Seattle Journal of Technology, Environmental & Innovation Law

Volume 12 | Issue 1 Article 5

1-19-2022

Tech and Authoritarianism: How the People's Republic of China is Using Data to Control Hong Kong and Why The U.S. is Vulnerable

Bryce Neary
Seattle University School of Law

Tech and Authoritarianism: How the People's Republic of China is Using Data to Control Hong Kong and Why The U.S. is Vulnerable

Cover Page Footnote

The author is a 3L at Seattle University School of Law and wishes to thank his friends and family for their continued support.

Tech and Authoritarianism: How the People's Republic of China is Using Data to Control Hong Kong and Why The U.S. is Vulnerable

Bryce Neary[*]

I. INTRODUCTION

To protect civil liberties, one must retain a level of privacy that is exempt from government intervention. As we continue to intertwine our lives with technology, it has become increasingly important to advocate for privacy laws and protect Fourth Amendment rights. The accumulation of a person's online data may be extremely revealing. A government's access to this data is a backdoor into every potential "suspect" and "terrorist" who has ever made a suspicious Google search, social media post, or phone call.

In the United States, the law must continue to adapt to new technologies to preserve individual rights to privacy that people have fought to protect since the country's inception.[1] Currently, law enforcement agencies continue to use "terrorism" to justify violating American's Fourth Amendment right to privacy.[2] The recent ruling in *U.S. v. Moalin* further emphasizes courts are not willing to find Fourth Amendment violations if intelligence agencies produce a guilty party.[3] However, if the courts in the United States continue to turn a blind eye to the federal government's blatant violation of individuals' right to privacy, Americans risks exposure to an authoritarian fate similar to that of the People's Republic of China (PRC) under the Chinese Communist Party (CCP). As demonstrated in the recent "retaking" of Hong Kong, fundamental freedoms can be stolen from citizens in the blink of an eye.[4]

---

[*] The author is a 3L at Seattle University School of Law and wishes to thank his friends and family for their continued support.

[1] *See e.g.*, Olmstead v. United States, 277 U.S. 438, 466 (1928); U.S. CONST. amend. IV.

[2] *See* Timothy B. Lee, *Here's Everything we know about PRISM to Date*, THE WASH. POST WONKBLOG (June 12, 2013), http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/ [https://perma.cc/NR26-QY83].

[3] United States v. Moalin, 973 F.3d 977, 985 (9th Cir. 2020).

[4] Paul Mozur & Lin Qiqing, *Hong Kong Takes Symbolic Stand Against China's High-Tech Controls*, N.Y. TIMES (Oct. 3, 2019), https://www.nytimes.com/2019/10/03/technology/hong-kong-china-tech-surveillance.html [https://perma.cc/7YRM-AL8C].

The ruling in *Moalin* creates serious implications for privacy rights in the United States and lessons we can learn from Hong Kong's fight against PRC surveillance. In *Moalin*, the court held that mass data surveillance of Americans without probable cause is unconstitutional under the Fourth Amendment.[5] In its reasoning, the Ninth Circuit held that the Foreign Intelligence Surveillance Act (FISA) requires records to be relevant to a specific investigation rather than counterterrorism investigations generally.[6] This was a pivotal ruling because it answered many constitutional questions that arose when whistleblower Edward Snowden revealed that United States intelligence agencies commonly monitored United States citizens' private data.[7]

In comparison, the pro-democracy events in the formerly semi-autonomous territory of Hong Kong took a turn for the worse when the PRC used mass surveillance methods to suppress information, track down dissidents, and silence protests.[8] The loss of civil liberties in Hong Kong is, without privacy regulations and safeguards, the United States is ripe to follow a similar path.

As journalists, protestors, and pro-democracy advocates continue to be hunted down and arrested, Hong Kong has shown us that anti-government sentiment can be easily molded into "terrorist activities."[9] This situation has demonstrated why privacy is necessary to protect civil liberties. Without proper regulation, sweeping surveillance invites the potential abuse of government police power. While the United States operates under the guise of pure terrorism prevention, the PRC has made it clear that there will not be any tolerance for anything remotely resembling anti-government behavior.[10]

As technology continues to evolve and our data becomes more interconnected and accessible than ever, the surveillance methods outlawed in *Moalin* will become obsolete, and the law will be inadequate to protect American's privacy. This growing digital footprint will allow United States federal intelligence agencies to engage in surveillance activities those used to silence dissent and denigrate democracy in Hong Kong.[11]

This article will outline the recent Ninth Circuit ruling in *Moalin*, its implications on privacy rights in the United States, and the United States' law enforcement's justified use of surveillance methods to track down the

---

[5] *Moalin*, 973 F.3d, at 996.
[6] *Id.*
[7] *Cf.* Fred H. Cate & Beth E. Cate, *The Supreme Court and Info. Priv.*, INT'L PRIV. AND DATA LAW (Sept. 26, 2012), https://academic.oup.com/idpl/article/2/4/255/676934 [https://perma.cc/LES6-BU28] (Edward Snowden leaked information from within the NSA, which some believed to be a heinous violation of both U.S. citizens' and U.S. residents' Fourth Amendment Constitutional right to privacy).
[8] *National Security Law: Hong Kong rounds up 53 pro-democracy activists*, BBC NEWS (Jan. 6, 2021), https://www.bbc.com/news/world-asia-china-55555299 [https://perma.cc/HEB4-3NN3].
[9] *Id.*
[10] James D. Fry, *Privacy, Predictability and Internet Surveillance in the U.S. and China: Better the Devil You Know?*, 37 U. Pa. J. Int'l L. 419, 440-442 (2015).
[11] Charlie Warzel & Stuart A. Thompson, *They Stormed the Capitol. Their Apps Tracked Them.*, N.Y. TIMES (Feb. 5, 2021), https://www.nytimes.com/2021/02/05/opinion/capitol-attack-cellphone-data.html [https://perma.cc/7MUV-MAEK].

rioters who stormed the United States Capitol Building. The United States system will then be compared to current Chinese law and the ethical balancing test that must be used when analyzing Hong Kong's fight against PRC surveillance. Furthermore, a discussion of the thin line that separates a government's compelling interest to protect its citizens through surveillance, and the potential infringement of their fundamental rights to privacy will follow. Lastly, this article will analyze how the Chinese government's use of surveillance in Hong Kong has provided the United States with a road map to combat government surveillance in the coming years. While China's use of surveillance is well known, the United States still operates under the guise of terrorism prevention. The unique perspective taken here will discuss events that are currently unfolding. The Trump supporters who flooded the United States Capitol in January 2021 have only convoluted this topic, as law enforcement agencies' use of surveillance within the United States has become widely justified.[12] To conclude, the uprising in Hong Kong and the United States Capitol will be compared and discussed to highlight when a society deems the use of surveillance to be rational or necessary.

II. THE SNOWDEN LEAK

Edward Snowden's leak revealed that the dictum, "If you have nothing to hide, you have nothing to fear," is a presumption that may no longer be true in the United States.[13]On June 5th, 2013, a British newspaper, *The Guardian,* began publishing a series of articles disclosing highly classified aspects of certain National Security Agency electronic surveillance operations involving not only extensive collection of foreign communications, including internet traffic, but the collection of metadata associated with phone calls made by United States citizens.[14] The NSA internet surveillance program involved the targeting of foreign persons "reasonably believed to be outside the United States using broad surveillance information from popular U.S. tech companies servers.[15] These companies included Microsoft, Google, and Facebook, among others.[16] Unlike a domestic criminal investigation, "[t]he NSA is engaging in bulk collection absent any reasonable suspicion that the individuals, whose telephone information is being collected, are engaged in *any* wrongdoing. To the contrary, almost all of the information obtained will bear no relationship whatsoever to criminal activity."[17]

This program gives the government access to a compilation of information that could be incredibly revealing for even the most innocent Americans, such as internet search histories, e-mails, file transfers, and

[12] *Id.*
[13] Ewen Macaskill & Gabriel Dance, *The NSA Files: Decoded*, THE GUARDIAN (Nov. 1, 2013), https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 [https://perma.cc/3PN4-5399].
[14] *Id.*
[15] *See* Lee, *supra* note 2.
[16] *Id.*
[17] Laura K. Donohue, *Bulk Metadata Collection: Statutory and Const. Considerations,* 37 HARV J.L. & PUB. POL'Y 757, 869 (2014).

live chats.[18] These obtrusive practices are justified based on the invisible threats that loom in cyberspace.[19] Many modern terrorist groups operate using covert agents who disguise their online communications and movements with normal peacetime behaviors.[20] The NSA states that their broad use of internet surveillance protects against terrorism globally, hostile foreign governments, and the online trade of weapons and drugs.[21] However, the broad data collection methods used to combat these issues have proved to infringe on the rights of United States residents far removed from such operations.[22]

Edward Snowden and NSA contractor Booz Allen Hamilton leaked sensitive information from within the NSA in 2013.[23] When *The Guardian* revealed Snowden's identity, the United States government charged Snowden with "unauthorized communication of national defense information" and "willful communication of classified communications intelligence information to an unauthorized person," under the 1917 Espionage Act.[24] Snowden sought refuge in Hong Kong, and then in Russia, where he has been ever since.[25]

In addition to the exposure of the United States government's infringement on citizens' rights, it was revealed that intelligence agencies monitored the phone conversations of thirty-five world leaders.[26] NSA officials encouraged "senior officials in customer departments such as the White House, State Department, and Pentagon to share their rolodexes" of contacts so the Agency could add the phone numbers of leading foreign politicians to their surveillance systems.[27] For example, German Prime

---

[18] *See* Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps into User Data of Apple, Google and Others*, THE GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [https://perma.cc/T53S-7JFL] (reporting on the previously undisclosed PRISM system and including the reaction of representatives from Google and Apple).

[19] *NSA Cybersecurity*, NAT'L SEC. AGENCY CENT. SEC. SER., https://www.nsa.gov/Cybersecurity/Overview/ [https://perma.cc/5FB2-54FS].

[20] John Yoo, *The Legality of the National Security Agency's Bulk Data Surveillance Programs*, 37 HARV J.L. & PUB. POL'Y 901, 905 (2014).

[21] *NSA Cybersecurity*, *supra* note 19.

[22] *See, e.g.*, Donohue, *supra* note 17 at 849.

[23] Glenn Greenwald ET AL., *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, THE GUARDIAN (June 13, 2013, 9:00 AM), https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance [https://perma.cc/3R85-Q9X6]. *See also* Deb Riechman, *Costs of Snowden leak still mounting 5 years later*, THE ASSOCIATED PRESS (June 3, 2018), https://apnews.com/article/hi-state-wire-national-security-europe-russia-government-surveillance-797f390ee28b4bfbb0e1b13cfedf0593 [https://perma.cc/H39Z-AXDG].

