3-2021

DIGITAL DOMINION: How the Syrian regime's mass digital surveillance violates human rights

Sarah Dávila-Ruhaak
UIC John Marshall Law School, sdavila@uic.edu

Nino Guruli
UIC John Marshall Law School

UIC John Marshall Law School International Human Rights Clinic

Dima Samaro
Access Now

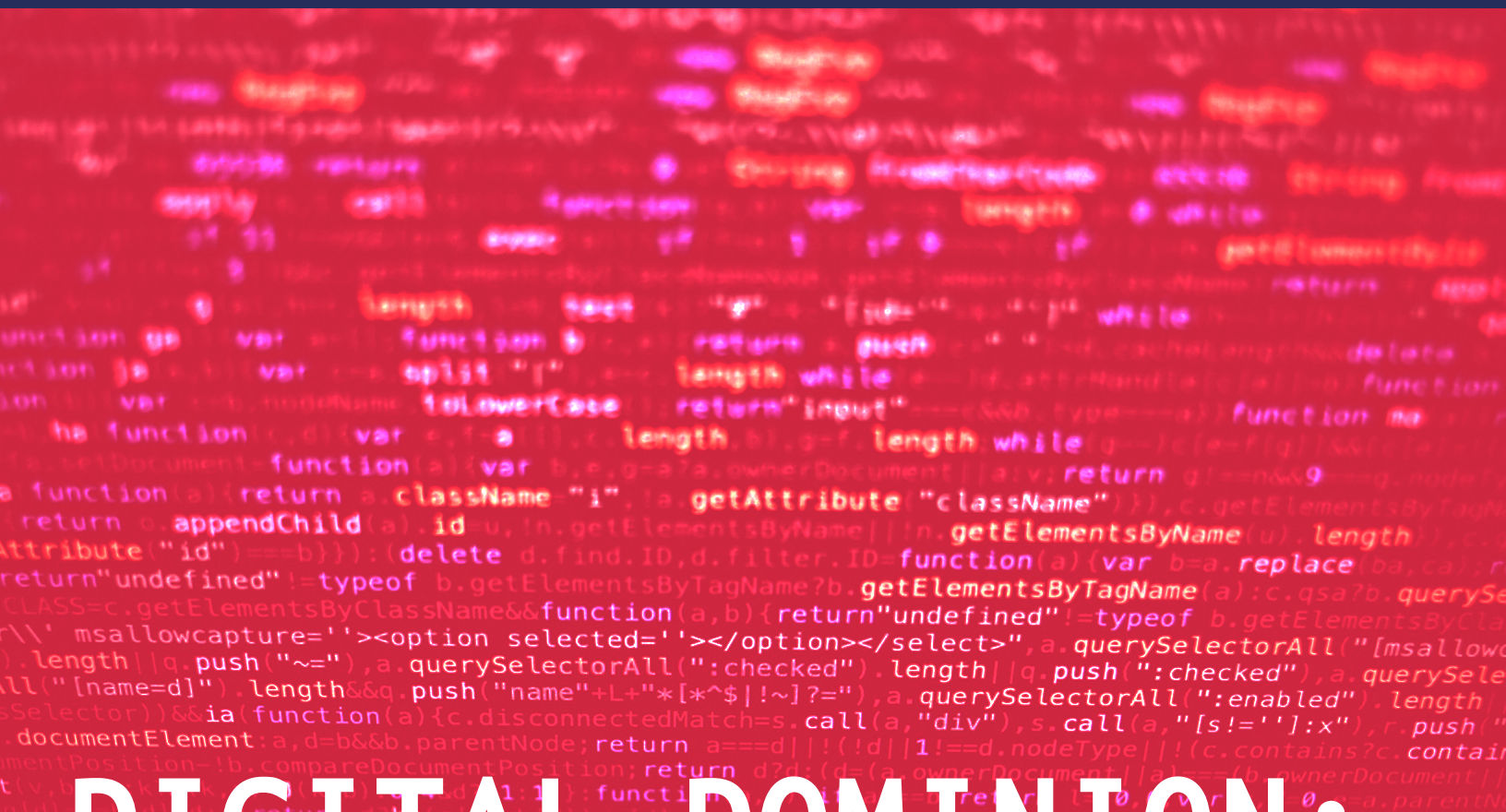
Access Now

accessnow

MedGlobal

UIC LAW

Syria Justice and Accountability Centre



DIGITAL DOMINION:

How the Syrian regime's mass digital surveillance violates human rights

March 2021

Contact:

Sarah Dávila-Ruhaak
Nino Guruli

UIC John Marshall Law School
International Human Rights Clinic
300 South State Street
Chicago, Illinois, USA 60604
Tel. +1 (312) 386-2888
sdavila@uic.edu

Dima Samaro

Access Now
463 Lincoln Place #241
Brooklyn, New York 11238
dima@accessnow.org

ABOUT THE AUTHORS

UIC John Marshall Law School International Human Rights Clinic

The UIC John Marshall Law School International Human Rights Clinic (IHRC) is a nonprofit, nonpartisan law school legal clinic dedicated to promoting and protecting human rights in the United States and around the world. The IHRC offers students a background in human rights advocacy through the practical experience of working in international human rights cases and projects.

Access Now

Access Now (https://www.accessnow.org) defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, legal interventions, and convenings such as RightsCon, we fight for human rights in the digital age.

Other Contributors:

Michael Drake
Marshall Janevicius
Abigail Simmons
Maritza Jaimes
Clayton Dant
Michael Hopkins
Michael Lynn

Digital Design Contributors:

Ryan Ruffatti
Salome Guruli

Supporting Organizations:

Syrian Justice & Accountability Centre
MedGlobal

TABLE OF CONTENTS

I. Introduction

"Privacy is not an option, and it shouldn't be the price we accept for just getting on the Internet." – Gary Kovacs[1]

The Assad regime conducts mass electronic and digital monitoring of its people. Anyone who dares to voice opposition or fails to proclaim their loyalty is deemed dangerous and quickly falls under suspicion. The privacy, freedom of expression, and the life and safety of millions has been imperiled by a government desperate to control the narrative. A sprawling infrastructure of surveillance, from control of Internet Service Providers (ISP), mobile service providers to aggressive hacking and tracking operations, has facilitated the monitoring, detention, and persecution of critics, journalists, and human rights defenders. This report exposes the monitoring carried out by the Syrian government in order to contribute to accountability for human rights violations and to promote the protection of the right to privacy, so essential for the realization of other rights.

The Assad regime has been able to conduct mass surveillance, in part, because it exercises complete control over the country's internet activity through the government controlled and regulated telecommunication infrastructure. The state-owned Syrian Telecommunications Establishment ("STE") is both an internet service provider (ISP) and the official telecommunications regulator. In 2007, the STE solicited bids for a Central Monitoring System with the "the ability to monitor *all the networks which use data communication services inside the Syrian territories."*[2] The resulting infrastructure provided the government power to monitor all traffic and to stockpile data for identifying and targeting individuals critical of the regime. [3] Since then, the Assad regime has continued to strengthen this invasive infrastructure by adding content filtering systems to combat political speech, cutting or "blacking out" internet access and service during the uprising and protests, blocking websites critical of or exposing corruption within the Assad regime, as well as temporarily blocking popular websites and online services such as YouTube, Facebook, and Skype. [4]

In conjunction with actively monitoring their own citizens, the Syrian regime, together with third party groups, is hacking websites and individuals critical of the regime. A group that calls themselves the Syrian Electronic Army ("SEA") is one such state-sanctioned hacking group that targets major news organizations and NGOs as well as local opposition groups and individual activists.[5] Through "phishing" operations, social engineering, malware downloads, and gaining access to passwords and networks through security force intimidation, the SEA and the Assad regime have used these practices to monitor and track down activists and human rights defenders in Syria, who are then tortured and killed. Bashar al-Assad, Syria's president, has publicly recognized the SEA and the support it has provided the regime by surveilling their dissenters and others who oppose the Syrian regime.[6]

---

[1] *See*, Gary Kovacs, *Tracking Our Online Trackers*, TED2012 (Feb. 2012), available at: https://www.ted.com/talks/gary_kovacs_tracking_our_online_trackers/transcript?language=en

[2] *Open Season: Building Syria's Surveillance* State, PRIVACY INTERNATIONAL, (Dec. 2016), available at: https://privacyinternational.org/report/1016/open-season-building-syrias-surveillance-state.

[3] *See, e.g.*, Zack Whittaker, *Surveillance and Censorship: Inside Syria's Internet*, CBS (Dec. 12, 2013), available at: https://www.cbsnews.com/news/surveillance-and-censorship-inside-syrias-internet/ ("[e]very single piece of traffic that goes through [the Syrian network] is being recorded to hard disk drives.").

[4] *Freedom on the Net: Syria* 2019, FREEDOM HOUSE, available at: https://freedomhouse.org/country/syria/freedom-net/2019.

[5] Max Fisher, *Syrian Hackers Claim AP Hack that Tipped Stock Market by $136 Billion. Is it Terrorism?*, WASH. POST (Apr. 23, 2013), https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/?utm_term=.e4be4274574a.

[6] Danny O'Brien, *Syria's Assad Gives Tacit OK to Online Attacks on Press*, COMMITTEE TO PROTECT JOURNALISTS (Jun. 24, 2011), available at: https://cpj.org/blog/2011/06/syrias-assad-gives-tacit-ok-to-online-attacks-on-p/ (recounting a speech in which Bashar al-Assad referenced the SEA).

This report details how the Syrian regime proactively monitors dissenters, either directly or through non-state actors, and how that digital monitoring facilitates the broader campaign of control and violence leading to arrests, torture, forced disappearances, and death of Syrian people. The report begins, in Section II, by providing the background on the infrastructure of surveillance and key state and state-sanctioned actors involved in surveillance activities. Next, Section III outlines the human rights implicated and being violated by the states campaign of mass surveillance and violence. Finally, Section IV identifies the direct violation of the rights of Syrian people and human rights defenders that result from this surveillance. An enabling legal and institutional infrastructure has facilitated both the mass surveillance and the accompanying violence carried out by the regime. As a result, human rights defenders, critics, and journalists, have been censored, monitored, hacked and tracked. This targeting has facilitated the detention, torture and extrajudicial killings of countless individuals. The purpose of the report is to document the systematic use of surveillance by the Syrian regime, the human rights violations suffered by those who have been surveilled, and to call upon the international community to seek accountability in Syria.

This Report seeks to shed light on the legal, political, and technological context in which surveillance is used to violate human rights. In doing so, advocates and the global community must push forward reforms to limit the use of surveillance to monitor and punish human rights activists. The analysis in this report provides a framework which journalists and others documenting the violence and human rights crisis in Syria may use to continue reporting on the regime's use of surveillance of the Syrian people. Finally, by documenting the current situation in Syria, this report hopes to inform broader conversations on state-sponsored surveillance and how it endangers activists and others who speak up against governments and powerful actors. The Assad regime's use of surveillance as a critical tool to intimidate and eliminate opposition must serve as a warning to the global community of the dangerous effects of the unchecked and broad powers of surveillance to silence and eliminate opposition. Countless critics, journalists, students, and others have been surveilled and persecuted for exercising their human rights to expression and association. This report is only the beginning of this broader conversation about the need to press for limitations in the use of surveillance and to hold the Syrian State accountable for the countless abuses that the Syrian people have endured.

II. Factual Background: Telecommunications Infrastructure and Key Players

The internet provides an essential platform for populations and governments to communicate, share ideas, and access essential information, services and networks. Much of today's communication, organizing, and collaboration happens on digital networks, through email, Voice-over-Internet Protocol applications and services (VoIP-like WhatsApp), social media accounts, and online platforms. As of 2010, almost 2 billion people around the world had access to the internet through computers or mobile devices.[7] In 2010, only 17.7% of the Syrian population, or 3.9 million individuals, had access to the internet.[8] This number has dropped significantly over the last ten years. In 2020, only 4.2% of the Syrian population had access to the internet.[9] Syria ranked as 12th out of 14 Middle Eastern countries, in terms of population percentage that uses the internet.[10] The number of mobile users or connections is significantly higher. As of January 2020, according to Data Reportal, the number of mobile internet users was 5.75 million, or 31% of the total population.[11] Mobile phones have played a key role in

[7] Roser, Max, et al. *Internet*. OUR WORLD DATA, available at: https://ourworldindata.org/internet.
[8] *Internet Usage in the Middle East*, INTERNET WORLD STATS, available at: https://www.internetworldstats.com/stats5.htm.
[9] *Internet Usage in the Middle East*, *supra* note 8.
[10] *Internet Usage in the Middle East*, *supra* note 8.
[11] Simon Kemp, *Digital 2020: Syria,* DATAREPORTAL (Feb. 18. 2020), at: https://datareportal.com/reports/digital-2020-syria.

