon Mendos, STATE SPONSORED HOMOPHOBIA, A WORLD SURVEY OF SEXUAL ORIENTATION LAWS: CRIMINALISATION, PROTECTION, AND RECOGNITION 8 (12th ed. 2017), https://ilga.org/downloads/2017/ ILGA_State_Sponsored_Homophobia_2017_WEB.pdf.

[16] Andrew Thompson, *How Governments use Big Data to Violate Human Rights*, THE INT'L F. FOR RESPONSIBLE MEDIA BLOG (Jan. 20, 2019), https://inforrm.org/2019/01/20/how-governments-use-big-data-to-violate-human-rights-andrew-thompson/.

[17] Bernal, *supra* note 1, at 257–58.

[18] ECHR, *supra* note 10, at arts. 10, 14.

Volume XXI – 2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.240 ● http://tlp.law.pitt.edu

be exploited and used to track down and expose vulnerable members of minority groups (i.e., LGBTQ+ and religious minority groups).

Despite this doom and gloom approach to the issues that Big Data and surveillance creates, there is value to the information that Big Data provides, and the way that it can assist in preventing attacks, human rights abuses, and even protecting information and data. Amnesty International and other human rights groups have adapted to the use of Big Data and developed an analytical system which can help to prevent human trafficking and can be used to prevent or pinpoint other human rights abuses. Bulk communications data can be analyzed to identify suspicious patterns of behaviour, using a more proactive form of analysis individuals and devices "worthy of further investigation" can be revealed.[19] Data retention is beneficial for solving and preventing crimes, and for speedier investigations.[20] This can be used to create a profile on individuals or groups that may pose a threat to public safety or national security and enable preventative measures to be taken before an act is carried out.

However, this use of data as well as the "new surveillance" use of data collection does not take place in a vacuum. They raise issues of sovereignty as well as issues caused by a lack of an established framework. Without an such framework in both approaches, Big Data can take place and be monitored. Finally, preventing abuses needs to be addressed under each approach.

III. Country Studies

Data surveillance is currently happening all over the world, including with Russia's collection of information on LGBTQ+ populations and with China's campaign against Uyghur Muslims. This portion of the paper will analyse and compare the situations in Russia and China and look at how the uninhibited access to data and surveillance is enabling the perpetration of these actions against targeted groups.

A. Russia and LGBTQ+

June 30, 2014, President Putin signed a federal anti-LGBTQ+ propaganda law making it illegal to disseminate propaganda, defined as: "[The] distribution of information that is aimed at the formation among minors of non-traditional sexual attitudes, attractiveness or non-traditional sexual relations, misperceptions of the social equivalence of a traditional and non-traditional sexual relations, or enforcing

[19] Murray & Fussey, *supra* note 3, at 38.

[20] *Id.* at 40.

Volume XXI – 2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.240 ● http://tlp.law.pitt.edu

information about non-traditional sexual relations that evokes interest to such relations."[21]

This anti-propaganda law specifically targets the sharing of any information regarding LGBTQ+ identities and orientations, making the sharing of any information about such identities an illegal act.[22] This law has had varied consequences. On the one hand there has been push-back from the international community and NGOs supporting LGBTQ+ rights. On the other, this categorization of LGBT+ as illegal has led to greater prosecution and attacks against the LGBTQ+ community.[23] The further classification of an entire group of people as taboo and their identities as something that is illegal to discuss, has dire legal consequences as well. "Legally LGBTQ+ people are barely recognized as a social group, that is why crimes of violence cannot be classified as hate crimes and a motive of hostility cannot be recognized as aggravating circumstances."[24]

How is this treatment of the LGBTQ+ community by the state implicating Big Data? There have been multiple credible reports of "purges" of LGBTQ+ people in 2017 in the Chechen Republic.[25] Stories of the violence confirm that the threats and actions against LGBTQ+ people were based solely on their belonging to the LGBTQ+ community.[26] "[A] number of offences has increased objectively since traditional political discourse is cultivating people's homophobia that allows aggressors to get support, impunity and a free hand to demonstrate their negative attitude towards LGBTQ+ people."[27]

The Russian Government's law enforcement agencies are able to require that companies, which the agency adds to a register, must hand over their consumer data

---

[21] *No Support: Russia's "Gay Propaganda" Law Imperils LGBT Youth*, HUMAN RIGHTS WATCH, https://www.hrw.org/report/2018/12/11/no-support/russias-gay-propaganda-law-imperils-lgbt-youth#page (last visited Feb. 22, 2020).