[24] Peter Finn & Sari Horwitz, *U.S. charges Snowden with espionage*, THE WASH. POST (June 21, 2013), https://www.washingtonpost.com/world/national-security/us-charges-snowden-with-espionage/2013/06/21/507497d8-dab1-11e2-a016-92547bf094cc_story.html [https://perma.cc/H6PL-AZPX].

[25] *See* Macaskill & Dance, *supra* note 13.

[26] James Ball, *NSA Monitored Calls of 35 World Leaders after US Official Handed over Contacts*, THE GUARDIAN (Oct. 24, 2013), http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls [https://perma.cc/PD6U-YP7G] (reporting on Snowden's document claiming surveillance of the phone conversations of world leaders by the National Security Agency).

[27] *Id.*

Minister Angela Merkel's mobile phone was allegedly monitored for eleven years before Snowden's leak.[28]

However, some believe that Snowden's wanton disregard for United States intelligence agencies' mission makes him a traitor.[29] "[I]n espionage terminology, an agent is a person who provides information to an operative... The agent might not be aware that he or she is providing information to a foreign spy depending upon how the operative approaches an agent."[30] In Snowden's case, "the fact that he was not an agent of a foreign government does not change the fact that he intentionally committed espionage and treason."[31] After all, Snowden fled to Russia of all places, a country which likely benefitted from Snowden's disclosures. Keith Alexander, director of the NSA, said Snowden's disclosures caused "irreversible and significant damage" to the agency's foreign surveillance operations.[32] NSA officials say that foreign individuals or groups targeted for surveillance may now switch to more secure communication methods.[33] "When Osama bin Laden learned that the NSA was monitoring his satellite telephone, for example, he switched to messages by courier."[34] This raises the question, does the breach of U.S. citizens' personal data justify giving foreign operatives an advantage?

To summarize this essential background: Snowden believed that United States intelligence agencies were abusing their power and infringing upon people's private sphere without proper justification or oversight. Whether his actions were right or wrong is up to debate; however, there is no doubt that his actions sparked a conversation about privacy laws in the United States. Thus, it is important to understand what privacy rights that people in the United States enjoy based on its foundational doctrine and case law. The next section of this article will analyze the framework of legal principles intended to ground this discussion; subsequent sections will focus on the arguments used to justify its exploitation.

III. U.S. LEGAL BACKGROUND

United States intelligence agencies utilize their surveillance techniques under either national security or law enforcement

---

[28] According to Snowden, the NSA monitored Chancellor Merkel's mobile phone for 11 years, including the numbers called, duration and location (metadata) and the contents of her calls and text messages. *See* Derek Scally, *Dial M for Merkel: Angela's Next Move*, IRISH TIMES (Nov. 2, 2013), https://www.irishtimes.com/news/world/dial-m-for-merkel-angela-s-next-move-1.1580987 [https://perma.cc/VRW8-9RT4] (reporting that Merkel's phone was monitored for 11 years by the National Security Agency and what the implications for Germany were).

[29] Ira Winkler, *Snowden wasn't a Russian agent, but a traitor just the same*, The Hill (April 5, 2017, 12:45 PM), https://thehill.com/blogs/pundits-blog/homeland-security/327414-snowden-wasnt-a-russian-agent-but-a-traitor-just-the [https://perma.cc/Q5KH-CER2].

[30] *Id.*

[31] *Id.*

[32] Tom Gjelten, *The Effects of the Snowden Leaks Aren't What He Intended,* NPR (Sept. 30, 2013, 4:34 PM), https://www.npr.org/2013/09/20/224423159/the-effects-of-the-snowden-leaks-arent-what-he-intended [https://perma.cc/4EMF-ZN59].

[33] *Id.*

[34] *Id.*

justifications.[35] Although the two are generally analyzed under different frameworks, they are not mutually exclusive. This section will delineate the two frameworks and focus on the major cornerstones of U.S. law that upholds the privacy rights of American citizens. This article will discuss five cornerstones of American privacy law. First, this article will consider the Fourth Amendment of the Constitution; second, the Foreign Intelligence Service Act (FISA), to establish the foundation of modern surveillance policy; third, an analysis of the broad allowances created by the USA PATRIOT Act; fourth, the subsequent USA Freedom Act and its refinement of those policies; and finally, multiple examples of U.S. case law will be introduced to provide insight into direct challenges of privacy infringement.

Although there is no single comprehensive federal law that governs privacy law in the United States, the Fourth Amendment of the United States Constitution forms the basis of privacy protection:

The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[36]

It should be noted, "all constitutional rights—whether to speak freely, confront one's accusers, be tried by a jury of one's peers—regulate the public, but not the private, sector. In the absence of state action, therefore, constitutional rights are not implicated in questions surrounding privacy."[37] Thus, in the absence of state interest, constitutional rights are not necessarily invoked in questions surrounding privacy.[38]

A. The Foreign Intelligence Service Act

To United States intelligence agencies' power, it is necessary to revert to the inception of FISA. In response to President Nixon's usage of federal resources, which included utilizing intelligence and law enforcement agencies to spy on a politically motivated opposition, President Carter signed the FISA into law in May of 1978.[39] FISA created a framework for the modern surveillance justifications that federal agencies still rely on today.[40] FISA allows the United States government to engage in electronic surveillance and physical searches to obtain "foreign intelligence information" that generally includes evidence of

[35] *NSA Cybersecurity*, *supra* note 19.
[36] U.S. CONST. amend. IV.
[37] "Although state action is usually found when the state acts toward a private person, the Supreme Court has also found state action when the state affords a legal right to one private party which impinges on the constitutional rights of another, see *New York Times Co. v Sullivan*, 376 U.S. 264, 265 (1964), and in rare cases when a private party undertakes a traditionally public function, see *Marsh v Alabama*, 326 U.S. 501 (1946), or when the activities of the state and a private entity are sufficiently intertwined to render the private parties' activities public, see *Evans v Newtown*, 382 U.S. 296 (1966)." *See* Cate & Cate, *supra* note 7
[38] *Id*. at 257.
[39] Encyclopedia of Criminal Justice Ethics 1282 (Bruce A. Arrigo ed., 2014).
[40] Yoo, *supra* note 20 at 906.

terrorism, espionage, and sabotage.[41] FISA can be used to target both U.S. citizens and foreign nationals within the country and provides "simplified procedures [to] obtain [] warrants for both electronic surveillance and physical searches."[42] FISA allows surveillance to be conducted within the United States based on a probable cause finding which suggests that the identified suspect is a member of a foreign terrorist group or an agent of a foreign power.[43] This low threshold is the clear differentiator between searches based on routine law enforcement proceedings and those done for national security purposes.

However, there are increased protections under FISA for U.S. citizens. To obtain a warrant targeting a U.S. citizen, the Agency must have probable cause to establish the person "knowingly engage[d] in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States."[44] Thus, FISA requires that the be knowingly done and in violation of a criminal statute. A warrant can be obtained for non-U.S. citizens if they act "in the United States as an officer of a foreign power, or as a member of a foreign power…irrespective of whether the person is inside the United States."[45]

Those seeking warrants under is tasked with overseeing the process by which executive agencies conduct surveillance for national security purposes.[46] FISC is composed of a panel of eleven judges, each of whom serves a seven-year term.[47] The Court of Review, composed of three judges, hears appeals.[48] Title I of FISA requires the government to obtain judicial warrants from the court to conduct electronic surveillance to satisfy national security needs.[49] Once granted a warrant, FISA includes no requirement that the Agency reports its activities back to the court.[50]

On its face, FISC seems like a plausible mechanism to uphold the rights of citizens and foreigners through fair judicial due processes. FISC is essentially a compromise between war–time powers and the

---

[41] As enacted in 1978, FISA covered only electronic surveillance. It was amended in 1994 to cover physical searches and again in 1998 to cover pen register, trap and trace devices, and business records acquisition. *See* 50 U.S.C. § 1821 et seq. (physical searches); *See also* 50 U.S.C § 1841 et seq. (pen register, trap and trace devices, and business records). "Foreign intelligence information" is a term of art and is defined as "information related to and, if concerning a United States person, necessary to, the ability of the United States to protect against an actual or potential attack, terrorism or sabotage by a foreign power or agents thereof, or clandestine intelligence activities of a foreign power or agent thereof, or information with respect to a foreign power or foreign territory that relates to and, if concerning a United States person, is necessary to, the national security of the United States or the conduct of the foreign affairs of the United States." 50 U.S.C. § 1801(e).

[42] Stephanie Cooper Blum, *What Really Is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform*, 18 B.U. PUB. INT. L.J. 269, 276 (2009).

[43] 50 U.S.C. § 1805.

[44] 50 U.S.C. § 1801(b)(2)(A).

[45] 50 U.S.C. §1801(b)(1)(A).

[46] 50 U.S.C. §§ 1804-05.

[47] *Foreign Intelligence Surveillance Court and Court of Review, 1978-present*, FED. JUD. CTR. (Oct. 20, 2021) https://www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court [https://perma.cc/EZ8X-SPXQ].

[48] *Id.*

[49] 50 U.S.C. § 1805.

[50] Jeremy D. Mayer, *9-11 and the Secret FISA Court: From Watchdog to Lapdog?*, 34 CASE W. RES. J. INT'L. L. 249, 250 (2002).

meticulousness of the United States criminal justice system.[51] FISA requires investigators to identify an individual target, show probable cause, and obtain a warrant issued by a federal court.[52] However, lenience is given to intelligence agencies because FISC "does not require a showing of probable cause of criminal activity by the target [of the investigation], which the Fourth Amendment would [generally] require."[53] The government must only show that the probable cause "is linked to a foreign power or terrorist group."[54]

Further, FISC's ruling statistics are contrary to their even-handed judicial appearance. In 2012, the government applied to FISC on 1,789 occasions to have the ability to conduct electronic surveillance, and FISC granted every one of those requests.[55] Between 1979 and 2012, government agencies were granted 99.97% of all FISA warrant requests.[56] FISA also allows warrantless surveillance up to one year for communications "used exclusively between or among foreign powers" where there is "no substantial likelihood" that a communication involving a U.S. person would be acquired.[57]

Justifications, such as war–time powers, foreign conspiracy, and the possibility of terrorism or espionage allow U.S. law enforcement to fast-track their investigations under FISA. There is little doubt that investigations regarding legitimate national security issues should be handled swiftly and efficiently. However, the question that remains is whether the safeguards created by FISC are substantial enough to protect innocent people from indiscriminate targeting and Fourth Amendment violations resulting from mass data collection methods. These questions and their implications will be discussed below.