Syria, "enabling 'citizen journalists' to capture events on the ground…[which] have served as a crucial source of information on the uprising."[12] Social media and other platforms are primarily used to disseminate information, to follow unfolding events, and to voice opinions and support for movements or ideas.[13]

A. The Infrastructure of Surveillance

The Syrian telecommunications market is the most restricted and regulated among all Middle Eastern countries, based on the percentage of State-owned telecommunications infrastructure.[14] The state-owned Syrian Telecommunications Establishment ("STE") is both an internet service provider (ISP) and the official telecommunications regulator. STE has a monopoly over wired and wireless services throughout the regime controlled areas of the country.[15] While the state has licensed to other smaller private providers, these providers rely on government infrastructure and are subject to state regulations.[16] Through this control, the regime not only censors information based on political, social, and religious beliefs, but can also conduct surveillance of internet users in Syria.[17] In essence, the STE provides the government control over what content the population can and cannot interact with on the internet.

In 2007, Nazem Bahsas, the head of the STE, solicited bids from companies to build a new "Central Monitoring System for public data networks and the Internet."[18] In 2008, the Syrian government solicited more requests for bids to build its surveillance system,[19] which would be a content filtering system[20] combatting politically inopportune speech.[21] Content filtering allows for the analysis of communication data packets through key words or attributes, which can then be stored for further analysis, blocked, or allowed to pass through without being stored. Alarmingly, Bahsas requested and clarified that this new system would be centralized so that it could have the capability of monitoring all telecommunications data inside Syria.[22] Additionally, Bahsas demanded real time location tracking ability of up to fifty targets and that the monitoring be completely undetected by the Syrians who are being monitored.[23] In other words, the Syrian regime sought the capability to select any Syrian individual for any reason, monitor every website they visit, track their mobile device to determine their real time location, and do all of this without the individual knowing they are being tracked.[24] While the STE claimed this authority was needed to ensure system security from hacking and foreign and domestic infiltration, the power to surveille that this system delivered for the regime and the subsequent targeting, torture and killing of dissenters tells a different story.[25]

In December 2008, the Syrian regime explained to prospective bidders that it was not interested in combating "classic spam."[26] Rather, it was concerned with "propaganda mail which has the shape of spam."[27] Within the context of the state-run STE system, this is troubling. Because the government has the power to determine what

---

[12] Olesya Tkacheva et. al, Internet Freedom and Political Space (2013) 85.
[13] *Id.* at 86.
[14] *Syria*, OpenNet Initiative (Aug. 7, 2009), available at: https://opennet.net/research/profiles/Syria.
[15] OpenNet Initiative, *supra* note 14.
[16] Tkacheva, *supra* note 12, at 85.
[17] OpenNet Initiative, *supra* note 14.
[18] *Open Season*, *supra* note 2.
[19] *Open Season*, *supra* note 2, at 16.
[20] *Open Season*, *supra* note 2, at 16 *("*Content filtering, in the context of communications traveling across the PDN and the internet, means analyzing the communications data packets and assessing them for key words or attributes, and then either blocking transmission of that message, storing a copy for further analysis, or letting the message pass through without storage. Such technologies are also widely used for censorship, particularly at politically sensitive moments, such as during public protests.").
[21] *Open Season*, *supra* note 2.
[22] *Open Season*, *supra* note 2 (emphasis added).
[23] *Open Season*, *supra* note 2, at 14.
[24] *Open Season*, *supra* note 2.
[25] *Open Season*, *supra* note *2.*
[26] *Open Season*, *supra* note 2, at 17.
[27] *Open Season*, *supra* note 2.

constitutes “propaganda mail”, it has the authority to impose severe censorship on those it deems critical of or a threat to the regime. Furthermore, since the network infrastructure is completely run by the government, Syrian individuals have no opportunity to view content deemed as “propaganda mail” nor to decide for themselves whether to view it or not.[28]

According to Fredric Jacobs, a researcher that spent time in Syria, “[e]very single piece of traffic that goes through [the Syrian network] is being recorded to hard disk drives.”[29] These drives are controlled and stockpiled by the Syrian regime.[30] Throughout the Syrian conflict that began in 2011, reports[31] surfaced indicating that the regime monitored and tracked human rights defenders through digital surveillance in order to arbitrarily arrest, detain, torture, and kill them as a result of their resistance.[32]

Mobile phone access is much more prevalent, making mobile service providers a key part of the telecommunications infrastructure. An estimated 55 percent of the country’s cellular market is dominated by Syriatel, a regime affiliated provider.[33] MTN Syria is the other major mobile service provider, a subsidiary of South African MTN. As outlined in Section IV below, MTN is subject to government regulation and has complied with government orders when it comes to filtering and blocking telecommunications of its users. The regime access to and surveillance of mobile phones is particularly consequential given the role mobile phones, in the hands of activists and human rights defenders, has come to play in bearing witness to the Civil War and ongoing violence in Syria. “The mobile phone has become the star of the popular revolutions…This small instrument has actually become stronger than the television cameras.”[34] Where outside observers and the international media fail to gain access to the country and local reporters and journalists are targeted and silenced, the citizen journalist has become the main witness and recorder of the situation in Syria.

B. Regime Intelligence Agencies

There are four main intelligence agencies in Syria, military and civilian. Their leadership and scope of operations is difficult to precisely identify as these agencies are secretive and the political situation is in constant state of flux.[35] The four agencies are: (1) The Department of Military Intelligence; (2) The Air Force Intelligence Directorate; (3) The General Intelligence Directorate; and (4) The Political Security Directorate.[36] The Military Intelligence and Air Force Intelligence fall under the Ministry of Defense. The General Intelligence Directorate and the Political Security Directorate fall under the remit of the Ministry of Interior. Each agency has multiple branches. The Department of Military Intelligence alone has 20 different branches. This means there are countless intelligence branches with responsibilities ranging from surveilling and controlling military and security

---

[28] *Open Season*, *supra* note *2,* at 16-17.
[29] *Id.*
[30] *Id.*
[31] Nicole Perlroth, *Hunting for Syrian Hackers’ Chain of Command*, NYTIMES (May 17, 2013), https://www.nytimes.com/2013/05/18/technology/financial-times-site-is-hacked.html?pagewanted=all&_r=0 (“Now sleuths are trying to figure out how much overlap there is between the rowdy pranks playing out on Twitter and the silent spying that also increasingly includes the monitoring of foreign aid workers.”).
[32] *See, e.g.*, Whittaker, *supra* note 3 (“[P]eople in Syria were being tracked online, and that information was being used to hunt down protesters.”).
[33] Tkacheva, *supra* note 12, at 85.
[34] “Mashhadiyāt Sūrīya [Vignettes from Syria],” al Hayat, March 26, 2012, quoted in Tkacheva, *supra* note 12, at 85.
[35] Human Rights Watch, *“By All Means Necessary” Individual and Command Responsibility for Crimes Against Humanity in Syria* (2011) 90, available at: https://www.hrw.org/report/2011/12/15/all-means-necessary/individual-and-command-responsibility-crimes-against-humanity (“Given the secretive nature of the Syrian intelligence agencies, it is very difficult to verify information about their structure and commanders.”).
[36] *Id.*

officers, to monitoring and surveilling opposition forces, as well as monitoring and targeting civilian activists and critics.

Within the Department of Military Intelligence there are a number of branches focusing on civilian surveillance and associated operations. For example, according to one report, there is Branch 211 within Military Intelligence, also known as the "Technical Branch or the Automatic Computer Branch or simply the Computer Branch."[37] This Branch monitors online activity and is involved in the blocking and unblocking of websites as well as providing support services to other surveillance branches, including Branch 225.

Branch 225, referred to as the "Communication Branch," is also part of the Department of Military Intelligence, though it's current placement within the state architecture is unclear. Branch 225 focuses on phone communications. It can "[block] specific numbers or [cut] off calls or [disable] SMS services."[38] The Branch can tap phones and surveille mobile phone communications. The Branch can stop a text message once it has been sent but before it arrives to the designated number. Some reports suggest that Branch 225 also monitors internet communications and is at the forefront of the regime's surveillance activities.[39] According to the Violations Documentation Center in Syria, this Branch has ballooned into a full department, affiliated with the Communications Department, and drawing officers from all four intelligence agencies.[40]

These surveillance divisions are part of a larger state architecture of military and security forces involved in the arrest, detention, torture and killing of the Syrian people.

C. The Syrian Electronic Army and Third-Party Hacking

The state infrastructure of surveillance is further supplemented by the monitoring and hacking performed by state affiliated third-party hacking groups.[41] These hacking groups are predominately referred to as "state-sponsored hackers."[42] State-sponsored hackers is a term used broadly to refer to hackers that are aligned with a government.[43] While the prevailing term is "state-sponsored hackers," this report refers to the Syrian Malware Team ("SMT") and Syrian Electronic Army ("SEA") as "state-sanctioned hackers" in order to more clearly reflect the nature of the relationship. The two most prominent state-sanctioned hackers in Syria are the SEA and the

---

[37] *A Report on Branch 215, Raid Brigade Military Intelligence Division—Damascus "A Conflict Between Death and Hope"* Violations Documentation Centre in Syria (Sept. 2013) 6, *available at* https://www.vdc-sy.info/pdf/reports/1380463510-English.pdf.

[38] *See e.g.* Mark Clayton, *Syria's Cyberwars: Using Social Media Against Dissent,* Christian Science Monitor (Jul. 25, 2012), *available at* https://www.csmonitor.com/USA/2012/0725/Syria-s-cyberwars-using-social-media-against-dissent.

[39] Clayton, *supra* note *38.*

[40] *A Report on Branch 215, supra* note 37, at 6.

[41] Third party hacking groups are hacking entities that are not officially governmental but may still be supplying the government with information obtained through hacking. *See, e.g.*, Eva Galperin, Morgan Marquis-Boire, & John Scott-Railton, *Quantum of Surveillance: Familiar Actors and Possible False Flags in Syrian Malware Campaigns*, Electronic Frontier Foundation, available at: https://www.eff.org/document/quantum-surveillance-familiar-actors-and-possible-false-flags-syrian-malware-campaigns (last visited Mar. 10, 2019) (establishing connections between certain Syrian malware and the Syrian government).

[42] *See, e.g.*, Kim Peretti, Emily Poole, & Nameir Abbas, *10 Lessons From US Indictments of State-Sponsored Hackers*, Law360 (Jan. 31, 2019), https://www.law360.com/articles/1123471/10-lessons-from-us-indictments-of-state-sponsored-hackers (outlining recent attacks by hackers with state connections); *see also* Cathal McMahon, *Exclusive: EirGrid Targeted by 'State Sponsored' Hackers Leaving Networks Exposed to 'Devious Attack'*, INDEPENDENT (Aug. 6, 2017), available at: https://www.independent.ie/irish-news/state-sponsored-hackers-targeted-eirgrid-electricity-network-in-devious-attack-36005921.html (discussing state sponsored hackers).

[43] JLT, *What Does State Sponsored Hacking Mean?*, Marsh (Dec. 22, 2017), https://www.jltspecialty.com/our-insights/publications/cyber-decoder/what-does-state-sponsored-hacking-mean; *see also* Tal Kopan, *DNC Hack: What You Need to Know*, CNN (Jun. 21, 2016, 1:30 PM), available at: https://www.cnn.com/2016/06/21/politics/dnc-hack-russians-guccifer-claims/ (Many governments worldwide have high-level cyberespionage groups working for them, who may target secrets from other governments, intelligence agencies, government contractors, think tanks and academics."); Sam Kim, *Inside North Korea's Hacker Army*, Bloomberg (Feb. 7, 2018), available at: https://www.bloomberg.com/news/features/2018-02-07/inside-kim-jong-un-s-hacker-army (Chronicling the lives of hackers that work at the behest of the North Korean government).

SMT.[44] While some reports refer to these two organizations as the same entity, others differentiate the two.[45] SEA is known to be directly linked to the Syrian regime. The exact nature of SMT's connection to SEA and the regime is up for debate. For example, certain members of the SMT have ties to the SEA. Connections like this suggest that the SMT may be a possible offshoot or part of the SEA.[46] Although the extent of their entanglement may be disputed, it is undeniable that both groups provide support to the Syrian regime.[47] In 2011, Assad affirmed the SEA's existence and that its work benefits the Syrian army, calling them the "real army in virtual reality."[48]

In 2011, following anti-government demonstrations and Assad vowing to quash his "opponents with an iron fist" through violence and surveillance, the SEA thanked him for recognizing them and their role in the suppression of dissenters.[49] The SEA warned anti-regime media, "our message to the news agencies and reporters: if you have a shortage of professionals to report the correct news … the hordes of the Syrian Electronic Army will not be forgiving with you."[50] After the SEA released this message, the group continued to target opponents of the regime.[51]

One of the first internationally recognized targets of the SEA was Harvard University.[52] There, the SEA hacked the Harvard homepage and replaced it with an image of Bashar al-Assad and wrote the message: "Syrian Electronic Army were here."[53] The SEA then accused the United States of actively working to overthrow the Syrian government.[54] This anti-U.S. message along with other consistent SEA attacks, and the hacking of Harvard's website, led Harvard University to investigate the domain name of the SEA.[55] Investigation results indicated that the SEA was created by the Syrian Computer Society; a group that was created by Bashar al-Assad prior to him assuming power.[56] The Syrian Computer Society was instrumental in providing the platform for the SEA to accomplish their hacking goals.[57]

The Harvard University hack was only the beginning of SEA's infiltration of foreign entities through hacking. Between 2011 and 2014, the SEA vandalized numerous other websites, including Forbes, CNBC, The Telegraph, The Chicago Tribune, Human Rights Watch, and UNICEF.[58] A message on the homepage of Human

---

[44] *See* Kyle Wilhoit & Thoufique Haq, *Connecting the Dots: Syrian Malway Team Uses Blackworm for Attacks*, FIREEYE (Aug. 29, 2014), available at: https://www.fireeye.com/blog/threat-research/2014/08/connecting-the-dots-syrian-malware-team-uses-blackworm-for-attacks.html.