[22] *Id.*

[23] *Id.*

[24] *Monitoring of Discrimination and Violence Based on Sexual Orientation and Gender Identity in Russia in 2016–2017*, RUSSIAN LGBT NETWORK (2018), https://lgbtnet.org/sites/default/files/discrimination.pdf.

[25] Adam Taylor, *Ramzan Kadyrov Says There Are No Gay Men in Chechnya—and if there Are Any, They Should Move to Canada*, WASH. POST, July 15 2017, https://www.washingtonpost.com/news/worldviews/wp/2017/07/15/ramzan-kadyrov-says-there-are-no-gay-men-in-chechnya-and-if-there-are-any-they-should-move-to-canada/; *see also Monitoring of Discrimination and Violence Based on Sexual Orientation and Gender Identity in Russia in 2016–2017*, *supra* note 24 (reporting of discrimination and violence against LGBT people in 2016–2017).

[26] *Monitoring of Discrimination and Violence Based on Sexual Orientation and Gender Identity in Russia in 2016–2017?*, *supra* note 24.

[27] *Id.*

Volume XXI – 2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.240 ● http://tlp.law.pitt.edu

to the government agency on demand.[28] If a company refuses to comply, the agency can block that company from having access to the Russian networks.[29] "Many popular home-grown email, messaging and social media websites are already on the Russian register."[30] Thus, the Russian government has access to the data of anyone who uses these websites, and can require that data at any point and for any reason.

In 2019, Tinder was added to such a register, and the Russian agency demanded that the company hand over its user data.[31] Tinder was not already on a register because it is a foreign company. If Tinder wants to continue to have access to the "market" in Russia, then it must comply with the agency, or risk being blocked from having access to Russia. If Tinder does comply with this demand, the repercussions would be potentially devastating. Government officials, such as the leader of the Chechen Republic could have access to data that would enable them to track down LGBTQ+ citizens.[32] This is a very real concern, as the 2017 purges demonstrate the open hostility of the government and what such a government is capable of. These purges, where individuals suspected of being LGBTQ+ were detained and tortured by those acting on behalf of the government, were addressed by Kadyrov, the Chechen leader, as not happening because "there are no gay men in Chechnya."[33] This outright denial of the existence of a group of people, coupled with the actions taken to silence and oppress them, demonstrate that if Tinder were to comply with this demand, it would be putting LGBTQ+ people at risk of further targeted persecution by the Russian government. One scholar said, "[i]t would be grossly, unjustifiably irresponsible for the brand to release information that could reveal swipers' sexual preferences to a government with a record of open hostility to its LGBTQ+ community."[34]

Not only is this "outing" by the government a gross violation of the right to privacy, it creates serious repercussions and risks for the outed individual to exist both in public as well as in private. An LGBTQ+ person is at risk of their family and

---

[28] Andrew Osborn, *Tinder, Despite Cooperation, Says It Hasn't Shared User Data with Russia Yet*, REUTERS (June 3, 2019, 12:19 PM), https://www.reuters.com/article/us-russia-tinder/russia-orders-tinder-dating-app-to-share-user-data-on-demand-idUSKCN1T425M.

[29] *Id.*

[30] *Id.*

[31] Rachel Altman, *Tinder's Data Sharing Endangers Russian LGBTQ Community*, USA TODAY, June 14, 2019, https://www.usatoday.com/story/opinion/2019/06/14/tinder-data-sharing-russia-endangers-lgbtq-community-column/1350929001/.

[32] *Id.*

[33] Taylor, *supra* note 25.

[34] Osborn, *supra* note 28.