B. The USA PATRIOT Act

The PATRIOT Act increased surveillance powers for national security purposes and loosened many of the FISA safeguards, which allowed law enforcement to utilize a faster and more effective system to combat terrorism.[58] Five weeks after the terrorist attacks of September 11th, 2001, Congress enacted the now-infamous Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and

---

[51] Yoo, *supra* note 20 at 905.
[52] *Id.*
[53] *Id.*
[54] *Id.*
[55] Letter from Peter J. Kadzik, Principal Deputy Asst. Att'y Gen., to the Hon. Harry Reid, Maj. Leader of U.S. S. 1 (Apr. 30, 2013), www.fas.org/irp/agency/doj/fisa/2012rept.pdf [https://perma.cc/TC64-E5WL].
[56] Conner Clark, *Is the Foreign Intelligence Surveillance Court Really a Rubber Stamp? Ex Parte Proceedings and the FISC Win Rate*, 66 STAN. L. REV. ONLINE 125, 125 (2014), https://www.stanfordlawreview.org/online/is-the-foreign-intelligence-surveillance-court-really-a-rubber-stamp/ [https://perma.cc/V5YP-K4YQ]; *See also* Evan Perez, *Secret Court's Oversight Gets* Scrutiny, WALL ST. J. (June 9, 2013), https://www.wsj.com/articles/SB10001424127887324904004578535670310514616 [https://perma.cc/Q543-3PEA].
[57] 50 U.S.C. 1802(a)(1) & (A)(i).
[58] *The USA Patriot Act: Preserving Life and Liberty*, Dep't of Just., https://www.justice.gov/archive/ll/highlights.htm [https://perma.cc/XL2M-DGTS].

Obstruct Terrorism Act (PATRIOT Act).[59] The Department of Justice (DOJ) website describes the PATRIOT Act as the "leading role… to protect innocent Americans from the deadly plans of terrorists dedicated to destroying America and our way of life."[60] Substantively, the DOJ claims that "[t]he Patriot Act allows investigators to use the tools that were already available to investigate organized crime and drug trafficking."[61] Alternatively, the ACLU claims that the PATRIOT Act n. It… is used in ways that treat everyone as a suspect, and chills free expression."[62]

Among other things, the PATRIOT Act changed the following: (1) allowed investigators to use surveillance methods deemed necessary for seventy-two hours before obtaining a FISA warrant (previously twenty-four); (2) broadly expanded the definition of "terrorist organization," to include many domestic groups that engage in civil disobedience; (3) expanded the search capabilities of investigators, allowing them to use mass data collection methods including pen registers, trap and trace devices, roving wiretaps; and (4) potentially the most consequential feature of the PATRIOT Act, which was the modification of the FISA language that set the standard for obtaining a warrant from a FISC judge.[63] To conduct surveillance before the FISA, the government had to assert that the "purpose of the surveillance is to obtain foreign intelligence information."[64] Under the new modification, the government is only required to show a "significant purpose."[65]

The PATRIOT Act permits a broad array of surveillance methods and devices.[66] Previously, investigators were required to narrow their inquiry based on a single target. However, the PATRIOT Act broadened investigator's inquiries by allowing them to "hop" to every individual's phone data who is in communication with the target's phone.[67] Below is

---

[59] Pub.L. No. 107-56, § 208(1), 115 Stat. 283 (2001). While this article will not go into the depth of this act and its residual effects, it is important to highlight its origins and reactionary policies, which lead to its more recent reductions.

[60] *The USA Patriot Act: Preserving Life and Liberty*, *supra* note 58.

[61] *Id.*

[62] *End Mass Surveillance Under the Patriot Act*, ACLU, https://www.aclu.org/issues/national-security/privacy-and-surveillance/end-mass-surveillance-under-patriot-act [https://perma.cc/CVL9-MYU4].

[63] USA PATRIOT ACT of 2001, Pub.L. No. 107-56, 115 Stat. 272. USA PATRIOT ACT section 411. (Section 411 expands the definition of terrorist organization as, "a political, social or other similar group whose public endorsement of acts of terrorist activity the Secretary of State has determined undermines United States efforts to reduce or eliminate terrorist activities"). *Id.* at 115 Stat. 286. *Id.* 115 Stat. 213.

[64] 50 U.S.C. § 1804(a)(7)(B) (2000) (effective December 27, 2000 to October 25, 2001).

[65] Sections 104(a)(7)(B) and section 303(a)(7)(B) (50 U.S.C. 1804(a)(7)(B) and 1823(a)(7)(B)) of the Foreign Intelligence Surveillance Act of 1978 are each amended by striking "the purpose" and inserting "a significant purpose". UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM (USA PATRIOT ACT) ACT OF 2001, PL 107–56, October 26, 2001, 115 Stat 291 Section 218; A FISA-related operation is justified where "a significant purpose" of such operation "is to obtain foreign intelligence. This has cleared away much of the detritus that developed around FISA that had historically impeded the use of FISA in criminal investigations and the use of FISA information in criminal prosecutions." JAMES G. MCADAMS, FEDERAL LAW ENFORCEMENT TRAINING CENTER, FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA): AN OVERVIEW, 10.

[66] *Id.* 115 Stat. 286.

[67] NSA Civil Liberties and Privacy Office, *Transparency Report: THE USA FREEDOM Act Business Records FISA Implementation* (15 January, 2016), https://www.nsa.gov/Portals/70/documents/about/civil-liberties/reports/UFA_Civil_Liberties_and_Privacy_Report.pdf.

the published example used by the NSA describing how the "hopping" method works in practice:

To illustrate the process, assume an NSA intelligence analyst identifies or learns that phone number (202) 555-1234 is being used by a suspected international terrorist. This is the "specific selection term" or "selector" that will be submitted to the FISC (or the Attorney General in an emergency) for approval using the RAS [reasonable articulable suspicion] standard. Also assume that, through NSA's examination of metadata produced by the provider(s) or in NSA's possession as a result of the Agency's otherwise lawfully permitted signals intelligence activities, NSA determines that the suspected terrorist has used a 202 area code phone number to call (301) 555-4321. The phone number with the 301-area code is a "first-hop" result. In turn, assume that further analysis or production from the provider(s) reveals (301) 555-4321 was used to call (410) 555-5678. The number with the 410-area code is a "second-hop" result.[68]

The PATRIOT Act covers a wide variety of surveillance methods across devices.[69] The investigator's scope of authority grows exponentially past the initial warrant, that only required there be a "significant purpose" relating to the target, as they "hop" between all communication connected to the target's phone. In practice, if a target realizes that they are being investigated, they may decide to discard their cell phone. A roving wiretap would allow the investigator to continue monitoring that person without obtaining a new warrant from a judge.

Because of these broad allowances, the PATRIOT Act was under intense scrutiny from civil and human rights watchdog groups for many years, but Edward Snowden's disclosures in 2013 finally brought the extent of the Act's abuses into the public eye.[70]

The original PATRIOT Act included sunset provisions that caused many of its laws to terminate on December 31, 2005.[71] Yet, Congress renewed the legislation in March of 2006, and President Obama subsequently extended many of the expiring provisions in May 2011, including "roving wiretaps, searches of business records, and the surveillance of 'lone wolves.'"[72] "Lone wolf" surveillance authority allows investigators to obtain surveillance orders without having to prove that an individual was connected to a specific organization or terrorist

[68] *Id.* at 6-7.

[69] A few additional examples of surveillance methods allowed under the PATRIOT Act include: (1) a pen register, which is an electronic device that records all outgoing communications from a particular phone or computer; (2) trap and trace devices, which record all incoming communications to a particular phone line or IP address; and (3) roving wiretaps, which allow investigators to follow a particular target across communication devices. In practice, if a target realizes that they are being investigated, they may decide to discard their cell phone. A roving wiretap would allow the investigator to continue monitoring that person without obtaining a new warrant from a judge. *Electronic Surveillance*, Legal Info. Inst., https://www.law.cornell.edu/wex/electronic_surveillance [https://perma.cc/Y5AM-UEWM]; UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM (USA PATRIOT ACT) ACT OF 2001, Pub. L. No. 107-56, § 218, 115 Stat. 291 (2001) (codified as amended in scattered sections of the U.S. Code).

[70] *End Mass Surveillance Under the Patriot Act*, *supra* note 62.

[71] *Electronic Surveillance*, *supra* note 69.

[72] *Id.*

group.[73] Finally, when the extensions expired in 2015, Congress repackaged many of its provisions in the equally aptly named USA FREEDOM Act.

C. The USA FREEDOM Act

In response to increasing public outcry, the USA FREEDOM Act modified many of the PATRIOT Act's provisions to reduce its exceedingly broad language.[74] Originally the FREEDOM Act was intended to stand for Fulfilling Rights and Ending Eavesdropping, Dragnet-Collection and Online Monitoring Act.[75] However, it was clear that the final version would not live up to that title.

The FREEDOM Act only has a few major modifications to its predecessor. First, the FREEDOM Act bans the bulk collection of Americans' telephone records and internet metadata.[76] Second, it limits the government's data collection to the "greatest extent reasonably practicable."[77] This standard differs in that the investigators can no longer collect large amounts of data pertaining to a specific geographic region alone, such as a city or an area code.[78] In practice, these adjustments require agencies, like the NSA, to stop using an accumulated bulk collection of phone data. Instead, the Agency may only request phone data that is within two "hops" of the target whose search has been approved.[79] This restriction greatly limits the data collection chain accessible to the government and is key to maintaining privacy.