[45] *See* Wilhoit & Haq, *supra* note 44; *see also* Kaspersky Law Global Research and Analysis Team, Syrian Malware, The Ever-Evolving Threat 31 (2018), available at: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08074802/KL_report_syrian_malware.pdf (hypothesizing that hacker operations are more likely different groups working together).

[46] *See* Wilhoit & Haq, *supra* note 44.

[47] Kaspersky Law Global Research and Analysis Team, *supra* note 45; *see also* 360 *Gold Rat Organization—Targeted Attacks in Syria*, Threat Intelligence Center (Jan. 4, 2018), available at: https://blogs.360.cn/post/SEA_role_influence_cyberattacks.html (describing the relationship between hackers and the Syrian government).

[48] Harding, Luke and Charles Arthur, "Syrian Electronic Army: Assad's cyber warriors." THE GUARDIAN (Apr. 20, 2013), available at: https://www.theguardian.com/technology/2013/apr/29/hacking-guardian-syria-background.

[49] *Id.*

[50] *Id.*

[51] *Id.*

[52] *See* Rodrique Ngowi, *Harvard Website Hacked, Defaced*, A.P. (Sept. 27, 2011), available at: http://archive.boston.com/news/local/massachusetts/articles/2011/09/27/harvard_website_hacked_defaced/ (explaining the details of the hack on Harvard's website, which was conducted in 2011—the same year anti-Assad protests began).

[53] *Id.*

[54] *Id.*

[55] *Id.*

[56] *Id.*

[57] *Id.*

[58] Katrina Bishop, *Global Websites Hacked by Syrian Electronic Army*, CNBC (Nov. 27, 2014), available at: https://www.cnbc.com/2014/11/27/global-websites-hacked-by-syrian-electronic-army.html.

Rights Watch, an NGO dedicated to documenting abuses of human rights in Syria and around the world, said "Syrian Electronic Army Was Here. All Your reports are FALSE!!! Stop lying!!!"[59]

In order to gain access to these websites, the SEA utilized "phishing."[60] While "spear phishing" is targeted towards an individual, often using personal information, "phishing" targets a large group of individuals in an attempt to steal information.[61] In these SEA phishing attacks, hackers sent emails to news outlets and organizations with links embedded with malware capable of transmitting location and intercepting communications.[62] Once the user opened the link, malware installed itself onto the computer or electronic device.[63]

This phishing technique was used by the SEA to hack into the Associated Press ("AP"). After successfully phishing an AP employee, SEA hackers then used the AP's twitter account to publish a false news story, "Breaking: Two Explosions in the White House and Barack Obama is injured."[64] Fortunately, the tweet was quickly determined to be baseless, but the damage had already been done. The initial panic caused by the fake tweet resulted in a loss of "$136 billion in equity market value."[65] Further, the SEA has successfully used these phishing techniques to gain access to the websites of The New York Times, the United Nations Human Rights Council, and Microsoft.[66] One of the SEA hackers, a Syrian national called Peter Romar, was arrested and convicted for participating in these attacks.[67]

The SEA also directed its capabilities and gained access to information on regime opponents and critics within Syria. The SEA shared information of anti-Assad activists' meeting locations and identities directly with the Syrian regime. For example, in 2013 SEA members hacked into the messaging app "Tango" and stole the personal phone numbers, email addresses and contact information for millions of people.[68] While Tango acknowledged a data breach, it did not confirm the extent of the information stolen, nor the method the SEA used to access the data.[69] After obtaining the Tango information, the SEA announced that it would be "handing the information over to its country's government"— the regime. Experts expressed concern that this would almost certainly lead to people being hurt or worse.[70] The SEA also obtained sensitive data about individual activists through other social media platforms and messaging apps.[71] This sensitive data included, people's birthdays, personal serial numbers, ID cards, CVs, and blood types.[72]

---

[59] Max Fisher, *Syria's Pro-Assad Hackers Infiltrate Human Rights Watch Website and Twitter Feed*, WASH. POST (Mar. 17, 2013), available at: https://www.washingtonpost.com/news/worldviews/wp/2013/03/17/syrias-pro-assad-hackers-infiltrate-human-rights-watch-web-site-and-twitter-feed/?utm_term=.9452432eb8b9.
[60] Fisher, *supra* note 5.
[61] *Phishing*, Microsoft Windows available at: https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/phishing#spear-phishing (last visited Apr. 3, 2019).
[62] Fisher, *supra* note 59.
[63] *Id.*
[64] *AP Twitter account hacked in fake 'White House blasts' post,* BBC NEWS (Apr. 24, 2013), available at: https://www.bbc.com/news/world-us-canada-21508660.
[65] *Id.*
[66] Lee Ferran, *Inside the Syrian Electronic Army*, REAL CLEAR LIFE (June 2018), available at: http://www.realclearlife.com/technology/inside-the-syrian-electronic-army/.
[67] Department of Justice, *Syrian Electronic Army Hacker Pleads Guilty*, (Sept. 28, 2016), available at: https://www.justice.gov/opa/pr/syrian-electronic-army-hacker-pleads-guilty.
[68] Jacob Kastrenakes, *Syrian Electronic Army Alleges Stealing "Millions" of Phone Numbers from Chat App Tango*, VERGE (July 22, 2013), available at: https://www.theverge.com/2013/7/22/4545838/sea-giving-hacked-tango-database-government.
[69] *Id.*
[70] *Id.*
[71] *Id.*
[72] *See* John Scott Railton, Daniel Regalado, Nart Villeneuve, *Behind the Syrian Conflict's Digital Frontlines*, 7-9 (Feb. 2015), available at: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-behind-the-syria-conflict.pdf.

SEA has used SMT malware, which some speculate has been developed with some assistance from Russia and/or Iran.[73] SMT malware is capable of remotely turning on a target's phone or computer and extracting files, contact lists, location data, passwords, and, in some cases, has the ability to copy all contents and programs on a user's phone.[74] One expert noted, "the minute you download this it will take control over your computer…[it] can turn on your phone camera, it can extract files" from any electronic device it is installed on.[75] While the older SEA monitoring techniques featured short, abrupt—often unsophisticated—messages accompanying the attack, alerting the user;[76] the new malware runs and functions like professional, legitimate programs, resulting in the user being less likely to know they are being monitored or had any sensitive information stolen.[77]

D. Mass Surveillance and Persecution

The regime controlled telecommunications infrastructure and a drove of state and state-sanctioned surveillance forces have empowered the Assad regime to conduct indiscriminate mass digital surveillance of the Syrian population.[78] The Syrian Ministry of Communications has created a network that allows the government nearly complete authority over the internet.[79] The regime monitors all online activity and websites for any content that is anti-regime.[80] As Section IV below shows, the regime then uses any content that it deems "revolutionary" to persecute critics and human rights defenders.[81] The vast and comprehensive scale at which this digital surveillance has occurred and is occurring inside Syria should be a great cause of concern for the international community as a whole.

Section III outlines the human rights implicated by mass surveillance. While the rights of all Syrian people, especially anyone critical of the regime, are endangered and have been breached as a result of surveillance, the rights of human rights defenders have been disproportionately impacted. The right to privacy, freedom of expression and of participation, the right to life and freedom from torture and cruel, inhuman and degrading treatment are all at stake in the regime's, and its affiliated groups', campaign of surveillance and persecution. Section IV identifies how the infrastructure of surveillance together with an enabling legal framework has led to censorship, monitoring, hacking and detention of journalists, activists and human rights defenders.

III. Human Rights and Surveillance

The Syrian regime's control over the telecommunications infrastructure is pervasive and has been deployed to monitor and silence, sometimes permanently, journalists, activists and those working to protect human rights in the country. The human rights of the Syrian people are being breached by the surveillance capacity of the state. The Syrian Arab Republic is a party to the International Covenant on Civil and Political Rights (ICCPR) and the

[73] *But c.f.* Interview by Justin Clark with Dlshad Othman, Security Analyst, (July 26, 2018), available at: https://syriadirect.org/cyber-attacks-and-surveillance-in-assads-syria-they-can-do-whatever-they-want-they-own-the-infrastructure/ ("A lot of people are saying that Russian hackers are helping the Syrian government. And they might help them on the strategic decision-making level, they might give them some advice on what approaches to use to target users, that makes sense, but when it comes to technology, we never saw any similarities between the two states. I don't think the Syrian Electronic Army needs Russian help.").
[74] Railton, *supra* note 72.
[75] *Id*.
[76] Andy Greenberg, *How the Syrian Electronic Army Hacked Us: A Detailed Timeline*, FORBES (Feb. 20, 2014), available at: https://www.forbes.com/sites/andygreenberg/2014/02/20/how-the-syrian-electronic-army-hacked-us-a-detailed-timeline/#d496edcc522c.
[77] Railton, *supra* note 72.
[78] Kastrenakes, *supra* note 68.
[79] *Internet Usage and Marketing Report: Syria*, Internet World Stats (2010) available at: https://www.internetworldstats.com/me/sy.htm. *See also* https://www.nytimes.com/2011/05/23/world/middleeast/23facebook.html.
[80] Jennifer Preston, *Seeking to Disrupt Protesters, Syria Cracks Down on Social Media,* NYTIMES (May. 22, 2011) available at: https://www.nytimes.com/2011/05/23/world/middleeast/23facebook.html.
[81] *Id.*

Convention against Torture and Other Cruel, Inhuman or Degrading Treatment (CAT), and is obligated to promote and protect the human rights of its' people.[82] These treaties guarantee the right to privacy; freedom of expression and the right to take part in public affairs; the right to be free from torture and cruel, inhumane and degrading treatment; the right to life; and the right to a remedy when any of these rights have been breached. This report documents the violations of the right to privacy of individuals in Syria through an illegal and arbitrary surveillance framework. This report also documents the breaches of other rights that follow from that surveillance and how the regime and its affiliated groups have hacked, tracked and targeted those critical of the regime.

While the rights of all people are endangered and are being breached, the surveillance regime has especially targeted and impacted the rights and lives of human rights defenders working in and out of the country to protect the human rights of the Syrian people. A "human rights defender" is anyone that works—alone or as part of a larger organization—in striving for the realization and protection of human rights.[83] Human rights defenders are identified above all by the actions they take to protect or further the protection of human rights.[84] Although anyone that defends human rights is a human rights defender, the most common examples of human rights defenders include lawyers, government officials, NGO workers, journalists, professors, and persons engaged in social movements for transformative change.[85]

Michel Frost, former UN Special Rapporteur on the situation of human rights defenders, explained that international human rights law "attaches particular importance to the special role of human rights defenders."[86] Human rights defenders are not granted more rights, but rather, since human rights defenders are vulnerable based on the type of work they do, they are afforded a higher duty of human rights protections.[87] Therefore, States must take necessary measures to ensure that human rights defenders are safe in "exercise[ing] the rights to freedom of opinion, expression, peaceful assembly and association, which are essential for the promotion and protection of [all] human rights."[88] States must take steps to ensure protection of human right defenders by refraining from portraying human rights defenders and their activities as dangerous, illegal or a threat to the security of the State.[89] States are also required to act with due diligence in preventing, investigating, and punishing those who violate the rights of human rights defenders.[90] This requires an effective legal system and a functioning and independent judiciary capable of holding violators accountable. While the human rights of all

---

[82] *International Covenant on Civil and Political Rights (ICCPR),* U.N. HUMAN RIGHTS (Dec. 16, 1966); *Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment,* 1465 U.N.T.S. 85 (Dec. 10, 1984).
[83] *Aliyev v. Azerbaijan*, (Judgment), App. Nos. 68762/14 & 71200/14, Eur. Ct. H.R. paras. 88-92 (2018) (discussing foundations of law related to human rights defenders); *see also* G.A. Res. 53/144, Declaration on Human Rights Defenders (Mar. 8, 1999) (adopting the declaration on human rights defenders).
[84] *Human Rights Defenders: Protecting the Right to Defend Human Rights*, UNITED NATIONS, 2, https://www.ohchr.org/Documents/Publications/FactSheet29en.pdf (last visited May 6, 2019).
[85] *E.g.*, Michel Frost (Special Rapporteur on the situation of human rights defenders), *Situation of Women Human Rights Defenders*, U.N. Doc. A/HRC/40/60 (Jan. 10, 2019) at para. 4.
[86] *Id.* at para. 208.
[87] Michel Frost (Special Rapporteur on the situation of human rights defenders), *Situation of Human Rights Defenders*, U.N. Doc. A/73/215 at para. 14 (July 23, 2018).
[88] *Aliyev v. Azerbaijan*, Eur. Ct. H.R. para. 88 (quoting G.A. Res. 31/32, Protecting Human Rights Defenders, Whether Individuals, Groups or Organs of Society, Addressing Economic, Social and Cultural Rights (Mar. 24, 2016)) (The UN's Declaration on Human Rights Defenders states that States are required to "protect, promote and implement all human rights."); General Assembly Resolution A/RES/53/144 adopting the Declaration on human rights defenders at section 2(b); *see also Aliyev v. Azerbaijan*, Eur. Ct. H.R. paras. 114-140 (analyzing allegations of "ill-treatment" of a human rights defender by the state of Azerbaijan); Human Rights Committee, Communication No. 2212/2012, (Judgment), *Sannikov v. Belarus*, views adopted July 12, 2012 (finding a violation of, amongst others, the right to be free from torture as it relates to a human rights defender); Human Rights Committee, Communication No. 1782/2008, (Judgment), *Aboufaied v. Libya*, (Judgment), views adopted Mar. 21, 2012 (finding a violation of the right to life and the right to be free from torture for a human rights defender in Libya); Human Rights Committee, Communication No. 2024/2011, *Israil v. Kazakhstan*, (Judgment), views adopted Oct. 31, 2011 (holding that deporting a human rights defender to his country of origin would violate the defender's rights to life and freedom from torture).
[89] Margaret Sekaggya, *Report of the Special Rapporteur on the Situation of Human Rights Defenders,* UNITED NATIONS GENERAL ASSEMBLY (Dec. 30, 2009) 6, available at: https://www2.ohchr.org/english/issues/defenders/docs/A.HRC.13.22.pdf.
[90] Frost *supra* note 85, at para 20.

people have been breached and continue to be in danger, the rights of human rights defenders are systematically and disproportionately impacted.