Volume XXI – 2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.240 ● http://tlp.law.pitt.edu

friends attacking them for their sexuality or identity as a result of the "tribe" mentality and the potential for honor killings due to the shame of having an LGBTQ+ person in their family or tribe.[35] "Both authorities and local society apply pressure on [the] family to punish [LGBTQ+ people]."[36]

This use of data by the state, to target and track a community of people for the express purpose of attacking them, is a stark example of the potential for misuse of data by organizations. Unfettered access to data compilations on society, and on groups of people, creates a myriad of opportunities to exploit the information and expose these vulnerable communities to serious risk of violence. The fact that there is no check on the use of data, and that the Russian government is able to demand access to data from private corporations and entities, creates a serious concern for the potential for human rights violations. At this point, other than outrage from the international community, which has taken the form of protests and sanctions against the Russian government, no real action has taken place to curtail the treatment of the LGBTQ+ community in Russia by the government. More to the point, nothing has been done to address the use of data in this treatment, and how continued access to data poses a serious risk to marginalized and vulnerable populations. There is no international structure through which the Russian government's use of data can be held accountable and prevented.

B. China and Uyghur Muslims

The use of data surveillance in China has been incredibly prevalent specifically in regard to the use of surveillance measures to identify and track ethnic Muslims in the Xinjiang region of the country. This situation provides a direct look at the potential that surveillance through Big Data has through the human rights abuses and issues that this presents.

At a presentation on surveillance measures proposed or already in use in China, this slogan was displayed: "If someone exists, there will be traces, and if there are connections, there will be information."[37] Xinjiang China has become the "incubator" for implementing surveillance systems for tracking and identifying the population in that region and uses these systems to discriminate against minority groups, specifically members of Muslim ethnic groups. A *New York Times* investigation found that "China is in effect hard-wiring Xinjiang for segregated

---

[35] Lucas Ramón Mendos, *State-Sponsored Homophobia 2019*, ILGA WORLD, Mar. 2019, at 1, 156, https://ilga.org/downloads/ILGA_State_Sponsored_Homophobia_2019 _light.pdf.

[36] *Id.*

[37] Chris Buckley & Paul Mozur, *How China Uses High-Tech Surveillance to Subdue Minorities*, N.Y. TIMES (May 22, 2019), https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html.

Volume XXI – 2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.240 ● http://tlp.law.pitt.edu

surveillance, using an army of security personnel to compel ethnic minorities to submit to monitoring and data collection."[38] This monitoring is conducted by the C.E.T.C. platform, which police use via a mobile app to enter data into the system, tracking information such as people who may "have stopped using a smartphone, have begun avoiding the use of the front door . . . , or have refueled someone else's car."[39] The police use the app at "checkpoints" which serve as virtual fences. The system can be set to trigger an alarm every time that person tries to leave a neighborhood or enters a public place.[40]

State surveillance of the population has led to members of the targeted group attempting to distance themselves from others who could expose their identity, or who may be implicated or punished for a connection to them. Many Uyghurs living in Turkey do not have contact with their families in China for this reason. They have been deleted from social media and have no contact due to the fear of punishment from the Chinese authorities.[41]

Surveillance is not just an aspect of the online lives of people living in China, in the Xinjiang province this level of scrutiny is a part of everyday life. People travelling through the province or returning home from other areas of China are subjected to facial scanning by police when they arrive in the province.[42] There are surveillance devices located everywhere in public, "at the entrances to every supermarket, mall, and hospital."[43] According to a Dutch cybersecurity expert, there are police checkpoints and security cameras which have been, and continue to, record the location data of citizens in the Xinjiang province.[44] This surveillance includes a database of the names and identification information (birth dates, ID card numbers, photos, and employment details) of people who the government is monitoring.[45] The government maintains a tight net of surveillance over Uyghurs in China, and focusses this surveillance on the Xinjiang province due to its proximity to Turkey and its large

[38] *Id.*

[39] *Id.*

[40] *Id.* (The *New York Times* quoting Human Rights Watch.).

[41] Isobel Cockerell, *Inside China's Massive Surveillance Operation*, WIRED (May 9, 2019, 7:00 AM), https://www.wired.com/story/inside-chinas-massive-surveillance-operation/.