While these modifications curtail the broad data collection authority given to United States authorities under the PATRIOT Act, there are several other provisions worth noting: (1) the FREEDOM Act provides the government with new reporting requirements to FISA authorities; (2) it gives private companies more opportunities to report information about the FISA orders they receive publicly; (3) it declassifies FISA court opinions that require extensive legal interpretation, or, if not possible, requires that a summary is provided; (4) it requires the FISC to designate a panel of amicus curiae (civil oversight) to represent public interest; and (5) it significantly extends multiple PATRIOT Act provisions, including roving wiretaps and lone wolf surveillance authority.[80]

Thus, the FREEDOM Act contains significant improvements to the "war–time" powers that the PATRIOT Act provided by banning bulk data collection, increasing transparency, and providing additional

---

[73] FISA Reauthorization, SENATE RPC (Feb. 25, 2020), https://www.rpc.senate.gov/policy-papers/fisa-reauthorization[https://perma.cc/7Y8J-UMFR].
[74] *End Mass Surveillance Under the Patriot Act*, *supra* note 62.
[75] Fry, *supra* note 10
[76] The USA Freedom Act, 1 Policies and Practices § 63:6.
[77] Section (k) definitions, (4)(A)(i)(II) reads: "(II) is used to limit, to the greatest extent reasonably practicable, the scope of tangible things sought consistent with the purpose for seeking the tangible things. USA Patriot Act of 2001, Pub. L. No. 114-23, § 107, 129 Stat. 274 (2015) (codified as amended in scattered sections of the U.S. Code).
[78] *Id* at § 201, 129 Stat 277.
[79] NSA CIVIL LIBERTIES & PRIVACY OFFICE, TRANSPARENCY REPORT: THE USA FREEDOM ACT BUSINESS RECORDS FISA IMPLEMENTATION, at 6 (2016).
[80] Under Title VI, specifically § 604, 115 Stat. at 286. § 402, 115 Stat. at 286. See also Yoo, *supra* note 20 at 905.

oversight to the FISA courts.[81] With the United States surveillance legislation background summarized in this section, the subsequent section will narrow the analysis of these issues by looking to U.S. surveillance case law, specifically focusing on the following pivotal cases: *U.S. v. Carpenter* and *U.S. v. Moalin*.

D. U.S. Surveillance Case Law

It is unlikely that the Constitution's framers could have anticipated the technological revolution that the world has undergone in the last twenty years. The historical arguments advocating for privacy under the Fourth Amendment were contingent on physical invasion.[82] Today, many investigations can be done remotely since an individual's most revealing information now lies within the data trail of their phone or computer. *Katz v. United States* was the first major deviation from the narrow Fourth Amendment interpretations limiting protections only to "persons, houses, papers and effects."[83] The Court created a two–part test: (1) did the person have a subjective expectation of privacy under the circumstances, and (2) was the person's expectation of privacy objectively reasonable?[84] Given the broad interconnectivity most individuals have between online accounts, phone companies, social media, etc., this 1960's test creates difficult questions when one asks, is there a subjective expectation of privacy anymore, and when is it objectively reasonable to expect it?

In *Katz,* the Court held that the defendant had a reasonable expectation of privacy while using a phone booth.[85] Law enforcement had installed a wiretap into the phone booth the defendant was using, which was used to find illegal activity.[86] Similarly, in *Kyllo v. United States*, the Court held that the defendant had a reasonable expectation of privacy within his own home.[87] In *Kyllo,* law enforcement used thermal imaging to detect heat lamps used to grow marijuana.[88] Because thermal imaging devices were not available to the general public, it was reasonable to assume that that tool would not be used without probable cause and a warrant.[89]

Analogizing *Katz,* the internet could arguably be the modern equivalent to a phone booth in the 1960s. Just as a person should have had a reasonable expectation of privacy when making a call in a phone booth, they should likewise have a reasonable expectation that the information accessed and transmitted via the internet will not be accessible to the government without a warrant. Analogizing *Kyllo,* the tools that

---

[81] *Id.*
[82] *See e.g.*, *Olmstead*, 277 U.S. at 466 (holding that the wiretapping of defendant's phone conversations did not constitute a violation of his constitutional rights), *overruled in part by* Berger v. State of N.Y., 388 U.S. 41 (1967), *and* Katz v. United States, 389 U.S. 347 (1967).
[83] Katz v. United States, 389 U.S. 347, 352 (1967) (The Court's reasoning implies that the Fourth Amendment's protection are applicable to all areas where citizens have reasonable expectations of privacy).
[84] *Id*. at 361 (Harlan, J., concurring).
[85] *Id*. at 350-51 (majority opinion).
[86] *Id*. at 348.
[87] Kyllo v. United States, 533 U.S. 27, 34, 121 S. Ct. 2038, 2046, 150 L. Ed. 2d 94 (2001).
[88] *Id*. at 29.
[89] *Id*. at 34.

government agencies such as the NSA have available to them are not available to the public. Hence, metadata is arguably like thermal imaging, and citizens should have the reasonable expectation that their internet and phone data is private absent a warrant.[90]

The following cases: *U.S. v. Carpenter* and *U.S. v. Moalin,* raise issues under current surveillance legislation. First, the Supreme Court upheld law enforcement's ability to track the defendant based on his cell-site location information in a 5-4 decision in *Carpenter*. Second, in *Moalin*, the "hopping" method—as described above—was put to the test, and national security justifications were held sufficient to uphold the conviction. These cases set the stage for the current law in the U.S. and will be used to analyze the government's methods in relation to that of the People's Republic of China in later sections.

i. U.S. v. Carpenter

In *Carpenter v. United States,* the Court faced questions regarding Fourth Amendment violations based on the investigative methods used to convict a defendant of multiple armed robberies. Law enforcement used Cell-Site Location Information (CSLI) to determine if the defendant was in the geographic areas in question at the times relevant to each robbery. CSLI is generated "[e]ach time the phone connects to a cell site,"[91] and "[w]ireless carriers collect and store CSLI for their own business purposes."[92]

The Court made three critical points. First, cell phone companies are considered third parties. Under the third-party doctrine, a person has no legitimate expectation of privacy, for Fourth Amendment purposes, in information he voluntarily turns over to third parties. As a result, the government is typically free to obtain such information from the recipient without triggering Fourth Amendment protections.[93] Second, despite cell phone companies being considered third parties, an individual maintains a legitimate expectation of privacy in the records of his physical movements as captured through CSLI and cell phone carrier data.[94] Third, the government must obtain a warrant based on a finding of probable cause before acquiring CSLI from a wireless carrier.[95] The Court explained, "although the ultimate measure of the constitutionality of a government search is 'reasonableness,' our cases establish that warrantless searches are typically unreasonable where a search is undertaken by officials to discover evidence of criminal wrongdoing."[96]

Although narrow, *Carpenter's* holding established a historic precedent that protects a user's third-party cell phone data from warrantless searches. Specifically, the protection of a user's CSLI and other data that an individual could legitimately expect to be held private.

---

[90] Fry, *supra* note 10.
[91]
[92] *Id.* at 2211-2212.
[93] *Id.* at 2216.
[94] *Id.* at 2217.
[95] *Id.* at 2221.
[96] *Id.*

This standard could be reasonably be extended across multiple platforms including the following: login-in locations on social media, Wi-Fi connections, app data tracking movement and health, and browser location data. *Carpenter* makes a specific acknowledgment to the "privacies of life"[97] that have historically been protected by the Fourth Amendment.

However, the discussion raised by *Carpenter*, and most Fourth Amendment case law, applies to law enforcement's request for a specific individual's data based on probable cause. As noted in the previous sections, these issues are only compounded when government agencies use technology to conduct surveillance on large populations.

ii. U.S. v. Moalin

In *U.S. v. Moalin*, mass data surveillance methods were used in an investigation to identify a national security threat, and consequently, the Fourth Amendment violations of the parties' collateral to the investigation became largely justified.[98] The U.S. Court of Appeals for the Ninth Circuit affirmed the lower court's ruling to convict four U.S. residents accused of conspiring to provide support to a foreign terrorist organization, al-Shabaab,[99] and conspiracy to launder monetary instruments.[100]

Al-Shabaab uses distinctive methods of violence, such as improvised explosive devices and suicide bombings.[101] Many people from Somalia had fled the country in response to the conflict.[102] Moalin and his codefendants immigrated to southern California but remained actively engaged in the developments in Somalia.[103] The four defendants were attempting to send approximately $19,000 to their Somali contacts under the pretense of "funding efforts relating to a school."[104]

At trial, the government's principal evidence consisted of multiple recordings of phone conversations between Moalin, his codefendants, and their Somali contacts.[105] These recordings were obtained through a FISC approved wiretap of Moalin's phone. The relevant excerpts from the recordings include Moalin speaking with a contact about "the young men who are firing the bullets"[106] and that "these men cut the throats of 60..."[107] Ethiopians and destroyed five vehicles.[108] Several of the calls involved a suspected terrorist leader in al-Shabaab.[109]

The government obtained the telephone call records and acquired the wire approval using bulk metadata collection methods under the "business

---

[97] *Id.* at 2214 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).
[98] *Moalin*, 973 F.3d, at 985.
[99] *Id.* at 1010.
[100] *Id.* at 985.
[101] *Id.* at 984.
[102] *Id.* at 985.
[103] *Id.*
[104] *Id.* at 986.
[105] *Id.*
[106] *Id.*
[107] *Id.*
[108] *Id.*
[109] Rachael Hanna, *Metadata Collection Violated FISA, Ninth Circuit Rules,* LAWFARE (Sept. 14, 2020), https://www.lawfareblog.com/metadata-collection-violated-fisa-ninth-circuit-rules [https://perma.cc/8QSX-YF3L].

records" subsection of the FISA.[110] The bulk data collection was still compliant with Federal law because the investigation took place before the FREEDOM Act took effect. Thus, the government was allowed to use the phone company's database when NSA officials were determined to have "reasonable, articulable suspicion" that the suspect's phone number was connected with "one of the identified international terrorist organizations."[111] Further, the government was allowed to search phone numbers within three "hops" of the suspected phone number.[112]

On appeal, the defendants contended that the meta data collection methods used in this case violated their Fourth Amendment rights and the FISA section used to authorize the search.[113] At this point, the bulk data collection methods used had been replaced by new provisions under the FREEDOM Act, as described above. As a result, the defendants argued that the phone data collected under the former program were "fruits of the poisonous tree"[114] and should therefore be suppressed. [115]

The Court denied Moalin's suppression motion and did not grant security-cleared defense counsel access to the documents supporting the FISA orders.[116] Although the bulk data collection practice was declared unconstitutional, the court found that this practice did "not taint the evidence introduced by the government at trial,"[117] and the "fruit of the poisonous tree" argument did not apply here. The metadata "did not and was not necessary to support the requisite probable cause showing."[118] Accordingly, the court substantiated the evidence, while simultaneously condemning the bulk metadata collection practice.[119] As a result, the conviction was affirmed despite the government's questionable methods in acquiring the data.[120]

Moalin is significant for three reasons. First, the court held that the NSA's bulk meta data collection program violated the FISA.[121] Not only were the collection methods used to obtain Moalin's phone records possibly unconstitutional, but so was the collection of thousands of Americans' phone records that were affected in the process.[122] Second, *Moalin* is the first ruling to acknowledge and confirm Edward Snowden's 2013 disclosures. Third, the court held that even if the bulk metadata collection program violated citizens' Fourth Amendment rights under the "auspices of foreign intelligence investigation," suppression of the

---

[110] *Moalin,* 973 F.3d, at 988.
[111] *Id.*at 989.
[112] *Id.*
[113] *Id.*
[114] This is a doctrine "extends the exclusionary rule to make evidence inadmissible in court if it was derived from evidence that was illegally obtained. As the metaphor suggests, if the evidential "tree" is tainted, so is its fruit." *Fruit of the Poisonous Tree,* LEGAL INFORMATION INSTITUTE, https://www.law.cornell.edu/wex/fruit_of_the_poisonous_tree [https://perma.cc/B53G-SZKU].
[115] *Id.*
[116] *Moalin,* 973 F.3d, at 989-90.
[117] *Id.* at 993.
[118] *Id.* at 997.
[119] *Id.* at 993.
[120] *Id.* at 1010.
[121] *Id.* at 984.
[122] *Id.*

evidence was not warranted.[123] Therefore, although the evidence was "fruit of the poisonous tree," the court held that the manner in which it was obtained was not prejudicial enough to suppress the evidence under current law.[124]

Although privacy rights of countless innocent people were violated in the *Moalin* investigation processes, the method worked. This outcome raises difficult questions concerning the delicate balancing act between trusting law enforcement to track only those that pose a threat to the U.S. and its interests, while preventing the collateral damage that can result from the abuse of such power. Although this case was seen as a success, and validated many of Edward Snowden's claims, a consistent narrative persists throughout U.S. policy: the privacy violations inflicted upon innocent Americans are a necessary byproduct of the war on terrorism.