This section identifies the human rights implicated by the surveillance capabilities of the Syrian regime. The next section sets out how surveillance leads to tracking, hacking and violence in breach of these rights.

A. The Right to Privacy

A surveillance state with the capabilities to monitor and track its people implicates the privacy rights of everyone. Syria's surveillance system operates pursuant to arbitrary and imprecise legal standards, breaching the privacy rights of its people and facilitating further human rights violations from the right to freedom of expression to the right to life. Article 17 of the ICCPR protects individuals from arbitrary or unlawful interference with their "privacy, family, home or correspondence."[91] Violations of the right to privacy can occur when a state intercepts correspondence, including electronic and non-electronic correspondence such as letters, emails, or social media activity.[92] Other invasions of privacy include collecting metadata regarding communications,[93] audio-visual observation,[94] GPS tracking,[95] and the unauthorized storing and subsequent use of personal information.[96] Privacy is not an absolute right, it may be interfered with to advance legitimate state interests so long as that interference is lawful, necessary and proportionate.[97]

The term "unlawful" means that no interference can take place except in cases authorized by law.[98] To meet the requirement that an invasion of privacy be lawful, the surveillance program must be justified by legislation.[99] The legislation must be consistent with the provisions, aims, and objectives of the Covenant, pursuant to domestic and international law, foreseeable and accessible in a manner that is timely and accurate,[100] precise, specific and clearly defined.[101] A law is accessible when it is not left to "secret" determinations by unaccountable bodies,

---

[91] *ICCPR*, *supra* note 82, Article 17.
[92] UN HRC, *The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights*, 27th session, 2nd and 3rd agenda item, A/HRC/27/37 (explaining that correspondence covers electronic correspondence); Human Rights Committee, Communication 2079/2011, *Khadzhiev v. Turkmenistan*, views adopted 1 April 2015, para. 8.8 (holding that interference with mail from a prisoner to his family violates the right to privacy).
[93] *Malone v. United Kingdom*, (Judgment), App. No. 8691/79, 82 Eur. Ct. H.R. (ser. A), para. 84 (1984); *see also* UN HRC, *The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights*, 27th session, 2nd and 3rd agenda item, A/HRC/27/37 ("The aggregation of information commonly referred to as 'metadata' may give an insight into an individual's behavior, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication.").
[94] *El-Haski v. Belgium*, App. No. 649/08, Eur. Ct. H.R. (2012).
[95] *Uzan v. Germany*, (Judgment), App. No. 35623/05, Eur. Ct. H.R. para. 12-13 (2010).
[96] *See S. v. United Kingdom*, (Judgment), App. Nos. 30562/04 & 30566/04, Eur. Ct. H.R. paras. 20, 33 (2008).
[97] *E.g.*, Human Rights Committee, Communication No. 2326/2013, *N.K. v. Netherlands*, views adopted July 18, 2017, para. 9.3 (No specific legislation has been adopted to regulate surveillance for law enforcement agencies or intelligence services in Syria.).
[98] Human Rights Committee, General Comment 16, U.N. Doc. HRI/GEN/1/Rev.1 at 21 (1994), available at: http://hrlibrary.umn.edu/gencomm/hrcom16.htm.
[99] High Comm'r For Human Rights, *Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/27/37 (30 June 2014) paras. 22-23 (citing Communication No. 903/1999, *Van Hulst v. Netherlands*, Views adopted Nov. 1, 2004; Human Rights Committee, *Concluding Observations on the Fourth Periodic Report of the United States of America*, CCPR/C/USA/CO/4 (2014); *Uzun v. Germany*, (Judgment), App. No. 35623/05, Eur. Ct. H.R., (2010); *Weber v. Germany*, (Decision), App. No. 54934/00, Eur. Ct. H.R., para. 4 (2006); *Escher v. Brazil* (Judgment), IACHR (Nov. 20, 2009); Martin Sheinin (Special Rapporteur on the Promotion and Protection of Fundamental Freedoms While Countering Terrorism), U.N. Doc. A/HRC/13/37 (Dec. 28, 2009); Frank La Rue (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), U.N. Doc. A/HRC/23/40 (Apr. 17, 2013)).
[100] *Id.*
[101] *See* Human Rights Committee, Communication No. 2081/2011, *D.T. v. Canada*, views adopted July 15, 2016, para. 7.10 (holding that a violation of the right to privacy occurred although the violation—deportation of an individual to Nigeria—was provided for in national law, the law failed to account for the best interest of children); *see also Big Brother Watch and Others v. The United Kingdom*, (Judgment), Eu. Ct. H.R., App. Nos. 58170/13, 62322/14, 24960/15 (Sept. 13, 2018) paras. 387-388 ("[The Court] is satisfied that the intelligence services of the United Kingdom take their Convention obligations seriously and are not abusing their powers under [the national law]. Nevertheless, an examination of those powers has identified two principal areas of concern; first, the lack of oversight of

and it is "foreseeable" when the consequences of a given action is known, in order to allow people to regulate their conduct in accordance with the law.[102] Domestic law must be "precise" and "clearly" defined. To be clear and precise, the legal justification for surveillance must "precisely define" the situations in which the interception, collection, and analysis of communications is legally justified.[103]

Human Rights Council General Comment 16 recognizes that "gathering and holding of personal information on computers, databanks and other devices, whether by public authorities or private individuals or bodies must be regulated by law."[104] However, even when the surveillance is authorized by law, that surveillance can still interfere with the privacy rights of individuals. Therefore, the law itself must meet substantive standards and ensure the interference is not arbitrary or disproportionate.[105] Legislation that "allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights."[106] In other words, legislation that permits secret surveillance without clear standards and processes for establishing specific justifications is in itself an interference with the privacy rights of the people.

Any interference authorized by law must also satisfy the principle of proportionality. For a surveillance program to meet the requirement of proportionality, any interference with privacy must be necessary given the circumstances,[107] and must be proportionate to the legitimate aim it seeks to address.[108] To satisfy proportionality, the law must have a legitimate aim, have a rational connection to that aim, minimally impair the right to privacy, and strike a fair balance between pursuit of the aim and limitation of the right.[109] The proportionality test applies even in cases where national security concerns are implicated.

Merely stating that secret mass digital surveillance is necessary for safety or national security does not satisfy proportionality.[110] The state justifying the surveillance must produce "sufficient factual basis for the application of secret intelligence gathering measures" that would justify any surveillance "on the basis of an individual suspicion regarding the target person."[111] The law must also use the least intrusive method to obtain the desired result.[112]

---

the entire selection process, including the selection of bearers for interception, the selectors and search criteria for filtering intercepted communications, and the selection of material for examination by an analyst; and secondly, the absence of any real safeguards applicable to the selection of related communications data for examination. In view of these shortcomings and to the extent just outlined, the Court finds that that the [national law] does not meet the 'quality of law' requirement and is incapable of keeping the 'interference' to what is 'necessary in a democratic society'. There has accordingly been a violation of Article 8 of the Convention."); *see also The Human Right to Privacy in the Digital Age*, ACLU (Feb. 2015) available at: https://www.aclu.org/other/human-right-privacy-digital-age.

[102] *Right to Privacy in the Digital Age*, *supra* note 99 ("Secret rules and secrete interpretations—even secret judicial interpretations—of law do not have the necessary qualities of law.").

[103] Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, *Freedom of Expression and the Internet*, (Dec., 31 2013); *see also Malone v. United Kingdom*, (Judgment), App. No. 8691/79, 82 Eur. Ct. H.R. (ser. A), para. 79 (1984).

[104] General Comment 16, *supra* note 97, at 10 (1994).

[105] General Comment 16, provides that interferences "provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, *reasonable in the particular circumstances* (emphasis added)." General Comment 16, *supra* note 97, at para. 4; See also, U.N. Human Rights Comm., Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Concluding Observations, Jamaica, U.N. Doc. CCPR/C/79/Add.83 at para. 20 (Nov. 19, 1997) [hereinafter U.N. Human Rights Comm., Concluding Observations on Jamaica].; U.N. Human Rights Comm., Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Comments, Russian Federation, U.N. Doc. CCPR/C/79/Add.54 at para. 19 (July 26, 1995) [hereinafter U.N. Human Rights Comm., Concluding Observations on Russia].

[106] *Weber v. Germany*, (Decision), App. No. 54934/00, Eur. Ct. H.R., para. 78 (2006).

[107] *Id.*; *see also* Human Rights Committee, Communication No. 2273/2013, *Vondom v. Republic of Korea*, views adopted July 7, 2018, para. 8.7.

[108] *Id.*; *see also* Human Rights Committee, Communication No. 2326/2013, *N.K. v. Netherlands*, views adopted July 18, 2017, paras. 9.3-9.11 (holding that an interference with privacy, although minor, was disproportionate to the legitimate aim the DNA collection program sought to address).

[109] *The Human Right to Privacy in the Digital Age, supra* note 101.

[110] *Szabo and Vissy v. Hungary*, (Judgment), Eur. Ct. H.R., App. No. 37138/14, paras. 71-73 (2016).

[111] *Id.*; *see also Weber v. Germany*, (Decision), Eur. Ct. H.R., App. No. 54934/00, paras. 104-06 (2006).

[112] *Right to Privacy in the Digital Age*, *supra* note 99, at para. 25.

Further, there must be "a rational connection between the means employed and the aim sought to be achieved," as well as a balanced relationship between the public need and the privacy interference.[113] As outlined in Section IV, the legal infrastructure empowering the Syrian regime's surveillance operations fails to satisfy the legality and the proportionality requirements established by international law. No legislation clearly articulates the scope and limits of surveillance powers.