[42] *Id.*

[43] *Id.*

[44] Chris Baynes, *Chinese 'Muslim Tracker' Surveillance System Monitoring Movements of 2.5m People in Xinjiang*, THE INDEP. (Feb. 19, 2019), https://www.independent.co.uk/news/world/asia/china-uighur-muslim-crackdown-xinjiang-surveillance-tracking-sensenets-a8786076.html.

[45] *Id.*

Volume XXI – 2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.240 ● http://tlp.law.pitt.edu

population of Uyghurs.[46] In addition to the existing surveillance in the province, Human Rights Watch (HRW) has stated that they believe the Chinese Ministry of Public Security is working to pilot a system to monitor telephone conversations, further violating the right to privacy, and the protections which should be in place.[47]

C. Section III Conclusion

A key takeaway from this is that the government in China is exercising unprecedented control through surveillance and is using this information to monitor and target a specific ethnic group. There is no regulation in place to prevent the use of data and surveillance for such a purpose, no framework under which such exploitation of information is made illegal, or no location where states and private actors can be held accountable for their use of data. These same challenges are present in the situation in Russia. Currently there is no functioning framework that can be effectively used to address these concerns.

Self-regulation by states of their own collection and use of data is not enough to properly address a growing issue, and as evidenced by the above case studies, it is not working. Such self-regulation is even less effective in non-democratic states, where there is not an internal political check on the government's exercise of power. However, this does not mean that democratic states are much further ahead in preventing the exploitation of data by the government and by private actors. This facet of the issue has largely been overlooked by scholars and experts who seek to propose regulation models for the use of data. Most of these proposed models are for democratic states and do not take into consideration the application to non-democratic states.

IV. PROPOSED MODELS

Article 8 of the Charter of Fundamental Rights of the European Union sets out the foundation of data protection laws in the EU and establishes several key requirements concerning data processing activities.[48] This article states that "everyone has the right to the protection of personal data concerning [them]." And that "such data must be processed *fairly* for *specified purposes* and on the basis of

[46] Cockerell, *supra* note 41.

[47] *Id.*

[48] Krysztof Garstka, *Between Security and Data Protection: Searching for a Model of a Legal Big Data Surveillance Scheme within the European Union Data Protection Framework*, THE HUM. RTS., BIG DATA & TECH. PROJECT OCCASIONAL PAPER SERIES 1, 9 (2018), https://www.hrbdt.ac.uk/download/between-security-and-data-protection-searching-for-a-model-big-data-surveillance-scheme-within-the-european-union-data-protection-framework/.

Volume XXI – 2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.240 ● http://tlp.law.pitt.edu

the *consent of the person concerned or some other legitimate basis laid down by law*." (emphasis added).[49]

The codification of the UN Charter right to privacy, in the circumstances of Big Data, is an important step in influencing international law towards development of a policy for the use of data, and to create and implement an international framework for Big Data and surveillance.

A. For Assessment

1. Proportionality Assessment

The 2018 Annual Report from the Office of the High Chancellor for Human Rights (OHCHR) lays out how privacy, as a right, should be protected, and that if it is to be "limited" then such a limit is subject to a proportionality test or assessment:

> Privacy and other related rights shall only be limited when necessary. If a measure is necessary, a proportionality assessment shall be carried out following a three-step test: First, the measure which is taken must be potentially capable of realizing the aim. Secondly, the measure which is taken is required to reach the aim (in other words it must be the least intrusive measure). Thirdly, the measure which is taken must be proportionate "strictu sensu."[50]

Proportionality is one of the pillars of international law, both in international human rights law and international humanitarian law (law of armed conflicts). This concept requires that a balancing test be applied—before the act is undertaken, and with the information available to the individual at the time—to determine if the military advantage, or "gain" outweighs the casualties or "harm" caused.[51]

Here, the balancing is not only taking place in an armed conflict, but also in times of relative peace or stability. The harm contemplated is the violation of several recognized international human rights—undermining an individual's right to privacy, and several other rights which are related to or flow from privacy, such as the right to assembly, to freedom of thought and association etc.[52] In order to measure the gain from using Big Data, this balancing test should be undertaken on a case-by-case basis, and not generalized to include the potential gain the entire structure would provide. In such a circumstance, the gain may be the potential to reveal a member of

[49] Commission Proclamation on Charter of Fundamental Rights of the European Union, art. 8, 2000 O.J. (C 364) 1, 10 (Dec. 7, 2000).