Carpenter set an important precedent, but the use of digital surveillance remains clouded in secrecy, and it is difficult to determine whether legitimate national security purposes justify the use of surveillance.[125] Perhaps, it is even more challenging when assessing whether the methods used by intelligence agencies are proportional to the actual threats the U.S. faces. Comparing international digital surveillance policy with that of the U.S. may allow for a clearer understanding of what laws are proportional when analyzing an appropriate balance between national security and individual privacy rights. The next section will analyze the PRC's surveillance practices and how they have been put into practice during the recent uprising in Hong Kong.

IV. MAINLAND CHINESE LAW

Freedom of speech and the right to privacy have been important in China since ancient times.[126] Despite stereotypical beliefs that a collectivist society may not value privacy rights as an individualistic society would, Article 40 of the PRC's Constitution states that freedom of privacy of correspondence of citizens of the People's Republic of China are protected by law.[127] No organization or individual may, on any ground, infringe upon citizens' freedom and privacy."[128] However, Article 40 goes on to say, "[e]xcept in cases where, to meet the needs of State security or of criminal investigation, public security or procuratorial [*sic*.] organs are

[123] *Id.* at 984.
[124] *Id.* at 997.
[125] *See, e.g.*, Klayman v. Obama, 957 F. Supp. 2d 1, 40 (D.D.C. 2013) (noting that "the Government does *not* cite a single instance in which analysis of the NSA's bulk metadata collection actually stopped an imminent attack, or otherwise aided the Government in achieving any objective that was time-sensitive in nature"), *vacated*, 800 F.3d 559 (D.C. Cir. 2015).
[126] Jingchun Cao, *Protecting the Right to Privacy in China*, 36 VICTORIA U. WELLINGTON L. REV. 645, 646-47 (2005) (asserting that privacy was protected, to some extent, in ancient China and an awareness of privacy may be found all the way back to the Warring States Period).
[127] *Country Profiles - China*, OPENNET INITIATIVE. (Aug. 9, 2012), https://opennet.net/research/profiles/china-including-hong-kong [https://perma.cc/868Q-HLKR].
[128] Const. of the People's Republic of China, art. 40 (Mar. 14, 2004), [hereinafter Const. China] http://www.npc.gov.cn/zgrdw/englishnpc/Constitution/2007-11/15/content_1372964.htm [https://perma.cc/4J46-RG8L].

permitted to censor correspondence in accordance with the procedures prescribed by law."[129]

Further, Article 35 guarantees the same five basic rights as the First Amendment of the U.S. Constitution.[130] Thus, the Chinese Constitution is strikingly similar to the foundational principles of U.S. law. For instance, both systems pledge to protect and value individual citizens' freedom of speech, assembly, and privacy from government intervention. Nevertheless, the PRC has "one of the most pervasive and sophisticated regimes of internet filtering and information control" in the world.[131]

While internet use in China has grown almost exponentially over the last decade, the Chinese Government has integrated its surveillance techniques along with it.[132] The internet was believed to be a catalyst in its early stages, allowing the Chinese people to break free from the information vacuum under a post-Mao authoritarian government.[133] However, the Chinese government has utilized technology to control individuals more intimately than ever before.[134] "In an environment where information flows pervasively, the most effective and efficient tool for government control is probably neither strict law nor military force, but technology itself."[135]

Before proceeding into further analysis, it should be noted that PRC case law concerning electronic privacy, surveillance, and censorship goes unpublished which makes it inaccessible.[136] State secrets and personal privacy law cases are said to be explicitly conducted in a closed court.[137] First, this may be because the government does not wish for these cases to be publicized because they may draw criticism, both domestically and internationally. Second, the information in many of these cases may be confidential state secrets, or the government does not want to expose the extent of its surveillance programs. Lastly, the cases may not be handled in open court but by compartmentalized government agencies.[138] With this baseline established, the proceeding section will analyze the current shift in Hong Kong as mainland China continues to force a transition to bring the region under PRC law.

---

[129] *Id.*
[130] Const. China, *supra* note 128, art. 35.
[131] Country Profiles – China, *supra* note 127.
[132] Jyh-An Lee & Ching-Yi Liu, *Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China*, 13 MINN. J.L. SCI. & TECH. 125, 126 (2012).
[133] Andrew Jacobs & Jonathan Ansfield, *Nobel Peace Prize Given to Jailed Chinese Dissident*, N.Y. TIMES (Oct. 9, 2010), www.nytimes.com/2010/10/09/world/09nobel.html?pagewanted=all [https://perma.cc/3M4M-EUAD].
[134] Lee & Liu, *supra* note 132.
[135] *Id.*
[136] For cases not tried in open court sessions because of their involvement of state secrets, *see* CRIM. PROC. LAW OF THE PEOPLE'S REPUBLIC OF CHINA, art. 183 (1996) [hereinafter CRIM. PROC. LAW], *See also* CIVIL PROC. LAW OF THE PEOPLE'S REPUBLIC OF CHINA, art. 134 (1991) [hereinafter CIVIL PROC. LAW] (stating that cases that involve state secrets shall not be heard publicly by people's courts). *See generally* ADMIN. PROC. LAW OF THE PEOPLE'S REPUBLIC OF CHINA, art. 65 (1989) [hereinafter ADMIN. PROC. LAW].
[137] CRIM. PROC. LAW, *supra* note 136, art. 183 ("A people's court shall try cases of first instance in open court sessions, except for the cases involving state secrets or personal privacy.").
[138] Fry, *supra* note 10.

V. HONG KONG DISSENTION

First, it is necessary to establish the events leading up to the current status of the formerly semiautonomous territory of Hong Kong. Second, the national security laws imposed on Hong Kong in May 2020 will be discussed in relation to citizens' loss of freedoms, specific acts of privacy infringement, and the justifications given by the Chinese government for these actions. The last subsection will analyze how technology has been a tool in the takeover of the formerly semiautonomous territory.

A. Historical Background

Until 1997, the small island of Hong Kong, which sits on China's southeastern edge, had been a territory of the United Kingdom for 155 years. Britain seized the territory during the First Opium War after the Qing dynasty cracked down on the illegal opium trade conducted out of the thriving port town.[139] In 1898, the two countries agreed to the Convention for the Extension of Hong Kong Territory, which leased Hong Kong.[140]

As the treaty's expiration loomed in the early 1980s, the countries agreed to the Sino-British Joint Declaration, which established the "one country, two systems" policy for 50 years.[141] After the treaty officially expired, Hong Kong was considered a Special Administrative Region of China but maintained its own constitution under its Basic Law.[142] Until recently, these policies held firm.[143] Hong Kong has maintained a court system closely resembling that of the United Kingdom. It even retained British judges.[144]

However, since 2014 this independence has slowly chipped as elections have been conducted using a list of candidates vetted by Beijing.[145] In the last year, Hong Kong's government, autonomy, and independent court systems have been fundamentally uprooted and replaced by mainland Chinese law.[146] The policies approved under pro-mainland officials have become the breaking point for many Hong Kong

---

[139] Erin Blakemore, *How Hong Kong's complex history explains its current crisis with China,* NATIONAL GEOGRAPHIC (Aug. 7, 2019), https://www.nationalgeographic.com/culture/topics/reference/hong-kong-history-explain-relationship-china/ [https://perma.cc/KN7R-X7VK].

[140] *Id.*

[141] *Id.*

[142] Full Text of the Const. and the Basic Law, CONST. AND MAINLAND AFFAIRS BUREAU, https://www.basiclaw.gov.hk/en/basiclawtext/index.html [https://perma.cc/SNC9-TD4H].

[143] *Hong Kong national security law full text,* SOUTH CHINA MORNING POST (July 2, 2020), https://www.scmp.com/news/hong-kong/politics/article/3091595/hong-kong-national-security-law-read-full-text [https://perma.cc/AF3A-FDTR].

[144] Reuters Staff, *UK Considers Whether to Remove British Judges from Hong Kong Court* (Nov. 23, 2020), https://www.reuters.com/article/us-hongkong-britain/uk-considers-whether-to-remove-british-judges-from-hong-kong-court-idUSKBN2832S9 [https://perma.cc/AY4C-VTE4].

[145] *The End of One Country, Two Systems*?: *Implications of Beijing's National Security Law in Hong Kong*, U.S. Congress, House Committee on Foreign Affairs, 116th Cong., 2nd sess., (July 1, 2020) (Testimony of Lee Cheuk-Yan).

[146] *China's National Security Law for Hong Kong: Issues for Congress,* Congressional Research Service (Aug. 3, 2020), at 25, https://fas.org/sgp/crs/row/R46473.pdf [https://perma.cc/Z3BF-RE2T].

residents who have grown accustomed to the semi-autonomous territory's uniquely independent position.[147]

The initial spark began in February 2019 when the Hong Kong legislature approved the Fugitive Offender and Mutual Legal Assistance in Criminal Matter Legislation (Amendment) Bill.[148] The specific concern over the legislation is the possibility for extradition to mainland China.[149] Opponents to this bill believed that citizens could be unjustly persecuted based on political motivations and result in unfair trials on mainland China.[150] Essentially, Hong Kong citizens feared that they could be subject to the harsh anti-government crimes that limit the free speech of mainlanders.