B. Freedom of Expression and the Right to Participate in Public Affairs

Surveillance, particularly when coupled with censorship, intimidation and violence, breaches the peoples' right to freedom of expression and interferes with the peoples' right to fully participate in public affairs. Article 19 of the ICCPR states that "everyone shall have the right to hold opinions without interference," and "everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice."[114]

Article 19 protects the ability of all persons to freely exchange ideas.[115] Because part of the work that human rights defenders do is to report human rights abuses and provide a voice for victims of human rights violations, their ability to freely share information and ideas is essential to the nature of their work.[116] The right to freely hold and express opinions guarantees the right "to receive and impart information and ideas of all kinds, regardless of frontiers and through any medium."[117] The protection of human rights more broadly is enhanced when human rights defenders are able to share ideas and information with the rest of the population and the world.[118] Therefore, there must be an environment that permits and protects the ability of all persons, including human rights defenders, to freely form, hold, and express opinions and to publicize and share information.[119]

Although the right to freely hold and express opinions may be limited by national law in select situations, any such limitation must be necessary and proportionate to a legitimate aim.[120] There are two legitimate aims identified by the Convention: "(a) for the respect of the rights and reputation of others and (b) for the protection

---

[113] Special Rapporteur, *Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism*, U.N. Doc. A/69/397, para. 51 (Sept. 23, 2014).
[114] *ICCPR, supra* note 82.
[115] *ICCPR, supra* note 82, at Art. 19; *See* Human Rights Committee, Communication No. 2158/2012, *Sviridov v. Kazakhstan*, (Judgment), views adopted July 13, 2017 para. 10.2.
[116] David Kaye (Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression), U.N. Doc. A/HRC/38/35 para. 21 (Apr. 6, 2018) ("The Declaration also protects the right to develop and discuss new human rights ideas, allowing all people to be part of the progressive development of human rights ideas and to be actively engaged in setting new directions for the human rights project. This right recognizes that some of these new ideas may be culturally, religiously or politically controversial; it is precisely this potential for controversy that demands space for free and open discussion and debate.").
[117] *Id.* at para. 5 (internal quotations omitted) (quoting ICCPR art. 19) (citing African Charter on Human and Peoples' Rights art. 9, June 27, 1981, 1520 U.N.T.S. 217; American Convention on Human Rights "Pact of San José, Costa Rica" art. 13, Nov. 22, 1969, 1144 U.N.T.S. 123; Convention for the Protection of Human Rights and Fundamental Freedoms art. 10, Nov. 4, 1950, Europ. T.S. No. 5, 213 U.N.T.S. 221).
[118] *Sviridov v. Kazakhstan*, *supra* note 114, para. 10.3.
[119] Kaye, *supra* note 115 at para. 6; s*ee also Sviridov v. Kazakhstan*, *supra* note 114; Human Rights Committee, Communication No. 1553/2007, *Korneenko v. Belarus*, (Judgment), views adopted Mar. 20, 2009; *Big Brother Watch and Others v. The United Kingdom*, (Judgment), App. Nos. 68762/14 & 71200/14 paras. 469-500 (2018) (holding that the U.K.'s mass surveillance system violates the right to hold and express an opinion and privacy); *Matasaru v. Moldova*, (Judgment), Eu. Ct. H.R., App. Nos. 69714/16 & 71685/16 para. 28 (Jan. 15, 2019) ("[The right to freedom of expression and opinion] is applicable not only to 'information' or 'ideas' that are favorably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any section of the population. Such are the demands of that pluralism, tolerance and broadmindedness without which there is no 'democratic society.'").
[120] Article 17 ICCPR does not explicitly stipulate that any restriction on the right to privacy must be necessary for a specified purpose, but both the UN Special Rapporteur on Counter-Terrorism and the UN Special Rapporteur on Freedom of Expression have held that the "permissible limitations" test under Article 19 among other articles of the ICCPR, was equally applicable to Article 17 ICCPR. Article 19, Electronic Frontier Foundation, *International Principles on the Application of Human Rights Law to Communications Surveillance* (May 2014) available at: https://www.ohchr.org/Documents/Issues/Privacy/ElectronicFrontierFoundation.pdf.

of national security or public order (*odre public*) or public health or morals."[121] Vague and unsubstantiated claims of national security cannot satisfy the requirements established by international law for what amounts to a necessary and proportionate interference.[122] Where surveillance is used specifically to silence criticism and is part of a system of state violence, the interference fails to advance a legitimate aim and to satisfy the principle of proportionality and the right is breached.[123]

All persons have the right to freely participate in public affairs as guaranteed by Article 25 of the ICCPR.[124] To freely participate includes the right to vote, the right to be elected, and the right to access public benefits.[125] The right to participation is critical to the advancement of all human rights because it promotes democracy, the rule of law, social inclusion, and economic development.[126] The right to participation protects and provides for individuals and communities to actively engage in decision-making processes that affect them.[127] As it relates to human rights defenders, the universal human right to participate in public affairs extends beyond the state and into the international human rights system.[128]

Like the right to privacy and the right to freely hold and express opinions, the right to participation is threatened by the very existence of mass digital surveillance technology.[129] Mass digital surveillance prevents people from fully participating in public life due to potential fears of retribution and violence.[130]

C. Right to Life and Freedom from Torture and CIDT

As Section IV below documents, mass surveillance can be a key tool in a state's campaign of suppression and violence. When surveillance facilitates the torture and extrajudicial killing of people, then it leads to the breach of the right to life and the right to be free from torture and cruel, inhuman, and degrading treatment. Both rights are non-derogable, meaning no justification of war or national security can excuse the state from having to protect the peoples' right to be free from torture and extrajudicial killing. Article 6 of the ICCPR guarantees that "[e]very human being has the inherent right to life. This right shall be protected by law. No one shall be arbitrarily deprived of his life."[131] As stated in General Comment 36 of the Human Rights Committee, "the effective protection of [the right to life] is the prerequisite for the enjoyment of all other human rights and the content of

---

[121] Human Rights Committee, Communication No. 1553/2007, *Korneenko v. Belarus*, (Judgment), views adopted Mar. 20, 2009 para. 8.3 ("The Committee recalls, first, that the right to freedom of expression is not absolute and that its enjoyment may be subject to limitations … [L]imitations are permissible as are provided for by law and that are necessary (a) for respect of the rights or reputation of others; (b) for the protection of national security or of public order (*ordre public*), or of public health or morals.").
[122] *Roman Zakharov v. Russia*, Eu. Ct. H. R., Grand Chamber (Judgement), App. No. 47143/06 (Dec. 4, 2015).
[123] Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Unites Nations General Assembly (May. 16, 2011) available at: https://www.ohchr.org/Documents/Issues/Opinion/A.66.290.pdf.
[124] ICCPR, *supra* note 82, at Art. 25 ("Every citizen shall have the right and the opportunity, without any of the distinctions mentioned in article 2 and without unreasonable restrictions: (1) To take part in the conduct of public affairs, directly or through freely chosen representatives; (2) To vote and to be elected at genuine periodic elections which shall be by universal and equal suffrage…"); Comm. on the Right to Participate in Public Affairs, Voting Rights and the Right of Equal Access to Public Service, Off. of High Comm'r for Human Rights on Its Fifty-Seventh Session, U.N. Doc. CCPR/C/21/Rev.1/Add.7 (1996).
[125]ICCPR, *supra* note 82, at Art. 25; *see also* Human Rights Committee, Communication No. 2250/2013, *Katashynski v. Ukraine*, (Judgment), views adopted July 25, 2018 (holding the right to participation was violated when the state interfered with election results and refused to allow an appeal for such); Human Rights Committee, Communication No. 2668/2015, *Sanila-Aikio v. Finland*, (Judgment), views adopted Nov. 1, 2018 paras. 6.5-6.12 (explaining that the right to participation has a collective element when applied to indigenous groups).
[126] Report of High Commissioner for Human Rights, *Draft Guidelines for States on the Effective Implementation of the Right to Participate in Public Affairs*, U.N. Doc. A/HRC/39/28 at para. 1 (2018).
[127] *Guidelines for States on the effective implementation of the right to participate in public affairs*, OHCHR, 14-15, available at: https://www.ohchr.org/Documents/Issues/PublicAffairs/GuidelinesRightParticipatePublicAffairs_web.pdf.
[128] Frost, *supra* note 85, at para. 56.
[129] *See* U.N. General Assembly, *Resolution on the Right to Privacy in the Digital Age*, U.N. Doc. A/RES/73/179 (Dec. 17, 2018) at para. 7; Kaye, *supra* note 116.
[130] *Id.*
[131] ICCPR, *supra* note 82, at Art. 6.

which can be informed by other human rights."[132] States are required to refrain from any conduct that can result in the arbitrary loss of life. Arbitrariness must be interpreted "broadly to include elements of inappropriateness, injustice, lack of predictability and due process of law, as well as elements of reasonableness, necessity and proportionality."[133] Where a legal system fails to safeguard life, to ensure proper investigations of the loss of life and processes for accountability and redress, the right to life is breached.

Article 7 of ICCPR guarantees that "no one shall be subjected to torture or to cruel, inhuman or degrading treatment or punishment."[134] Article 2 of the CAT requires states to "take effective legislative, administrative, judicial or other measures to prevent acts of torture."[135] The right to be free from torture protects individuals from physical or mental torture and cruel, inhuman or degrading treatment.[136] Article 1 of the CAT recognizes that torture can occur by "means of any act by which severe pain or suffering whether physical or mental, is intentionally inflicted on a person."[137] States breach their obligation to protect individuals from torture through their acts or omissions, irrespective of their justification under domestic law.[138]

Where state surveillance leads to the arrest, detention and torture of critics and human rights defenders, the right to be free from torture and the right to life are breached. In an environment where speaking up against the regime or documenting human rights violations committed by the state can lead to immediate reprisal, surveillance and violence are part and parcel of a unified campaign of repression and violence.

D. The Right to a Remedy

To ensure the rights enumerated above, the state is obligated, through a functioning legal system, to provide processes through which people can vindicate their rights and be provided a remedy when rights are violated.[139] Article 2 of the ICCPR requires states to provide any person who has their rights or freedoms violated access to an effective remedy.[140] A remedy may be procedural in nature, such a judicial remedy or an independent investigation, or substantive in nature, such as a reparation.[141]

The right to effective remedy is imperative to establishing a "safe and enabling environment" for human rights defenders.[142] The Human Rights Council laid out five key elements in how States should maintain this "safe and

---

[132] U.N. Human Rights Committee, *General Comment no. 36 (Right to Life),* CCPR/C/GC/35 (Sept. 3, 2019) para. 2, available *at*: https://www.refworld.org/docid/5e5e75e04.html.
[133] *Id.* at para. 12.
[134] ICCPR, *supra* note 82, at Art. 7.
[135] CAT, *supra* note 82, at Art. 2.
[136] Under Article 1 of the Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment treaty, torture means "any act by which severe pain or suffering, whether physical or mental, is intentionally inflicted on a person for such purposes as obtaining from him or a third person information or a confession, punishing him for an act he or a third person has committed or is suspected of having committed, or intimidating or coercing him or a third person, or for any reason based on discrimination of any kind, when such pain or suffering is inflicted by or at the instigation of or with the consent or acquiescence of a public official or other person acting in an official capacity. It does not include pain or suffering arising only from, inherent in or incidental to lawful sanctions." CAT, *supra* note 82, at Art. 1.
[137] *Id.*
[138] *See generally* Committee Against Torture, General Comment No. 3, CAT/C/GC/3 (Dec. 13, 2012).
[139] *ICCPR*, *supra* note 82, at Art. 2
[140] *ICCPR*, *supra* note 82, at Art. 2
[141] International Commission of Jurists, *The Right to a Remedy and Reparation for Gross Human Rights Violations* (2018) para 52, available at: https://www.icj.org/wp-content/uploads/2018/11/Universal-Right-to-a-Remedy-Publications-Reports-Practitioners-Guides-2018-ENG.pdf; Human Rights Committee, General Comment No. 31 on the Nature of the General Legal Obligation Imposed on States Parties to the Covenant, UN Doc CCPR/C/21/Rev.1/Add.13 (2004), para 16.
[142] Frost, *supra* note 85, at para. 27.

enabling environment";[143] they are: (1) a robust legal framework that is compliant with international standards as well as a strong national human rights protection system that safeguards public freedoms and ensures effective access to justice; (2) a political environment conducive to civil society work; (3) access to information; (4) avenues for participation by civil society in decision-making processes; (5) and long-term support and resources for civil society.

As the following section shows, the Syrian state's campaign of mass surveillance and violence has led to the breach of the human rights of the Syrian people, most especially of journalists, activists, and human rights defenders. The legal infrastructure has failed to protect human rights, on paper and in practice. In fact, the legal and institutional infrastructure of the state has facilitated the systematic violation of the peoples' rights to privacy, freedom of expression and of participation, the right to life and freedom from torture and cruel, inhuman and degrading treatment.

IV. How Surveillance Leads to Censorship, Monitoring, Hacking and Violence

The unchecked and pervasive power of surveillance exercised by the Syrian regime and affiliated groups, is a key cog in the machinery of state control and violence. That power is established and unleashed through a flawed legal and institutional infrastructure that provides for broad authority and lacks institutional processes for oversight and accountability.[144] This power has been used by the regime in various ways to silence, torture, and kill human rights defenders and those the State deems a threat. Surveillance has facilitated censorship on the internet and interference with access; hacking, tracking and monitoring of journalists, human rights defenders and critics of the regime; and the detention, torture and execution of journalists, human rights defenders and critics of the regime. As a result, the Syrian peoples' ability to express themselves, to share information and ideas, to organize and participate in political life without fear of immediate and severe reprisal is systematically extinguished. These acts of control and violence are facilitated by tools and technologies supplied by multinational and foreign corporate entities. Lack of corporate accountability further undermines efforts to challenge and stop the Assad regime's ongoing assault on safety and security of the Syrian people.

A. Abuse Enabling Legal and Institutional Infrastructure

The state is required to establish a legal framework and institutions to ensure human rights obligations it has taken on under international law and duties it owes to its people. The protection of the right to privacy, the right to life and freedom from torture, all require a legislative and institutional infrastructure that empowers and limits official actors and provides for processes of oversight and accountability. The legal framework authorizing the state's power to surveil, to detain, and to punish, however, provides broad grants of power and authorizes the targeting, arrest and prosecution of individuals for vague and imprecise interests. No privacy protecting legislation exists to safeguard the rights of people from illegal and disproportionate government surveillance, and the penal and cyber laws set imprecise standards and allow for broad discretion and authority. This legal framework has been used to surveille and punish individuals engaged in or suspected of opposing the regime.

[143] The Report of the United Nations High Commissioner for Human Rights, *Practical Recommendations for the Creation and Maintenance of a Safe and Enabling Environment for Civil Society, based on Good Practices and Lessons Learned,* A/HRC/32/20 (Apr. 11, 2016) 17, available at: https://undocs.org/en/A/HRC/32/20.