[50] United Nations, *Human Rights Report 2018*, 1, 9 (2018), https://www.europarl.europa.eu/charter/pdf/text_en.pdf.

[51] For the purposes of this paper, the terms "gain" and "harm" will be used when discussing a proportionality assessment, rather than "military advantage" and "cost."

[52] ECHR, *supra* note 10.

Volume XXI – 2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.240 ● http://tlp.law.pitt.edu

a group planning an attack, which in the abstract may be presented as outweighing the collective right to the protection of privacy. Rather, the analysis should be particularized, as with case study of Russia, and the actions taken by the government agency towards requiring Tinder to release private data. There, a proportionality balancing test would show that the harm of violation of the right to privacy of people in general, but also of a specific and targeted minority group, outweighs any gain that the government may propose to receive from such information.

Similarly, in the case study of China, weighing the government's increased surveillance and tracking of citizens in the Xinjiang province violates the right to privacy, freedom of speech, and assembly as well as other related rights. The potential gain which the government may get from such surveillance is that the government can take preventative measures to stop any potential attacks or actions by rebels in the area. However, the question remains whether this level of harm is proportional to the "gain" the government receives. Arguably, it is not. The entire lives of a specific targeted minority group are catalogued and tracked based solely on their group characteristic of religion and ethnicity. This level of surveillance and complete violation of privacy is applied without discrimination to all members of the group, pre-emptively and without there needing to be an establishment of any kind of threshold activity to flag such an individual as being of interest to the government. Furthermore, there are multiple reports coming out about how the government in the Xinjiang province is compiling databases with this surveillance information and using them to detain Uyghurs. Such an unchecked use of the power of the state with the use of data is a serious challenge to human rights.

The consideration of the potential harms and gains associated with the protection of personal data should be undertaken with the above case studies in mind. The potential harms flowing from the use of data in such a way include: honor killings, torture, imprisonment, ostracization, and a lack of security. While the gain to be had from continued access to data by a state may be presented as the potential to address or prevent threats to national security, such gains must be considered on a case-by-case basis with the facts of the situation at hand as they arise. These cases should not be generalized due to a fear for allowing broad state action without any consequence or check on that power.

2. Human Rights Law assessment of legitimacy of surveillance measures

Under human rights law, for a surveillance measure to be considered legitimate, it must satisfy each prong of the following three-part test. First, it requires a domestic legal basis for surveillance to take place, such as legislation in place directly addressing or contemplating the use of surveillance. If such a basis exists, then it must be sufficient to protect against "arbitrary interference with the rights of

Volume XXI – 2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.240 ● http://tlp.law.pitt.edu

individuals."[53] This prong requires that the surveillance measure taken would be legal under that nation's legal framework, that the surveillance does not interfere arbitrarily with an individual's rights, and that the measures are targeted and specific enough to extract the necessary information without creating a legal issue surrounding other rights, or other individual's rights. The second prong requires that the surveillance to be undertaken has a legitimate aim (i.e., that it is intended to be used to prevent a threat, and not to "out" an individual). Once a sufficient legal basis and legitimate aim is found, the third prong requires an analysis of whether the surveillance is necessary in a democratic society (i.e., does the surveillance "answer a pressing social need and is it proportionate to the legitimate aim pursued?").[54]

This three-part test incorporates an aspect of the proportionality analysis discussed above. Whereby if the proposed surveillance measure meets the first two prongs of legality, it must still be a proportional measure to be undertaken in the circumstances. However, the third prong of this test is explicit in its applicability only to democratic nations and does not address these same concerns in a nation with another structure of government.

The proposed three-part test focuses on the legal basis of a democratic nation and applies the analysis of the proposed surveillance measure to that framework. This implicitly assumes that there would be a legal basis including legislation which addresses the use of surveillance, and a government in place which would respect or abide by such laws, and if it does not, that can be held accountable for such missteps.