For example, Lam Wing-kee, Causeway Bay Books manger in Hong Kong, maintained a stock of books that are analogous to tabloid material.[151] From twisted love affairs involving CCP leader Xi Jinping, to questionable tales about the innerworkings of the Party, many of these paperbacks could be written off as wildly fictional.[152] However harmless these stories may seem, Mr. Lam was kidnapped and taken to mainland China, where he suffered eight months of "mental torture" in a prison cell.[153] This account is one of many that caused outrage throughout Hong Kong and fueled an increasingly urgent fight to maintain autonomy.

On July 6, 2019, after almost eight months of increasingly violent protests, a shut-down of the economic center, and countless arrests, the Hong Kong legislature backed down and withdrew the bill in its entirety.[154] However, this was seen as an insufficient remedy for many people who had been personally affected by police brutality and lengthy prison sentences related to the protests.[155] As a result, riots continued, and the pro-democracy movement raged on.

---

[147] Mike Ives, *What is Hong Kong's Extradition Bill,* N.Y. TIMES (June 10, 2019), https://www.nytimes.com/2019/06/10/world/asia/hong-kong-extradition-bill.html?auth=login-email&login=email [https://perma.cc/LG6K-RZQ4].

[148] Fugitive Offenders and Mutual Legal Assistance in Criminal Matters Legislation (Amendment) Bill 2019.

[149] Ives, *supra* note 147.*; see also* Fugitive Offenders and Mutual Legal Assistance in Criminal Matters Legislation (Amendment) Bill 2019 at C501.

[150] Ives, *supra* note 147.

[151] Michael Forsythe & Andrew Jacobs, *In China, Books that Make Money, and Enemies,* N.Y. TIMES (Feb. 4, 2016), https://www.nytimes.com/2016/02/07/business/international/in-china-books-that-make-money-and-enemies.html [https://perma.cc/8BJR-JQYZ]; Phila Siu, Ng Kang-chung and Owen Fung, *Bookseller Lam Wing-kee reveals explosive details of his mainland China detention, claims Lee Po told him he was 'taken away from Hong Kong'* SOUTH CHINA MORNING POST (June 16, 2016), https://www.scmp.com/news/hong-kong/politics/article/1976489/bookseller-lam-wing-kee-reveals-explosive-details-his?module=perpetual_scroll&pgtype=article&campaign=1976489 [https://perma.cc/EN7E-2QNS].

[152] *Id.*

[153] Alan Wong et al., *Defying China, Hong Kong Bookseller Describes Detention,* N.Y. TIMES (June 16, 2016), https://www.nytimes.com/2016/06/17/world/asia/hong-kong-bookseller-lam-wing-kee.html?module=inline&login=email&auth=login-email&login=email&auth=login-email [https://perma.cc/9DHN-QKEN]; Siu, Kang-chung & Fung, *supra* note 162.

[154] Amy Qin, *Extradition Bill is 'Dead," Says Hong Kong Leader, Carrie Lam,* N.Y. TIMES (July 8, 2019), https://www.nytimes.com/2019/07/08/world/asia/carrie-lam-hong-kong.html?searchResultPosition=2 [https://perma.cc/SN72-L73L].

[155] *Hong Kong formally scraps extradition bill that sparked protests,* BBC CHINA (Oct. 23, 2019), https://www.bbc.com/news/world-asia-china-50150853 [https://perma.cc/EG9N-YFL6].

B. National Security Law

The CCP, however, was not ready to back down. On June 30, 2020, in response to the outbreak of dissent generated by the Hong Kong protests, President Xi Jinping signed a broad new National Security Law (NSL) that would fundamentally change Hong Kong's freedoms and its relationship with the mainland. The following is a revealing excerpt from the English version of the law:

> Safeguarding national security; preventing, suppressing and imposing punishment for the offences of secession, subversion, organization and perpetration of terrorist activities, and collusion with a foreign country or with external elements to endanger national security in relation to the Hong Kong Special Administrative Region; protecting the lawful rights and interests of the residents of the Hong Kong Special Administrative Region.[156]

In May 2020, National People's Congress (Chinese legislature) Vice Chairman Chen cited "growing risks to China's national security in the city since the outbreak of anti-extradition bill protests in June 2019."[157] Chen asserted that protestors were "anti-China" and wanted to "bring chaos to Hong Kong."[158] He then stated that protestors "openly insulted and defaced the national flag" and "incited Hong Kong people to be anti-China and anti-communist party."[159]

The NSL allows Chinese law enforcement to arrest and try individuals in the Hong Kong region for any crimes involving anti-government sentiment.[160] In addition, the PRC has appointed officials to serve in two new pro-communist entities established by the law and created the Office for Safeguarding National Security, a new department related to enforcement on the ground.[161] Regarding the "one country, two systems" agreement, PRC appointed officer [162] Zhang stated that the NSL "intends to move closer to the side of 'one country."[163]

Article 62 of the NSL states that the law "shall prevail where provisions of the local laws of the Hong Kong Special Administrative region are inconsistent with this law," thus establishing supremacy over the Hong Kong Basic Law that upheld many rights similar to the United States' First Amendment.[164] As a result, on July 1, 2020, the first day the NSL was implemented, ten people were arrested for violations under the

---

[156] SOUTH CHINA MORNING POST *supra* note 143.
[157] CONGRESSIONAL RESEARCH SERVICE, *supra note 146*
[158] *Id.*
[159] *Id.*
[160] *Id.* at 20-22.
[161] *Id.* at 16.
[162] William Zheng & Echo Xie, *China upgrades Hong Kong affairs with new chief,* SOUTH CHINA MORNING POST (Feb. 13, 2020), https://www.scmp.com/news/china/politics/article/3050401/china-appoints-new-director-hong-kong-and-macau-liaison-office [https://perma.cc/KS7Q-EYUS**].**
[163] State Council Information Office of the PRC, *SCIO Briefing on the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region*, (July 1, 2020), http://english.scio.gov.cn/pressroom/2020-07/04/content_76236573.htm [https://perma.cc/GZ2L-S8ZM].
[164] Congressional Research Service, *supra* note 146

law.[165] The violations included Hong Kong citizens showcasing banners, T-shirts, and books; with slogans like, "One Nation, One Hong Kong,"[166] and "Restore Hong Kong. Revolution of Our Times."[167] The people arrested ranged from age fifteen to sixty-seven.[168]

This crack down on anti-mainland dissent only touches the surface of the issue. Blatant banners advocating for an independent Hong Kong make it easy for law enforcement to spot and arrest their creators. However, hiding in plain sight are thousands of CCTV cameras equipped with the latest facial recognition technology.[169] Regardless of public opinion on the NSL, the provisions clearly state what kinds of action will lead to punishment, and PRC surveillance is difficult to evade.[170]

It should be noted that the laws do not expressly, or even implicitly, restrict the government's internet surveillance powers, and surely will not when national security interests are involved.[171] The next section will discuss the role technology has played in PRC surveillance, both in Hong Kong and on the mainland, and predictions regarding its future ramifications.

C. PRC Digital Surveillance

The Chinese government has created perhaps the world's largest internet filtering system, and the information that people have access to on the Chinese internet is limited.[172] Many western search engines, social media companies, and websites, are banned completely.[173] The blocked websites and services are those that are perceived threats to the Chinese Communist Party: including information regarding the Tiananmen uprising in Hong Kong; the anniversary of Tibetan protests; and human rights violations of the Uyghur Muslim minority.[174] One of the more humorous examples involves blocking the name and image of the cartoon bear Winnie the Pooh, after CCP leader Xi Jinping's likeness was equated

---

[165] *Id.* at 21.
[166] *Id.*
[167] *Id.*
[168] *Id.*
[169] Phoebe Zhang, *Privacy in China: The Growth of Facial Recognition Technology in the Private Sector Raises Concerns about Security and Identity*, SOUTH CHINA MORNING POST (Nov. 26, 2020), https://www.scmp.com/lifestyle/article/3111428/privacy-china-growth-facial-recognition-technology-private-sector-raises. [https://perma.cc/6X47-5NQ9].
[170] Congressional Research Service, *supra* note 146 at 11.
[171] CONSTITUTION OF THE PEOPLE'S REPUBLIC OF CHINA, arts. 38 and 40.
[172] See, e.g., OpenNet Initiative (ONI), China, 271 (Aug 9, 2012), http://access.opennet.net/wp-content/uploads/2011/12/accesscontested-china.pdf; See also Yuezhi Zhao, Communication in China: Political, Economy, Power, and Conflict 32 (2008), https://ebin.pub/communication-in-china-political-economy-power-and-conflict-state-and-society-in-east-asia-074251966x-9780742519664.html ("With the increasing sophistication of firewalls and filtering software, the survival time for offensive content in cyberspace has been progressively reduced.") [https://perma.cc/5V55-7FRN].
[173] *Id.*
[174] *See*, Robert Faris & Nart Villeneuve (Ronald Deibert et al. eds), *Measuring Global Internet Filtering, in Access Denied: The Practice and Policy of Global Internet Filtering* 5, 9, 12 (2008). Tania Branigan, *China Blocks Twitter, Flickr and Hotmail Ahead of Tiananmen Anniversary*, THE GUARDIAN (June 2, 2009) http://www.guardian.co.uk/technology/2009/jun/02/twitter-china [https://perma.cc/8F9S-FQWX].NPR Interview with Adrian Zenz, *China Suppression of Uighur Minorities Meets U.N. Definition of Genocide, Report Says* (July 4, 2020), https://www.npr.org/2020/07/04/887239225/china-suppression-of-uighur-minorities-meets-u-n-definition-of-genocide-report-s [https://perma.cc/LL27-WSQJ].

to the character.[175] China's censors tend not to tolerate ridicule of the country's leader.[176] The CCP argues that these internet censorship practices are desirable as they help to maintain social order, productivity, and stability.[177]

China's surveillance regime foundation is based on the "Golden Shield Project," which is a digital surveillance network that covers all means of security across the country.[178] Since 2006, this system has connected Chinese surveillance networks, including local police station surveillance, security cameras, data management centers, and internet cafés.[179] Notably, this system is particularly effective when combined with the government's implementation of real-name registration rules, which require internet users to disclose their identities when accessing the internet, thus holding them accountable and encouraging "responsible" internet use.[180]