[144] *See generally* United States Department of State, Bureau of Democracy, Human Rights, and Labor, *Syria 2019 Human Rights Report*, available at https://www.state.gov/wp-content/uploads/2020/03/SYRIA-2019-HUMAN-RIGHTS-REPORT.pdf (last visited Dec. 2, 2020).

Lack of judicial independence and an institutional infrastructure that facilitates human rights violations means there are no checks and no remedies for those pursued and ensnared by the regime.

The regime has relied on a set of laws granting the government broad discretion to arrest and prosecute individuals it deems a threat. Most prominently, the Penal Code 148/1949, Media Law 108/2011, the Cybercrime Law 17/2012 and the Anti-Cybercrime Law 9/2018 have been used to prosecute internet users, journalists and dissidents for vague offenses that grant the state almost absolute discretion. These offenses include "threatening national unity" or "publishing false news that may weaken national sentiment."[145]

While the constitution sets general due process guarantees, the lack of a rule of law oriented legal infrastructure means the constitutional guarantees are little more than paper promises. As a result, the right to privacy and the related rights to freedom of expression, freedom from torture and cruel, inhumane and degrading treatment, the right to liberty and of life are systematically undermined.

Syria's Emergency Law, enacted in 1963 - the day that the Assad Baath party (under Hafez al-Assad) seized power – provided government agents the right to both monitor and imprison individuals with no explanation or justification.[146] This law suppressed rights guaranteed in the Syrian Constitution, such as freedom of assembly, freedom of speech, and freedom of movement by granting Syrian authorities wide latitude to arrest and detain individuals without due process or access to lawyers.[147] Specifically, the Emergency Law gave the government nearly unlimited authority to restrict individual freedoms and to investigate and detain suspects when national security and public safety were deemed to be at risk.[148] Further, the law granted the government authority to detain anyone who opposed the Syrian regime, including journalists, lawyers, and other human rights defenders with no legal justification beyond that of unspecified interests of national security.[149]

As a response to the protests in 2011, Bashar al-Assad repealed the Emergency Law.[150] However, since its repeal, there has been no real change in practice and similarly problematic legislation remained in place while new problematic legislation was enacted to take its place. Journalists and human rights defenders have been charged and detained pursuant to Article 285 and 286 of the Penal Code for undermining national unity and promoting fake news.[151] Media Law 108/2011, the Cybercrime Law 17/2012 and the subsequent Anti-Cybercrime Law 9/2018 grant the government authority to arrest individuals for their online expressions with little or no judicial oversight. The 2012 Cybercrime Law requires website owners "to save a copy of their content and traffic data to allow verification of the identity of persons who contribute content on the network."[152] In other words, the law requires websites not only to publish the names of the owners and administrators but also to provide to the government the names of those who contribute or post on the platform or website and the content of those posts.

---

[145] Freedom House, *Freedom on the Net 2018 – Syria,* 1 November 2018, available at: https://www.refworld.org/docid/5be16af6116.html (accessed Dec. 3, 2020).
[146] *See* Human Rights Committee, Communication No. 2326/2013, *N.K. v. Netherlands*, views adopted July 18, 2017, at para. 9.5 ("Even with regard to interferences that conform to the Covenant, relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted.").
[147] *Id.*
[148] *Syria's Emergency Law Lifted After 48 Years (Ask and Editor)*, ENCYCLOPEDIA BRITANNICA BLOG (Apr. 19, 2011) available at: http://blogs.britannica.com/2011/04/syrias-emergency-law-lifted-48-years-editor/.
[149] Human Rights Watch, *A Wasted Decade: Human Rights in Syria During Bash al-Asad's First Ten Years in Power* (July 16, 2010) available at: https://www.hrw.org/report/2010/07/16/wasted-decade/human-rights-syria-during-bashar-al-asads-first-ten-years-power.
[150] *See, e.g.*, *Syria Protests: Bashar al-Assad Lifts Emergency Law*, BBC (Apr. 21, 2011), available at: https://www.bbc.com/news/world-middle-east-13161329 ("The repeal of the emergency law was a key demand of protesters. It abolishes state security courts and allows citizens to protest peacefully. But prominent opposition figure Haitham al-Maleh said the move was 'useless,' reported Reuters news agency.").
[151] Penal Code 148/1949, Arts. 285-86; *see also Syrian Government Passes New Anti-Cybercrime Bill,* SMEX (Mar. 14, 2018) available at: https://smex.org/syrian-government-passes-new-anti-cybercrime-bill/#:~:text=On%20March%205%2C%20the%20Syrian,at%20the%20Court%20of%20Appeal (last visited Dec. 3, 2020).
[152] *Freedom on the Net 2018-Syria, supra* note 145.

The regime can arrest and detain anyone who deliberately fails to comply with these requirements.[153] These laws empower the state to compel compliance from telecommunications providers in order to gather information on individuals, and then to punish individuals for what they say and who they associate with.

The human rights violations facilitated by broad grants of substantive authority are further compounded by due process and fair trial failures. For example, as part of the new Anti-Cybercrime Law (2018), Syria appointed 58 new judges to oversee special courts charged with public prosecutions and enforcement of cybercrime laws.[154] These judges were trained by the Syrian regime in "filtering online content, especially on social media, and collecting data stored on computers, information systems or storage devices to vindicate cases."[155] Human rights experts raised concerns about the independence of these newly created courts and the continuing targeting and detention of individuals engaged in speech online.

As widely reported, the Assad regime "detained without access to fair public trial tens of thousands of individuals, including those associated with NGOs, human rights activists, journalists, relief workers, religious figures and medical providers."[156] There is a lack of an independent judiciary and rampant due process violations.[157] The Human Rights Council stated that:

> While the Syrian Constitution provides due process guarantees and outlaws arbitrary detention, the Syrian criminal justice system, which encompasses civilian courts, the Counter terrorism Court, military and field courts, is systemically failing to uphold international human rights standards at every step of the judicial process…The judiciary fails to conduct oversight of the national justice system and provides no effective remedy for victims of violations attributable to the State, with individuals not daring to challenge abuses for fear of retribution.[158]

Dissidents and human rights defenders have been arrested and lost in the state's jails and detention centers, unable to access a lawyer or to have their day in court.[159] According to the Syrian Network for Human Rights from the start of the conflict in 2011 to August 2020, there have been 130,758 arbitrary arrests and 84,371 forced disappearances carried out by the regime.[160] When cases are finally assigned to a court, that assignment occurs in "an apparently arbitrary manner to Counterterrorism Court (CTC), courts-martial, or criminal courts."[161] Once individuals are brought before the courts, both "[m]ilitary and civilian courts consistently failed to order investigations into cases where detainees appeared before a judge were visibly illtreated, sometimes displaying severe injuries, and in cases of deaths in custody."[162] Military intelligence memo's found by the nonprofit organization, Commission for International Justice and Accountability, revealed measures taken by intelligence leadership to shield officers involved in torture and extrajudicial killings from prosecution, outlining steps to ensure "judicial immunity."[163]

---

[153] *Freedom on the Net 2018-Syria*, *supra* note 145.
[154] *Syria: Newly Enacted Anti-Cybercrime Law Threatens Online Freedom of Opinion and Expression*, GCHR (May 16, 2018), available at: https://www.gc4hr.org/news/view/1861 (last visited Nov. 25, 2018).
[155] *Id.*
[156] *Syria 2019 Human Rights Report, supra* note 144, at 15.
[157] *See, e.g.*, Freedom House, *supra* note 4.
[158] *Out of Sight, Out of Mind: Deaths in Detention in the Syrian Arab Republic*, HUMAN RIGHTS COUNCIL (Feb. 3, 2016) at para. 16 (citing Article 51-53, Constitution of the Syrian Arab Republic) available at: https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/a_hrc_31_crp_1.pdf.
[159] *Syria 2019 Human Rights Report, supra* note 144, at 11-12 ("The law limits the length of time authorities may hold a person without charge to 60 days, but according to various NGOs, activists, and former detainees, police held many individuals for longer periods or indefinitely.").
[160] Syrian Network for Human Rights, *Statistics of 2020*, *at* https://sn4hr.org/ (last visited Dec. 12, 2020); *see also Id.* at 12 ("Regime authorities held the vast majority without due process or access to legal representation or to their families.").
[161] *Syria 2019 Human Rights Report, supra* note 144, at 11-12.
[162] *Out of Sight, Out of Mind, supra* note 158, at para. 89.
[163] Anne Barnard, *Inside Syria's Secret Torture Prisons: How Bashar al-Assad Crushed Dissent*, NYTIMES (May 11, 2019), available at: https://www.nytimes.com/2019/05/11/world/middleeast/syria-torture-prisons.html.

The laws and the legal system broadly enabled and empowered the regime to take whatever measures it deemed necessary in the name of self-preservation. Lacking an independent judiciary, the regime has been able to establish systems of mass surveillance and an infrastructure of intimidation and violence with no fear of oversight or exposure.

B. Access Shutdowns, Censorship and Self-Censorship

The extent of government control over internet infrastructure empowers the state to shutdown internet access during critical periods in specific locations and to filter and remove content the authorities deem critical of the regime. Websites and certain platforms have been used by human rights defenders, protestors, and those critical of the Assad regime to share information and opinions, organize and mobilize the opposition, to document human rights abuses and to publicize the reality on the ground. Unsurprisingly, these sites and specific messages were blocked by the regime. Areas controlled by the regime have seen internet shutdowns and slowdowns, targeted censorship and filtering of information online, and censorship of mobile communications. The level of monitoring and censorship has in turn led to significant levels of self-censorship by individuals too afraid to express an opinion and journalists afraid to report the news. Such interference with the peoples' ability to speak and to receive information, to organize and to commiserate, violates the rights to freedom of expression and of participation in public affairs. Given the targeting of critics and those involved in opposing the regime or holding it to account, that interference has especially impacted human rights defenders and journalists working in the country.

The state-owned STE and private ISPs have shut down the internet in response to unrest, planned protests or in support of kinetic operations.[164] In the immediate aftermath of the 2011 uprising, the Syrian regime shut down all access to the internet in eastern Syria.[165] Localized blackouts were reported in the aftermath of the uprising,[166] and continued throughout the conflict.[167] Reports suggest that the Syrian regime decreased internet speeds and entirely shut off 3G services prior to besieging an area during the Civil War.[168] During this time, activists and authorities in Syria told the Associated Press that cell phone networks and landlines were unavailable in parts of the capital.[169] Further, the regime has "cut phone lines and Internet access in areas where regime forces [were] conducting major military operations".[170]

These practices have continued. According to the State Department 2019 Human Rights Report "regime officials obstructed connectivity through their control of key infrastructure, at times shutting down the internet and mobile telephone networks entirely or at particular sites of unrest."[171] Removing access to the internet and the mobile telephone networks cuts off peoples' access to information and silences them, frustrating their ability to speak and to communicate and organize with others.[172] Lacking such access can lead to even more severe consequences when information is needed to seek safety or to help individuals on the ground to access lifesaving

---

[164] Christopher Rhoads, *Syria's Internet Blockage Brings Risk of Backfire*, WALL ST. J. (Jun. 3, 2011), available at: https://www.wsj.com/articles/SB10001424052702304563104576363763722080144.
[165] *Open Season, supra* note 2.
[166] *Id.*
[167] Freedom House, *supra* note 4.
[168] *Open Season, supra* note 2; *but see* Spencer Ackerman, *Snowden: NSA Accidentally Caused Syria's Internet Blackout in 2012*, THE GUARDIAN (Aug. 13, 2014), available at: https://www.theguardian.com/world/2014/aug/13/snowden-nsa-syria-internet-outage-civil-war (relaying Edward Snowden's claim that the 2012 internet blackout in Syria was caused by the U.S.).
[169] *Open Season, supra* note 2.
[170] Catharine Smith, *Syria's Internet Reportedly Shut Down,* HUFFPOST, (Nov. 29, 2012) available at: https://www.huffpost.com/entry/syria-internet-down_n_2211458.
[171] *Syria 2019 Human Rights Report, supra* note 143, at 41.
[172] *See* Kaye, *supra* note 116, at para. 6 ("Human rights law imposes duties on States to ensure enabling environments for freedom of expression to protect its exercise. The duty to ensure freedom of expression obligates States to promote, *inter alia*, media diversity and independence and access to information. Additionally, international and regional bodies have urged States to promote universal Internet access.").

medical care or services. Along with shutdowns, the regime has blocked the websites of critics and human rights organizations including the Syrian Observatory for Human Rights and the Syrian Human Rights Committee.[173]

The government has also engaged in more targeted censorship, filtering text messages in connection with planning of protests and individual posts and articles critical of the government. According to one report, special intelligence unit named Branch 225 ordered telephone providers Syriatel and MTN Syria to block text messages that contained words indicating planning or participation in a protest, words included "revolution" and "demonstration."[174] Similar targeted censorship removed specific social media posts, articles and blogs critical of the regime. For example, in a 2019 report, Freedom House reported on a journalist who was instructed by the security services to remove a Facebook post on living conditions in Syria and an activist who was made to unlike a Facebook post by the security services.[175] According to logs accessed by a hacktivist group mapping the Syrian regime's use of surveillance and censorship, social-networking and video-sharing websites were especially targeted by the government, as were websites and blogs covering the uprising.[176]

The censorship and monitoring of individuals' social media posts and articles has led many to stay quiet for fear of retaliation. The serious risk of torture and death, as documented in the section below, means many will self-censor. [177] One student interviewed by researchers, Ahmad,[178] a Syrian student attending university in 2011 spoke about how he changed his behavior due to fears of government surveillance. Ahmad was not a regime supporter and attended peaceful protests after the revolution.[179] Ahmad and his friends suspected that their social media accounts were being monitored by the university's Student Union, which was a state sponsored organization with staff members appointed by the regime.[180] He suspected that the Student Union office was monitoring him and his friends because they were called into the Student Union Office and was shown pictures of himself [Ahmad] and his friends' social media pages.[181]Although Ahmad was not arrested for his posts, this caused him to take more steps to ensure that his accounts were private and to self-monitor what he was posting online.[182] Ahmad's fear of retaliation and of persecution was shared by many student protesters and others who through in-person activism or social media posts shared anti-regime views.