"Evaluating the legal basis, and the quality of this legal basis, is dependent on the specific legal framework applicable in a given jurisdiction, while the uses of surveillance measures by intelligence and security services typically satisfy the legitimate aim test on the basis of protecting national security or public order."[55]

Furthermore, the concept of necessity as broached by this three-part test, looks to an analysis of the "utility of the benefit" from the proposed surveillance measure, as viewed through a "value-laden assessment of the worth of these distinct and potential uses."[56] In the case studies above this would mean looking at the utility of the benefit of the level of surveillance in the Xinjiang province, as providing the state with information, when considered in an assessment of the worth of the uses of that information both explicitly stated and those that are implied potential uses. In the

[53] Murray & Fussey, *supra* note 3, at 33.

[54] *Id.*

[55] *Id.*

[56] *Id.* at 37.

Volume XXI – 2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.240 ● http://tlp.law.pitt.edu

China case study, arguably the assessment would come out with the consideration being against the continued use of such extreme surveillance of the population.

B. For Protection of Human Rights

The human rights analysis of surveillance and bulk data focuses on whether the surveillance is "strictly necessary for the obtaining of vital intelligence in an individual operation."[57] This distinction in the approach to Big Data (bulk data), is an important one, creating a high threshold which must be met before surveillance measures can be used. In conjunction with the tests considered above, this distinction could also be scaled down to the individual claim level as well, where this threshold must be met, and a proportionality balancing test should be conducted before such measures are used.

> "In determining how human rights law could more effectively respond to bulk communications monitoring, four factors should be taken into account: (i) the extent of information that can be revealed by communications data; (ii) the extent to which harm associated with the retention of communications data affects other rights; (iii) the ease of analysing communications data; and (iv) the operational utility of bulk collection."[58]

This proposed test places heavy significance on the potential that such surveillance measures may have on what information is revealed and how that information may affect other rights. The test focuses on the actual and the probable effects of the proposed surveillance measures, and what the logical conclusions are of those measures. This enables a more holistic view of the use of data, rather than only looking at what the proposed purpose is of the surveillance measures.

V. CRITIQUES AND SUGGESTIONS

Many scholars in the fields of international relations, human rights, and data collection respectively have called attention to the issues addressed in this paper in various ways. In addition to scholarship on the issues, they also offer critiques and suggestions on models proposed to attempt to resolve these issues.

One of the critiques of the use of surveillance data in general is that it leads to harms outside of the specific area addressed. For example, evidence points to harms such as: "chilling effects; and shifting modes of suspicion—subdivided into issues of labelling and mental health."[59] Chilling effects include the self-policing of one's online activities based on the understanding that you may be under surveillance, in

[57] *Id.* at 41.

[58] *Id.* at 50.

[59] *Id.* at 43.

Volume XXI – 2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.240 ● http://tlp.law.pitt.edu

an attempt to prevent identification as a member of a group. An example of this would be the use of social media in China, where Uyghur's are deleting family members' information and policing what they say when texting or messaging on apps. This self-policing impacts their everyday lives and ties into the issues surrounding mental health as well as the fear for their own safety of those around them.

Another critique of the use of surveillance and the collection of bulk data is that there is a lack of discrimination in selecting whose information is collected. "Bulk monitoring elevates millions into the realm of the potentially suspicious in a narrowed field of enquiry. In such circumstances, suspicion does not precede data collection—surveillance is not initiated on the basis of 'reasonable suspicion.' Rather, it is generated by analysis of the data itself."[60] This is a key issue of the debate surrounding human rights and data analysis because the data collection and analysis *itself* creates the "suspicion" upon which the use of surveillance and monitoring is justified. This catch-22 situation enables governments and organizations to argue that access to and continued use of surveillance data is necessary to enable them to determine who could pose a threat to national security. However, such an argument far oversteps the proportionality assessment discussed above, with the actual harm—violations of the right to privacy, freedom of speech, and the effect of self-policing, among others—outweighing the potential gain of identifying *potential* threats. Rather than this approach to the use of data, a more finetuned and streamlined approach should be taken.