Further, the introduction of facial recognition technology has become unignorable in recent years. Using CCTV cameras and artificial intelligence (AI), government databases can filter through millions of citizens' registration pictures to identify individuals.[181] Of course, the use of this technology is justified for safety and law enforcement purposes. When a person is wanted for a crime, authorities may locate them any time they appear in a public place. A notable example of this was when a man wanted for financial crimes was recognized by this system while he was standing in a crowd of fifty thousand people at a Chinese pop concert.[182] CCTV cameras captured his face, AI distinguished it from the millions of people registered, and he was quickly apprehended.[183]

In Shenzen, a giant billboard displays the registration photo of people that CCTV catches jaywalking, as well as a list of names of people who haven't paid their debts.[184] One Chinese company boasted that its facial recognition technology is 97.7%[185] Another creative example with known use is the robotic dove.[186] The bird-like drones fly just as a real bird would and reportedly to go undetected, even in other animals' presence.[187] With

---

[175] Stephen McDonell, *Why China censors banned Winnie the Pooh*, BBC NEWS (July 17, 2017), https://www.bbc.com/news/blogs-china-blog-40627855 [https://perma.cc/QPR6-B38B].
[176] *Id.*
[177] *China, in Access Controlled, supra* note 172, at 12-13.
[178] ONI China, at 282; *See also* Trina K. Kissel, License to Blog: Internet Regulation in the People's Republic of China, 17 INT'L & COMP. L. REV. 229, 236 (2007) (discussing regulations developed by CPP that hold "many entities and individuals accountable for accessible content on the Internet").
[179] ONI China, at 283; *See* Christopher Stevenson, *Breaching the Great Firewall: China's Internet Censorship and the Quest for Freedom of Expression in a Connected World*, 30 BC INT'L & COMP. L. REV. 531, 538 (2007)
[180] Jyh-An Lee & Ching-Yi Liu, supra note 132, at 126.
[181] Zhang, *supra* note 169.
[182] *Id.*
[183] *Id.*
[184] Paul Mozur, *Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras*, N.Y. TIMES (July 8, 2018), https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html [https://perma.cc/NK3Q-89R8].
[185] Zhang, *supra* note 169.
[186] Stephen Chen, *China takes surveillance to new heights with flock of robotic Doves, but do they come in peace?*, The South China Morning Post (June 2018), https://www.scmp.com/news/china/society/article/2152027/china-takes-surveillance-new-heights-flock-robotic-doves-do-they [https://perma.cc/G7T9-PAYN].
[187] *Id.*

this vast array of technology encroaching on every facet of citizens' lives, it is hard to imagine any "privacies of life" that are truly safe.[188]

D. Effect on Hong Kong

The border between the mainland city of Shenzen and the island of Hong Kong is not separated by a physical wall, but a digital one.[189] While the mainland is controlled by internet filters, surveillance, and facial recognition, Hong Kong's internet is still open and unabated.[190] Although the PRC's electronic dragnet has closed in on Hong Kong, protestors have been quick to fight against the comprehensive system. Fearful of the encroaching surveillance presence, CCTV cameras are painted, covered, and smashed to prevent the AI surveillance from taking over the city.[191]

As described above, numerous anti-government behaviors have been declared illegal.[192] The laws are broadly written, and many protestors will be tracked down and prosecuted if the "Golden Shield" systems take control of Hong Kong.[193] For example, a person will be deemed guilty under Article 29 of the NSL if they commit any of the following offenses: (1) threatening to use force to undermine, and territorial integrity of the PRC; (2) disrupting the formulation and implementation of laws or policies… by the Central People's Government; (3) engaging in hostile activities against the… PRC government; (4) provoking by unlawful means the hatred among Hong Kong residents towards the Central People's Government.[194]

The combination of strict National Security Laws and comprehensive, unavoidable surveillance technology would fundamentally change the freedoms that the people of Hong Kong have enjoyed. Strict regulation of speech, protest, and freedom of information would be implemented, and those who had been involved in anti-mainland activities would have "big brother" watching them at every turn.

In addition, when Hong Kong citizens retreated from the protests to voice their opposition at voting polls, Beijing responded with oppressive, controlling policies.[195] A senior Communist Party official recently announced that China's national legislature planned to "rewrite election rules in Hong Kong to ensure that the territory was run by patriots, which Beijing defines as people loyal to the national government and Communist Party."[196] Pro-democracy candidates had hoped to win a majority in the Hong Kong legislature in the September 2020 elections in order to block budgets; force communist-backed leader, Carrie Lam, to resign; and fight

---

[188] *Carpenter*, 138 S. Ct. at 2214 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)).
[189] Mozur & Qiqing, *supra* note 4.
[190] *Id.*
[191] *Id.*
[192] Congressional Research Service, *supra* note 146.
[193] *Id.*
[194] *Id.*at 12.
[195] Keith Bradsher & Austin Ramzy, *Demanding Loyalty, China Moves to Overhaul Hong Kong Elections*, N.Y. TIMES (March 4, 2021), https://www.nytimes.com/2021/03/04/world/asia/china-hong-kong-election-law.html [https://perma.cc/99QW-D5N7].
[196] *Id.*

to preserve the city's relative autonomy.[197] Communist officials claim that these actions equated to "interfering with government functions," which is an offense under the NSL.

These additional moves seek to solidify mainland China's power in Hong Kong and crush any hopes of the free and open elections that residents have sought after since Britain returned the territory to Chinese rule in 1997. Thus, the watchful eyes of the CCP are close to asserting their unabated surveillance control over Hong Kong in the near future.

VI. POLICY COMPARISONS AND IMPLICATIONS

There are significant differences between PRC and U.S. implementation, enforcement, oversight of surveillance, and data collection. While the U.S. has sought to implement safeguards and oversight, with the Fourth Amendment extending to digital surveillance, many government agencies are still operating behind closed doors, and the extent of their power is largely unknown.

Although the PRC policies described above may create allusions to an Orwellian dystopia, Chinese policy only varies slightly from those of the U.S. While the U.S. creates exceptions to privacy in their hunt for terrorists, the PRC does the same under less ambiguous labels. Both governments have unfettered access to a wide array of private data when national security is involved. Thus, the question becomes: which system is more appealing to private citizens, and why? Is it more valuable for a citizen to know that a government is actively watching them? Or is it more attractive for citizens to put their faith in the law that relies on the fact that the government is not watching, even if they are?[198]

A. U.S. Capitol Protests

To many Americans, the invasion of the U.S. Capitol building on January 6, 2021, was a shocking attack on the foundations of American democracy. However, a substantial population of Americans may have considered the attack on the U.S Capitol to be a heroic, last-ditch effort to uphold a strong nationalist American under Donald Trump.[199] This subtle shift in perspective can change one's understanding of the government's use of surveillance technology after the Capitol riots from a necessary use of technology to a dangerous slippery slope.

After the September 11 terrorist attacks in NYC, it seemed clear that America needed to act quickly. Thus, the USA PATRIOT Act was born.[200] After Trump supporters stormed the Capitol, there was as similar reaction. People needed to be held accountable, and cell phone data collection was

[197] Austin Ramzy, et al., *Hong Kong Voters Defy Beijing, Endorsing Protest Leaders in Primary,* N.Y. TIMES (July 13, 2020), https://www.nytimes.com/2020/07/13/world/asia/hong-kong-elections-security.html [https://perma.cc/X5VF-BG6L].
[198] Fry, *supra* note 10.
[199] Jim Rutenberg et al., *77 Days: Trump's Campaign to Subvert the Election,* N.Y. TIMES (Feb. 12, 2021), https://www.nytimes.com/2021/01/31/us/trump-election-lie.html [https://perma.cc/4VT4-52BA]. The authors point out that the Capitol riots were the culmination of 77 days of Donald Trump planting seeds of election fraud before and after the U.S. presidential election.
[200] END MASS SURVEILLANCE UNDER THE PATRIOT ACT, *supra* note 62.

the best method. However, it has been argued that "[t]he data collected on Jan. 6 is a demonstration of the looming threat to our liberties posted by a surveillance economy that monetizes the movements of the righteous and wicked alike."[201]

Almost forty percent of the phone data linked to Trump's rally stage on the National Mall was found in and around the Capitol building during the siege.[202] Many rioter's cell phones connected to the cellular and wireless data infrastructure under the Capitol building upon arrival.[203] These individual cell towers quickly turned each person's phone into a tracking device as investigators identified each cellphone that connected to the localized network.[204] In addition, DOJ officials stated that investigators used facial recognition to identify rioters from the video and photo evidence from Capitol building cameras and social media postings.[205]

However, soon after these events, a source came to *The New York Times* with similar cell phone tracking data.[206] Although this was a private citizen, the data they provided "showed what some in the tech industry might call a God-view vantage of that dark day."[207] Not only were the protestors tracked from Trump's rally to the Capitol building, but the source was able to track individual's movements to and from their home states.[208]

On the one hand, law enforcement's cell phone data collection brought many rioters to justice. Without it, many people who stormed the Capitol building could have returned to their home states and never faced repercussions. Again, it can be argued that there are legitimate uses of broad data collection methods, with this being a prime example. On the other hand, "to think that the information will be used against individuals only if they've broken the law is naïve; such data is collected and remains vulnerable to use and abuse whether people gather in support of an insurrection, or they justly protect police violence."[209]

A shift in perspective, candidate, or political ideology, can quickly change one's view of the U.S. Capitol attack from an assault on democracy, to a heroic effort led by impassioned freedom fighters. The same goes for Hong Kong. To some, the anti-mainland rebels were simply

---

[201] Warzel & Thompson, *supra* note 11.
[202] *Id.*
[203] Craig Timberg, et al., *Police let most capitol rioters walk away. But cellphone data and videos could now lead to more arrests.*, WASH. POST (Jan. 8, 2021), https://www.washingtonpost.com/technology/2021/01/08/trump-mob-tech-arrests/ [https://perma.cc/FK9J-S6MW].
[204] *Id; see also* Carpenter v. United States, 138 S. Ct. 2206, 2217, 201 L. Ed. 2d 507 (2018) (in *Carpenter*, the Court ruled that an individual maintains a legitimate expectation of privacy in the records of his physical movements as captured through CSLI (Cell-site location information) and cell phone carrier data; and would thus need a warrant based on probable cause to track these individuals).
[205] Warzel & Thompson, *supra* note 11.
[206] *Id.*
[207] *Id.*
[208] *Id.*
[209] *Id.*

troublemakers.[210] To others, it was the territory's last chance at maintaining a semi-autonomous, democratic haven. The blurring of these moral lines between a righteous protest and a misguided one – only convolutes the discussion of justified government data access.