Fear of retaliation has led to self-censorship by news organizations and NGOs, as well as individuals. The news site Damascus Now had its offices raided and its director arrested in December of 2018 for publishing pieces the regime deemed critical. After the raid the site stopped publishing for several weeks and when it resumed publishing, it declined to publish anything on the arrest or the raid.[183] The new leadership received the message, 'report on anything that casts the regime in a negative light, and you too can be arrested and worse.' Reports from bloggers, journalists and human rights defenders indicate self-censorship has become a significant barrier to freedom of expression, sharing of information and publication of documented human rights violations.

---

[173] *Freedom on the Net 2018-Syria, supra* note 145.
[174] Freedom House, *supra* note 4.
[175] Freedom House, *supra* note 4.
[176] Jennifer Valentino-Devries, Paul Sonne & Nour Malas, *U.S. Firm Acknowledges Syria Uses Its Gear to Block Web,* WALL STREET JOURNAL (Oct. 29, 2011) available at: https://on.wsj.com/t6YI3W; Michael Pizzi, *The Syrian Opposition Is Disappearing From Facebook,* THE ATLANTIC (Feb. 4, 2014), available at: https://www.theatlantic.com/international/archive/2014/02/the-syrian-opposition-is-disappearing-from-facebook/283562/ ("Activists believe groups supportive of Syrian President Bashar al-Assad are gaming the system and reporting on their rivals [to Facebook to take post down]. Facebook does not disclose information about who reported whom, making it impossible to confirm these theories. But the pro-Assad Syrian Electronic Army (SEA)…has publicly gloated about this tactic.").
[177] Nicole Bogart, *Propaganda vs. self-censorship: Syria's virtual civil war*, GLOBAL NEWS (Aug. 29, 2013) available at: https://globalnews.ca/news/809766/propaganda-vs-self-censorship-syrias-virtual-civil-war/.
[178] Name has been changed to protect confidentiality.
[179] Interview by UIC John Marshall Law School International Human Rights Clinic with [Ahmad], February 11, 2020.
[180] Interview by UIC John Marshall Law School International Human Rights Clinic with [Ahmad], February 11, 2020.
[181] *Id.*
[182] *Id.*
[183] Freedom House, *supra* note 4.

C. Hacking, Tracking, and Monitoring

Removal of information and censorship are not the only tools deployed by the regime to surveille and control the population. The regime, with support from affiliated third-party hacking groups, has limited the Syrian peoples' ability to employ tools that facilitate anonymous communication while deploying hacking and tracking techniques to identify and monitor critics and human rights defenders. The combination of these strategies ensures a complete lack of privacy and provides the state with the information it needs to intimidate and silence. Unsurprisingly, these tools have been used as part of a broader campaign of violence, in the arrest, detention, and torture of human rights defenders.

Virtual Private Network (VPN) services are regularly used by internet users globally to safely connect to the internet. VPN services allow users to safeguard their privacy and anonymity online while also circumventing geographic based blocking and censorship. Because an internet user's personal information, browsing history, IP address and more can be tracked, particularly where the telecommunications infrastructure is government owned and managed, VPNs provide individuals means of safeguarding their privacy. The Syrian regime, however, blocks software and tools that allow internet users to communicate anonymously. Because the state controls the internet infrastructure, the government is able to use "deep packet inspection (DPI) filtering on the Syrian network, authorities were able to block secure communications tools such as OpenVPN, Later 2 Tunneling Protocol (L2TP), and Internet Protocol Security (IPsec)."[184] In fact, because government forces know people will need the tools to maintain anonymity on the internet "authorities have developed fake Skype encryption tools and a fake VPN application, both containing harmful Trojans" to infiltrate and surveille those seeking privacy.[185] Without VPNs, internet users are vulnerable to state and non-state surveillance.

This vulnerability is further exploited through aggressive strategies deployed by, among others, state affiliated hacking groups targeting regime critics. SEA, for example, sent links and fake software updates to install malware and gain access to devices and accounts of activists and human rights defenders.[186] Malicious software, or malware, "refers to software code designed to be harmful to the software user, often by breaking down protective security measures and giving access or control to unintended third parties."[187] Malware can "enable wiretapping, turn on cameras, or physically track someone."[188] According to reports, the SEA developed malware called SilverHawk built into Microsoft Word and YouTube fakes as well as fake updates for WhatsApp and Telegram to hack devices.[189] Once downloaded, the malware gives the SEA access to the users' device, opening up the users' content, location, and history.

SEA also began using fake profiles in conjunction with phishing and spear phishing techniques in order to target anti-regime activists on Facebook and Skype.[190] SEA targeted organizers or individuals connected to anti-Assad activities through fake profiles, often posing as women sympathetic to the cause. SEA were able to persuade the target to disclose sensitive information such as: meeting locations, whether anti-Assad groups were armed, and the identities of other people engaged in anti-Assad activism.[191] The SEA also deployed malware through

---

[184] Freedom House, *Freedom on the Net 2018-Syria, supra* note 144.
[185] *See* Freedom House, *supra* note 4.
[186] *See* Freedom House, *supra* note 4.
[187] ACLU, *How Malicious Software Updates Endanger Everyone*, available at: https://www.aclu.org/issues/privacy-technology/consumer-privacy/how-malicious-software-updates-endanger-everyone (last visited Dec. 12, 2020).
[188] *Id.*
[189] Thomas Brewster, *Syrian Electronic Army Hackers Are Targeting Android Phones with Fake WhatsApp Attacks,* Forbes (Dec. 5, 2018), available at: https://www.forbes.com/sites/thomasbrewster/2018/12/05/syrian-electronic-army-hackers-are-targeting-android-phones-with-fake-whatsapp-attacks/?sh=3031bf5d6ce4.
[190] Railton, *supra* note 71, at 11 (Although this report does not directly attribute the SEA to all of the stolen data and instead refers to pro-Assad hacking groups, the surveillance described in the report and the tactics used are similar to those known to be used by the SEA).
[191] *Id.* at 11-15.

Facebook and other forms of messaging services by sharing videos in support of anti-Assad groups.[192] By clicking these links, malware capable of reading file contents of the phone or computer would be installed on the individual's device.[193] Trojans such as Darkcoment and Xtreme, "[act] as remote action tools capable of capturing webcam activity, monitoring keystrokes, and stealing passwords."[194] The monitoring and hacking of devices are suspected to inform kinetic operations that have cost the lives of many and undermined the crucial work being done by doctors and human rights defenders.

Monitoring and hacking leads officials to dissidents, and in turn, dissidents lead officials to others in their networks. For example, a man in his 20s living in Syria said that the police demanded his Facebook password in April of 2011 after arresting him at his workplace and taking his laptop.[195] The unnamed man recalled his encounter with the Syrian police: "I told him, at first, I didn't have a Facebook account, but he told me, after he punched me in the face, that he knew I had one because they were watching my 'bad comments' on it;" which led him to conclude they were monitoring him.[196] Detentions and arrests of identified dissidents have been used to compel disclosure of online passwords for social media and other accounts leading to further monitoring and pursuit of networks of activists and human rights defenders.[197]

Such hacking and tracking techniques have been used against doctors and human rights defenders working to minimize the harm and destruction visited on the Syrian people. In 2016, an Aleppo hospital was bombed by suspected Russian warplanes, killing two patients.[198] The hospital was bombed after David Nott, a British surgeon and human rights defender, provided remote instructions via Skype and WhatsApp to assist doctors in performing surgery in the underground hospital.[199] Nott's instructions were broadcast on BBC days after providing the surgeons with remote instructions.[200] Nott believes that the timing of the attack—weeks after providing surgeons with remote instructions—and the precise nature of the bombing show that "the target could only have been gleaned from the coordinates on his computer."[201] Nott believes that the deadly bombing occurred because someone who saw the televised events targeted his computer and gained access to the data identifying those he had been in contact with in Syria.[202] While some experts believe Nott's theory is credible,[203]

---

[192] *Id.*
[193] *Id.*
[194] Olesya Tkacheva, *supra* note 12, at 90.
[195] Jennifer Preston, *Seeking to Disrupt Protesters, Syria Cracks Down on Social Media,* NYTimes (May. 22, 2011) available at: https://www.nytimes.com/2011/05/23/world/middleeast/23facebook.html.
[196] *Id.*
[197] Freedom House, *supra* note 4 ("Activists and bloggers released from custody have reportedly been pressured by security agents to provide the passwords of their Facebook, Gmail, Skype, and other online accounts. . . . The Law for the Regulation of Network Communication against Cyber Crime, passed in February 2012, requires websites to clearly publish the names and details of the owners and administrators."); *see also* Syria Telecommunications Law art. 51(e) ("No Telecommunications Network Operator, Service Provider, the affiliates thereof, and the Users of such services shall utilize any encryption of Telecommunications Services devices, without obtaining the Authority's prior approval, in coordination with the Ministry of Defense and the Relevant Security Agencies.").
[198] Hayley Dixon, Aisha Majid, & Steven Swinford, *Hackers 'Led Warplanes to Syrian Hospital' After Targeting British Surgeon's Computer*, Telegraph (Mar. 20, 2018), available at: https://www.telegraph.co.uk/news/2018/03/20/british-surgeon-helped-syrian-operations-hacked-reveal-secret/.
[199] *Id.*
[200] *Id.*
[201] *Id.*
[202] *Id.*
[203] *Id.* ("Prof Alan Woodward, from the Surrey Centre for Cyber Security, said Mr. Nott's computer or phone could have been hacked during the operation, but it would have been far easier to gain access at a later date to find out who he had been talking to. It is a method that has been used by governments and law enforcement agencies for a number of years, he said, adding: 'It is a fairly classic way of getting information. You don't need to do it at the time, you can break in at your leisure.'").

others are hesitant to establish a correlation.[204] After the hospital bombing, Nott has stated he will no longer provide lifesaving instructions to surgeons over the internet, in Syria or elsewhere.[205]

D. Detention, Torture, and Executions

Monitoring, tracing networks of activists and human rights defenders, and hacking devices, not only violates the privacy and expression rights of the Syrian people, it also forms a crucial part of an apparatus of systematic and widespread violence. The Syrian regime has continually punished human rights defenders for their work in documenting human rights abuses, protecting the human rights of the people, and speaking out against the regime's repressive practices. As has been widely reported and documented, the Syrian regime inflicts torture and forcibly disappears persons that it deems "revolutionary" or anti-regime.[206] According to a Human Rights Council Report and the Independent International Commission of Inquiry on the Syrian Arab Republic , "[t]ens of thousands of individuals in official and makeshift detention centers" are held, tortured, and "subsist in severely inhumane conditions."[207] The "whereabouts of tens of thousands of detainees remain unknown and unacknowledged by the state."[208] Some of the torture methods have included severe beating, kicking to the head and vital organs, mutilation of genitals, malnutrition to the point of emaciation, gastro-intestinal illnesses, and long term exposure to cold weather.[209] Long months of torture are compounded by terrible inhumane detention conditions and lack of medical assistance.[210] Many detainees who were later identified by family members were almost unidentifiable due to their emaciated and unrecognizable bodies.[211] Many torture victims suffered for long periods of time, sometimes months, before dying in detention.[212]

Surveillance capabilities facilitate the identification, location, and arrest of dissidents. Once in the regime's clutches, individuals are detained and subjected to inhumane treatment and conditions. Akram Raslan, a cartoonist who worked for the Hama-based newspaper Al-Fedaa and contributed to several other news websites was targeted and arrested for his work.[213] In 2012, intelligence officials arrested him at his workplace in Hama for publishing cartoons that "offended the state's prestige."[214] For two years, nobody knew where he was, he disappeared into the state's network of jails and detention sites with no contact with his family or an attorney. Then in 2015 it was reported that Raslan had been tortured to death in 2013.[215]