VI. CONCLUSION

The questions raised are: can an international system or framework be developed and effectively implemented that would enable the use of Big Data while protecting against violations of the rights of those being monitored? Additionally, would such a framework be able to operate across varied nation-states?

Many scholars agree that one avenue to create a legal framework or structure on the use of data is through utilising the system of creation of international norms, applicable as customary international law (and thus non-derogable unless the state had objected to the norm from its creation). With the creation of international norms and customary international law, the main issue is that this process is one that takes time. A norm is not developed overnight, and a norm does not become customary international law immediately. However, taking steps towards developing such a norm is a viable option for the international community and nation-states to consider.

[60] *Id.* at 47.

Volume XXI – 2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.240 ● http://tlp.law.pitt.edu

One such example is the Charter of Fundamental Rights of the European Union, a regional treaty which builds on the rights laid out in the UN Charter, and adapts them to be applied to Big Data.[61] While there is a lot more that can be said about the development of international customary law and international norms, that is not the focus of this paper, and will be dealt with in more generalized terms in order to further develop the question at issue here.[62]

In the interim, both as an option on its own, as well as in conjunction with the purpose of developing international customary laws, nation-states and other organizations (such as the UN, and treaty organizations) can create international monitoring bodies and treaty law. Such a proposed agreement would focus on the use of surveillance by nation-states within the borders and targeting the citizens of other nation-states, and should be expanded to include an agreement not to violate universally recognized human rights (which are non-derogable under the UN Charter for Human Rights and the Rome Statute which codify customary international law).

The steps that a multilateral agreement should set out to be followed, in preventing the abuse of access to data and surveillance, are as follows: First, the agreement should lay out that the object and purpose of the framework is to protect the rights of citizens in relation to the state, and of the sovereign nation-state in relation to other states, ensuring that there is no encroachment on these rights. Second, the agreement should establish a framework laying the boundaries of the agreement both as to the reach of the agreement and the boundaries that the nation-states must abide by. The boundaries of the reach of the agreement must be such that while monitoring the use of data by a state, the sovereignty of the state, and its right to protect itself are not imposed upon. The boundaries the nation-states must abide by are a more complex undertaking, which would need to be discussed and debated amongst the states implementing the agreement. Some recommendations of aspects to include are: that the agreement should establish an objective monitoring body which is tasked with reporting to the member-states the compliance with the requirements set out in the agreement by the members; and there must also be an enforcement mechanism available to the members, whether that is through arbitration, self-help, or adjudication—either by a neutral third party such as the ICJ, or by a body created from the agreement.

What does compliance with an international framework look like? As mentioned above, compliance would include respecting the rights of citizens and individuals when making use of data, as well as respecting the sovereignty of other

[61] Commission Proclamation on Charter of Fundamental Rights of the European Union, *supra* note 49.

[62] *See* Ashley Deeks, *An International Legal Framework for Surveillance*, 55 VA. J. OF INT'L L. 291, 319–42 (2015), https://www.ilsa.org/Jessup/Jessup16/Batch%202/DeeksLegalFramework.pdf.

Volume XXI – 2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.240 ● http://tlp.law.pitt.edu

nation-states. Beyond that, a framework should establish at what point does accessing data become "using" data: is it when the data is taken in bulk from the consumers and individuals; is it when the bulk data is sorted via algorithms into databases and data sets; or is it when the human element is introduced, analyzing the compilations of data? If it is the second option, of the compilation of data that defines "use," then the framework should create guidelines and rules surrounding this accessing of data and the compilation into data sets that are permissible under international law. For example, the use of data to compile databases on members of minority groups (ethnic, religious, sexual orientation, etc.), should be prohibited, unless such information is freely given by the individual (i.e., if there is a census and the individual voluntarily identifies themselves as a member of such a group). For the government to unilaterally develop such a data set of information without the consent of the targeted groups is dangerous and as is evident in the Russia and China case studies, can lead to discrimination, persecution, torture and threats of harm, including physical, psychological, economic, and social harms.

Volume XXI – 2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.240 ● http://tlp.law.pitt.edu