B. National Security Justifications

In both countries, the invasion of individual privacy rights has been justified under a consistent group of key words: "national security," "terrorism," "undermining sovereignty," and "collusion with foreign power" are a few examples. The question becomes: at what point is a passionate anti-government rioter a terrorist, and how much trust should citizens put into law enforcement agencies?

National security intelligence is about staying a step ahead of potential threats. During the Napoleonic Wars, the French created innovative land-based communication systems using towers that sent line-of-sight signals from tower to tower along the coast, decreasing communication time between bases and frontlines.[211] This information allowed the French to re-route forces, send supplies, and warn allies faster than any of their counterparts.[212] Recent wars in the Middle East have utilized predator drone imaging to produce multi-hour surveillance footage, revealing enemy encampments, supply lines, and geographic features.[213] This actionable information, which allows a government to be one step ahead of a threat, has always been a part of national security.[214] However, our modern age has changed the form of this actionable information and has made it more challenging than ever to uncover what is necessary for security.

Denis Clift, former Chief of Staff for the U.S. Defense Intelligence Agency, describes this modern perspective:

> The need for information superiority is, in many instances, is causing U.S. intelligence to take dramatically new approaches. The Internet era has become the Intelligence Communities new strength as well as its new challenge. Cold War assumptions driving intelligence collection and analysis- those enemy targets were closed societies and that superpower rivalry trumped all other issues- are assumptions of the past.[215]

Potential threats are no longer limited to major superpowers and can no longer be handled through traditional, direct methods.[216] True terroristic

---

[210] Ringo Yee & Tuen Mun, *Hong Kong is a better, safer city with national security law in place,* SOUTH CHINA MORNING POST (Nov. 7, 2020), https://www.scmp.com/comment/letters/article/3108719/hong-kong-better-safer-city-national-security-law-place [https://perma.cc/R4Y6-FPDF].
[211] Stephen E. Maffeo, *Most Secret and Confidential*, NAVAL INST. PRESS 68, 69 (2000).
[212] *Id.*
[213] Denis Clift, *Intelligence in the Internet Era,* CIA ARCHIVES 73, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB436/docs/EBB-008.pdf [https://perma.cc/828S-PNXG].
[214] *Id.*
[215] *Id.* at 76.
[216] Yoo, *supra* note 20 at 903.

threats are hard to detect ahead of time and this requires intelligence services to comb through an incredible amount of digital information. An example may be the bulk data collection deemed unconstitutional in *Moalin.*[217] Although individuals connected to *Moalin* were affected by the broad data collection, the suspect was caught, and law enforcement prevented U.S. residents from funding a Somali terrorist organization.[218]

After over a full year of protests, civil unrest, and economic disruption, some Hong Kong citizens are grateful for the National Security Laws.[219] One letter to the editor stated, "the national security law has helped make Hong Kong peaceful again. Complaints about suppression of freedom are not based on the full facts. Also, has your reader seen how those '[w]estern countries react to their own protestors?"[220] While some citizens may be relieved that life may be returning to some degree of normalcy, the system they are returning to is far different from its predecessor. The policies imposed by the PRC may provide safety and security for now, but the suppression of speech, censorship of information, and ever-watchful facial recognition technology will undoubtedly persist.

VII. SOLUTIONS

The USA FREEDOM Act was a major piece of bipartisan legislation. It closed the loophole allowing the NSA to engage in "warrantless searches for the phone calls or emails of law-abiding Americans" by bringing more transparency to the FISC and created an advocate for members of the public to represent them before the FISC.[221] As described above, the Act creates additional oversight within FISC, which promotes transparency for non-classified materials, and bans bulk metadata collection. [222] Additionally, case law has acknowledged privacy abuses in *Moalin* and *Carpenter*, and courts have emphasized the importance of Fourth Amendment Rights in our digital age.[223]

However, the U.S. has yet to enact comprehensive privacy law. While the European Union's omnibus General Data Protection Regulation (GDPR) stands as a model for the rest of the world, U.S. industry-specific privacy laws only provide piecemeal protection.[224] "[B]ig tech companies have an immense economic interest in making sure any online privacy regulations are weak and do not limit their business models… because knowledge, to them, can also equal power."[225] Because Congress is still

---

[217] *Moalin*, 973 F.3d at 985.
[218] *Id.*
[219] Yee & Mun, *supra* note 211.
[220] *Id.*
[221] James Ball & Spencer Ackerman, *NSA Loophole Allows Warrantless Search for US Citizens' Emails and Phone Calls*, THE GUARDIAN, 68, 69 (Aug. 9, 2013), http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls [https:perma.cc/B8KK-5L9E].
[222] The USA Freedom Act, 1 Policies and Practices § 63:6.
[223] *Carpenter*, 138 S. Ct. at 2217 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).
[224] Examples include: U.S. Privacy Act of 1974; Health Insurance Portability and Accountability Act of 1996 (HIPPA); Gramm-Leach-Bliley Act of 1999 (GLBA); and Children's Online Privacy Protection Act of 1998 (COPPA).
[225] Robert E.G. Beens, *The Privacy Mindset of The EU Vs. The US*, FORBES (July 29, 2020, 7:40 AM), https://www.forbes.com/sites/forbestechcouncil/2020/07/29/the-privacy-mindset-of-the-eu-vs-the-us/?sh=215fd37a7d01 [https://perma.cc/5JZ2-KWT2].

largely polarized, it seems that an omnibus federal data privacy law is still far from certain. Although, many progressive states have moved forward with their own comprehensive privacy laws, including California, Colorado, and Virginia.[226]

The new technologies being demonstrated in the PRC and Hong Kong are not limited to their continent. There is little doubt that similar practices will begin to be used in the U.S., and if privacy laws are not implemented beforehand, residents may be subject to Fourth Amendment violations before the public ever becomes aware.

Concerns over the use of facial recognition technology (FRT) can only be addressed by appropriate oversight, assessment, and careful implementation. While comprehensive federal law would be ideal, the Center for Strategic International Studies has stated that "each level of government that authorizes the use of FRT will need some oversight mechanism… FRT use will need to be accompanied by some assessment of the effects on privacy, both before deployment and on a regular basis after employment."[227]

Portland, Oregon became the first jurisdiction in the country to ban the commercial use of facial recognition technology in public places within the city, including stores, restaurants, and hotels. Beginning January 1, 2021, "private entities" will be prohibited from using "face recognition technologies" in "places of public accommodation" within Portland, except: "(1) to the extent necessary to comply with federal, state, or local laws; (2) for user verification purposes to access the user's own personal or employer-issued communication and electronic devices; or (3) in automatic face detection services in social media applications."[228]

Lastly, checks and balances can erode quickly. The Trump era was a stark example of how the executive branch can fire agency officials and quickly replace them based on loyalty rather than accountability. [229] Without executive integrity and agency oversight, broad discretionary

---

[226] *US State Privacy Law Update – June 11, 2021*, NAT'L LAW REV. (June 11, 2021), https://www.natlawreview.com/article/us-state-privacy-law-update-june-11-2021 [https://perma.cc/8992-YJSZ].

[227] James Andrew Lewis, *Facial Recognition Technology: Responsible Use Principles and the Legislative Landscape*, CENTER FOR STRATEGIC INT'L STUD. (Sept. 29, 2021) https://www.csis.org/analysis/facial-recognition-technology-responsible-use-principles-and-legislative-landscape [https://perma.cc/2BFV-HBF6].

[228] Hunton Andrews Kurth LLP., *Portland, Oregon Becomes First Jurisdiction in U.S. to Ban the Commercial Use of Facial Recognition Technology*, NAT'L L. REV. (Sept. 10, 2020), https://www.natlawreview.com/article/portland-oregon-becomes-first-jurisdiction-us-to-ban-commercial-use-facial [https://perma.cc/W7JT-LVSU]

[229] Michael Ellis was appointed as a general counsel at the NSA, despite objections from NSA director, Gen. Paul M. Nakasone. "These are the people who go in and do whatever they think is required to achieve his agenda... They are true soldiers in the war on government, the war on what Trump calls the deep state." David E Sanger & Eric Schmitt, *Trump Stacks the Pentagon and Intel Agencies With Loyalists. To What End?*, N.Y. TIMES (Nov. 16, 2020), https://www.nytimes.com/2020/11/11/us/politics/trump-pentagon-intelligence-iran.html [https://perma.cc/7FRP-BHJE]; John Ratcliffe is another top-level appointee who was thrusted to a high-level position when he was appointed as US Director of National Intelligence. "Democrats said they were skeptical that Ratcliffe would be an independent leader, despite his assurances during his confirmation hearing. The Republican has been an ardent defender of the president through House impeachment and investigations into Russian interference." *Trump Loyalist John Ratcliffe Confirmed as New US Intelligence Chief*, A.P. WASH. (May 21, 2020), https://www.theguardian.com/us-news/2020/may/21/john-ratcliffe-trump-director-of-national-intelligence [https://perma.cc/KMN2-CL7D].

power can result in abuse. Only the implementation of legislation narrowly tailored to privacy rights, backed by a high level of accountability and judicial oversight, will protect average citizens from the abuses of power our digital era has created. Few courts should operate in secret. Independent government agencies must review those handling the most sensitive national security concerns. The consequences of broad and unchecked surveillance power abuses are too great, and each inquiry which breaches an innocent American's rights must be justified under a high level of scrutiny.

IX. CONCLUSION

Globalization and technology have changed the way our society functions at all levels. With new national security threats, greater surveillance capabilities, and more information centered around the digital sphere than ever, maintaining a balance between transparency and security has become increasingly challenging.

The events in Hong Kong have provided a revealing example of the swift action a government can use to control a territory when seemingly justified. The PRC's combination of surveillance methods touches on many aspects of life: public, online, and private. Only Hong Kong's people can decide where their value systems lie and what rights are worth taking risks for. If push comes to shove, international condemnation may be a critical factor in determining Hong Kong's fate.

In the U.S., the law must continue to adapt to new technologies to preserve the privacies of life that people have fought to protect for so many years.[230] "Protection against such invasion of the sanctities of man's home and privacies of life was provided in the Fourth and Fifth Amendment by specific language. But time works changes, brings into existence new conditions and purposes."[231] Nevertheless, the current privacy law is far behind the conditions and purposes of the twenty-first century. Thus, each individual's right to privacy should be considered sacred moving forward, because once the flood gates have opened and everyone's digital profile is accessible, monitored, and tracked, there is no going back.

[230] *Carpenter*, 138 S. Ct. at 2217 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)). *Olmstead*, 277 U.S. at 466.
[231] *Id.* at 479 (quoting Boyd v. United States, 116 U.S. 626 (1886)).