---

[204] *See, e.g.*, Chris Baraniuk, *Surgeon David Nott: Hack Led to Syria Air Strike*, BBC (Mar. 21, 2018), available at: https://www.bbc.com/news/technology-43486131 ("Matthew Hickey of cyber-security company Hacker House pointed out that there were many other ways in which an aggressor could have spied on the hospital. Without accessing the computer devices used and analyzing them forensically, there was no way of knowing what actually happened, he told the BBC.").
[205] *Id.* ("Dr. Nott has said that, following advice from people working in war zones, he will not offer help to surgeons via the internet again. 'It is a crime against humanity that you can't even help a doctor in another country carry out an operation. It is a travesty,' he told the Telegraph.").
[206] *E.g.*, Amnesty International, *End the Horror in Syria's Torture Prisons* (2016) available at: https://www.amnesty.org/en/latest/campaigns/2016/08/syria-torture-prisons/ (last visited May 7, 2019).
[207] Independent International Commission of Inquiry on the Syrian Arab Republic, *Detention in the Syrian Arab Republic: A Way Forward* (Mar. 8, 2018), https://www.ohchr.org/Documents/HRBodies/HRCouncil/CoISyria/AWayForward_DetentionInSyria.pdf, at para. 1, citing, A/HRC/31/CRP.1, https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/a_hrc_31_crp_1.pdf, at paras. 1, 4.
[208] *Id.* at para. 2.
[209] *Id.* at paras. 20-29.
[210] *Id.* at paras. 29-31.
[211] *Id.* at para. 25.
[212] *Id.* at para. 28.
[213] Committee to Project Journalists, *Akram Raslan*, available at: https://cpj.org/data/people/akram-raslan/.
[214] *Id.*
[215] *Id.*

In 2012, an anti-Assad activist and human rights defender, Bassel Khartabil, was targeted and arrested.[216] Khartabil recorded videos of events happening in Syria and sent the recordings to outside news agencies.[217] The Syrian security forces raided Khartabil's office. In the summer of 2017, Khartabil's fiancé announced that he had been executed in 2015—without a trial— after three years of interrogation, torture, and imprisonment.[218] Prior to his arrest, execution, and torture, Khartabil was working on establishing a surveillance free internet in Syria and extending online access to the Syrian people.[219]

The scale of the state apparatus of torture is immense and substantiated by countless accounts from detainees and their families as well as documentary evidence.[220] Accounts of brutal torture and cruel, inhuman and degrading treatment paint a vivid picture of what awaits those the regime deems a threat. Muhannad Ghabbash, an anti-regime protester and law student from Aleppo who organized peaceful protests, was targeted and detained by the regime for daring to speak up. [221] He was tortured for twelve days straight, hung by his wrists for hours, beaten until he was bloody, and shocked with electricity. The torture continued until he wrote a forced confession.[222] After he wrote the confession, he was transferred to a prison in the Mezze air base in Damascus, where the torture continued.[223] He was shackled to a fence naked and sprayed with water, brutalized and degraded by his guards and witnessed the beatings and deaths of many around him.

The Syrian regime has carried out a systematic practice of torture and ill treatment in detention through arbitrary arrests, forced disappearances, and summary executions. The regime's tracking of human rights defenders has supported a campaign of terror where human rights defenders have been punished and paid the ultimate price.[224]

E. Corporate Involvement

The Assad regime's and affiliated groups' campaign of surveillance has been facilitated by an infrastructure and capabilities built on technologies and platforms created by foreign and multinational companies. From the U.S. cybersecurity company Blue Coat (now Symantec), to the Italian company Area SpA, South African MTN, and Facebook, these companies' technologies and processes have facilitated censorship, surveillance, and ultimately detention of activists, journalists and human rights defenders.[225]

---

[216] Rachel Rose O'Leary, *Murder, Censorship and Syria: Crypto and the Future of Uprisings*, CoinDesk (Apr. 29, 2019), available at: https://www.coindesk.com/murder-censorship-and-syria-crypto-and-the-future-of-uprisings.
[217] Alice Su, *How One Syrian Fought to the Death for a Free Internet*, WIRED (Sept. 27, 2017), available at: https://www.wired.com/story/how-one-syrian-fought-to-the-death-for-a-free-internet/.
[218] *Id.*; *see also* Al Jazeera, *Bassel Kartabil: Missing Syrian-Palestinian 'Executed'*, (Aug. 2, 2017) available at: https://www.aljazeera.com/news/2017/08/bassel-khartabil-missing-syrian-palestinian-executed-170802100920059.html.
[219] Front Line Defenders, *Bassel Khartabil,* available at: https://www.frontlinedefenders.org/en/profile/bassel-khartabil (last visited May 7, 2019); *see also* O'Leary, *supra* note 216 ("According to Halpin, who has been providing tech support to human rights activists in the region since Tahrir Square clashes, the last question [Bassel] Khartabil asked to hackers on IRC before his arrest was: 'Do you want to help the Syrian people to connect?'").
[220] *See e.g.* Julian Borger, *Syria's Truth Smugglers,* The Guardian (May 12, 2015), available at: https://www.theguardian.com/world/2015/may/12/syria-truth-smugglers-bashar-al-assad-war-crimes.
[221] Ann Barnard, *Inside Syria's Secret Torture Prisons: How Bashar al-Assad Crushed Dissent,* NYTimes (May 11, 2019) available at: https://www.nytimes.com/2019/05/11/world/middleeast/syria-torture-prisons.html.
[222] *Id.*
[223] *Id.*
[224] Danny Palmer, *These Hackers are Using Android Surveillance Malware to Target Opponents of the Syrian Government*, ZDNet (Dec. 10, 2018), available at: https://www.zdnet.com/article/these-hackers-are-using-android-surveillance-malware-to-target-opponents-of-the-syrian-government/; Frost, *supra* note 84, at para. 6 ("Countless . . . human rights defenders have suffered all forms of indignities and abuses."); *see also* Front Line Defenders, *Syria*, available at: https://www.frontlinedefenders.org/en/location/Syria (last visited May 7, 2019) (outlining the human rights violations against human rights defenders in Syria—often includes torture).
[225] Freedom House, *supra* note 4.

All businesses have the responsibility to engage in practices that protect human rights and ensure that States are not using their technologies, resources, and infrastructure to perpetuate human rights abuses.[226] It is especially important for internet companies to facilitate truthful and accessible information to create "a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity."[227] Prioritizing the protection of human rights is especially important because states are increasingly targeting online content.[228] Businesses have become entangled with State violations in different ways. Companies have provided technology, devices or software directly to the regime knowing what the regime is doing. Some companies are regulated or asked by the state to filter content or deliver malware. Corporate procedures have also been manipulated to advance regime goals. In each circumstance, corporate entities have the obligation to exercise due diligence and examine their business practices, supply chains, and processes to minimize human rights violations tied to their products and services. In 2011, the U.N Human Rights Council endorsed the Guiding Principles on Business and Human Rights, which established key global standards for businesses for the protection of human rights.[229] Principle 13 charges business enterprises with the responsibility of "[seeking] to prevent or mitigate adverse human rights impact that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts."[230] Appropriate action on the part of business enterprises to prevent and remedy human rights violations can vary depending on the circumstances but corporations have the responsibility to exercise due diligence and to alter their practices to mitigate harm.[231]

Syria's mass digital surveillance technology was built from 2007 to 2011, and expanded and reinforced thereafter.[232] Some of the filtering devices discussed above, that enable the regime to inspect encrypted and secured data, were manufactured by a U.S. company called Blue Coat, based out of California.[233] According to multiple reports, Blue Coat technology was used by the Syrian regime to log the activity and content of thousands of users, from "the sites they attempted to visit and every word of their communications with the IP addresses that pointed directly to their homes."[234] Blue coat sold 14 devices to an intermediary in Dubai that then sold 13 of the devices to Area SpA, an Italian company. These devices were then provided to the Syrian regime for surveillance and filtering purposes.[235]

Syria has two dominant mobile phone provides, one owned by the cousin of President al-Assad and the other, a subsidiary of MTN, a South African company.[236] As discussed above, MTN Syria was ordered by Branch 225, a special government intelligence unit, to block certain text messages during planned protests to interfere with organizers' and individuals' ability to coordinate and organize a protest. MTN implemented the order and blocked messages of its users.[237]

---

[226] Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework, https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf, Principle 1.
[227] Kaye, *supra* note 115, at para. 1 (citing John Perry Barlow, A Declaration of the Independence of Cyberspace), Feb. 8, 1996.
[228] Kaye, *supra* note 115, at para. 9 (citing Communication Nos. OL PAK 08/2016 & OL LAO 1/2014).
[229] Guiding Principles on Business and Human Rights, *supra* note 226.
[230] *Id.* at Principle 13.
[231] *Id.* at Principle 19.
[232] *Open Season, supra* note 2.
[233] *Id.*
[234] Andy Greenberg, *Meet Telecomix, The Hackers Bent on Exposing Those Who Censor and Surveil the Internet,* FORBES (Dec. 26, 2011), available at: https://www.forbes.com/sites/andygreenberg/2011/12/26/meet-telecomix-the-hackers-bent-on-exposing-those-who-censor-and-surveil-the-internet/?sh=6d0a0424b089.
[235] *Freedom on the Net 2018-Syria, supra* note 145.
[236] Freedom House, *supra* note 4.
[237] *Id.*

There are also reports that Assad regime associated groups and supporters have used Facebook's Community Standards to target and remove pages that document human rights abuses in the country.[238] According to a report by the Atlantic, the Syrian Electronic Army (SEA) has "publicly gloated" about the tactic of reporting their rivals to Facebook.[239] Since 2012, Facebook has regularly deleted the accounts of those documenting human rights abuses in Syria and critics and dissidents working to organize and oppose the regime.[240] In June of 2020, Facebook deleted 10,000 Facebook accounts belonging to regime opposition activist and political opponents.[241] The words: "Free Army" and "Abdel Bassel al-Sarout" in any post now violate Facebook rules, which results in the deletion of many anti-regime activist accounts. Facebook employs content moderators to address complaints but lacks sufficient number of moderators fluent in Arabic and its dialects. As a result, automated filters and moderators ill equipped to review the content become easy targets for SEA strategies. The ultimate effect of Facebook's enforcement of their Community Standards is the silencing of regime opponents.

As the Syrian regime continues to exercise its violent power over the Syrian people, the international community must commit to protecting the Syrian people and human rights defenders by holding global companies accountable for their role in helping facilitate violations of human rights. Exercising human rights due diligence is key for ensuring better corporate practices. Principle 17 of the UN Guiding Principles calls on business enterprises to develop processes that include "assessing actual and potential human rights impacts, integrating and acting upon the findings, tracking responses, and communicating how impacts are addressed."[242] The international community must prioritize the protection of human rights defenders and hold corporations and States responsible for human rights abuses in Syria.

IV. Conclusion

Online and mobile communications have become ubiquitous for self-expression, sharing of information and ideas, and for publicizing human rights violations to the global community. The threat to that access and consequences for speaking up against the state are especially severe where the government exercises broad and unchecked power over telecommunications systems and the security of the people. The Assad regime developed an infrastructure of surveillance that has allowed the regime to exercise control over internet access and use, monitoring and filtering expressions that challenge or criticize the state. The regime has hacked and tracked critics and human rights defenders, deploying sophisticated and coordinated strategies for identifying dissidents and speech it finds a threat. This system of surveillance is part of a larger campaign of silencing and persecution. The human rights of the Syrian people have been and continue to be violated. The right to privacy, the freedom of expression and of participation, the right to life and freedom from torture and cruel, inhuman and

[238] *See* Michael Pizzi, *The Syrian Opposition Is Disappearing From Facebook,* THE ATLANTIC (Feb. 4, 2014), available at: https://www.theatlantic.com/international/archive/2014/02/the-syrian-opposition-is-disappearing-from-facebook/283562/; Josh Halliday, *Facebook Apologises for Deleting Free Speech Group's Post on Syrian Torture,* THE GUARDIAN (Jul. 6, 2012) available at: https://www.theguardian.com/technology/2012/jul/06/facebook-apologises-free-speech-syria.

[239] Pizzi, *supra* note 239 (""We continue our reporting attacks," read a typical post from December 9 on the SEA's Facebook Page. "Our next target is the Local Coordination Committee of Barzeh [a neighborhood in Damascus], the page that is a partner in shedding Syrian blood and provoking sectarian division." It then provided two links to photos on the Barzeh page that could get the page taken down. Soon afterwards, the SEA removed its post as if it had never existed.")

[240] *See* Pizzi, *supra* note 239; Halliday, *supra* note 238.

[241] Al-Modon, *Facebook Deletes Accounts of Assad Opponents,* The Syrian Observer (Jun. 8, 2020) available at: https://syrianobserver.com/EN/news/58430/facebook-deletes-accounts-of-assad-opponents.html*; see also Facebook Has Been Bending to the Will of Arab Despots,* The Economists (Jul. 2, 2020), available at: https://www.economist.com/middle-east-and-africa/2020/07/02/facebook-has-been-bending-to-the-will-of-arab-despots.

[242] Guiding Principles on Business and Human Rights, HRC Res. 17/4, Principle 17 (Jun. 16, 2011), available at: https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf.

degrading treatment and the right to seek a remedy are being systematically violated by a regime bent on control and domination.