GENEVA ACADEMY
Académie de droit international humanitaire et de droits humains
Academy of International Humanitarian Law and Human Rights

RESEARCH BRIEF

HARNESSING DIGITAL TECHNOLOGY TO DISRUPT, REPRESS AND INTIMIDATE: A DEEP DIVE INTO SURVEILLANCE AND MONITORING TRENDS IN AUTHORITARIAN STATES

EXECUTIVE SUMMARY

In an increasingly interconnected world, digital technologies have emerged as a bedrock of modern business practice, governance and social interaction. They also play an increasingly indispensable role in facilitating the exercise of fundamental human rights. From organizing protests to mobilizing grassroots campaigns, digital spaces have proven to be empowering platforms that amplify voices, particularly for marginalized communities that often find their freedoms restricted in physical spaces.

Such innovation, however, has created a Janus-faced dilemma in that this new capacity to engage and connect simultaneously offers an opportunity and platform from which civil society and individuals can be monitored and surveilled. Such acts, perpetrated both by state and non-state actors, are not only deeply invasive but also threaten the enjoyment of basic rights. Technologies such as facial recognition and commercial spyware like FinFisher and Pegasus, for example, pose unprecedented challenges to privacy, freedom of assembly and protection from discrimination. Particularly in contexts of mal-governance and weak rule of law, this can create a chilling effect on public discourse and contribute to the erosion of civic spaces both online and offline. Moreover, pervasive monitoring often complements other forms of digital technology misuse, to sow distrust, undermine governance structures and further policies of protectionism. Surveillance, for example, both enables and is enabled by cybercrimes, such as espionage (including state-on-state), internet interruptions (e.g. to disrupt elections or cover up human rights abuses) and exploitation (e.g. doxing).

This paradox underscores the imperative of striking a balance between leveraging digital technologies for civic engagement, public safety and government accountability, while at the same time adopting safeguards to mitigate the threats they pose. Private companies also have a role to play, especially when their surveillance technologies are deployed against activists, journalists and human rights defenders.

Against these challenges, this report starts by offering a comprehensive explanation of how modern monitoring and surveillance technologies work, including commercial spyware, real-time surveillance apparatus, and location-tracking devices. It then presents case studies on Iran, Uganda and Russia with a view to unpacking how misuse is encroaching on a range of human rights.

DECEMBER 2024 | ERICA HARPER, JONATHAN ANDREW, FLORENCE FOSTER, JOSHUA NIYO, AND CATHERINE STURGESS

This publication has been externally peer-reviewed

THE GENEVA ACADEMY A JOINT CENTER OF
GENEVA GRADUATE INSTITUTE
INSTITUT DE HAUTES ÉTUDES INTERNATIONALES ET DU DÉVELOPPEMENT
GRADUATE INSTITUTE OF INTERNATIONAL AND DEVELOPMENT STUDIES
UNIVERSITÉ DE GENÈVE
FACULTY OF LAW

In Iran, for example, a sophisticated system of surveillance monitors citizens' online communications, physical movement, interpersonal associations and – most recently – women's attire. Such oversight is enabled by regulation that permits the installation of surveillance cameras in public places, including to identify non-veiled women. In Uganda, reforms introduced in 2021 mandated the installation of surveillance cameras and cellular-network-connected tracking devices in every vehicle. While justified (and legally enabled) as a means of safeguarding public security and investigating crime, the scope for misuse – including to identify and target protestors – is wide. In Russia, the internet (and social media in particular) is viewed as a form of soft power that can both influence the public and serve as a platform for intelligence gathering. This is showcased in how Russia's cyber infrastructure has been built, the programs the government runs and the technologies it is seeking to develop. Most recently, the broad roll-out of facial recognition surveillance cameras, including in the capital city's metro system, showcases how the government is pooling a range of technologies to map threats, control dissent and regulate behaviour. Together, the case studies reflect a widespread surge in the availability and complexity of technological instruments utilized by authoritarian countries to strengthen their hold on power and counteract dissent. Practice also shows that governments are learning from one another, including through technology-sharing agreements. The report then goes on to discuss the main trends and spillover risks posed to individuals and civil society and the applicable international law. Five key areas of risk highlighted for action by governments, civil society and multilateral organizations are as follows:

1. **Data retention and future use**: The rapid growth of data storage capacity has incentivized the retention of data. Given the difficulty of predicting future innovations in data analysis, this raises concern around consent, and whether data collection has taken place within the scope permitted by law.
2. **Consent**: Even when people are aware that they are being monitored, technology is changing so rapidly that it is difficult for them to discern how their behaviour is being observed and by what means their activities are subject to observation.[1] It is also critical to recognize that various groups and individuals have different levels of understanding of how new technologies function and are deployed.[2]
3. **Broad or vague legislation**: Especially given the fast pace of technological development, overly broad legislation and/or insufficient oversight creates risks around invasive surveillance and the arbitrary application of existing law.
4. **Increasing deployment of spyware**: Against the rising threat of cybercrime, and the numerous ways that a nation's security can be jeopardized through cyber operations, governments are increasingly compelled to enhance their cyber military capabilities. The dual-use[3] nature of these technologies means that in doing so, governments acquire an enhanced capability to surveil their own citizens.
5. **Insufficient foresight**: Too few resources are expended on forecasting and developing effective scenario planning and risk mitigation activities around new and emerging digital surveillance technologies. In particular, while data can be collected, processed and retained in the first instance for genuinely benign purposes, it may be repurposed at a later juncture for malign objectives.[4]

MODERN MONITORING AND SURVEILLANCE TECHNOLOGIES AND HOW THEY WORK

Advances in cyber-surveillance and monitoring technologies have brought about a paradigm shift in how activities and individuals can be observed. This has broadened the capacity of state entities to oversee the content of political, human rights and civil society movements, as well as the individuals who organize and participate in them.[5] A parallel development is 'hidden in plain sight' surveillance – the leveraging of information shared on social networks and mobile applications (apps), many of which transmit sensitive data in plain (i.e. non-encrypted) text.[6] Such platforms constitute a rich bank of open-source information that can be combined with covert surveillance to provide unprecedented insight into persons and areas of interest.[7]

COMMERCIAL SPYWARE

Commercial spyware is sophisticated software tools designed to infiltrate smartphones, computers and certain 'wearable' devices. Once installed, spyware enables the tracking of activities, interception of communications, and sometimes the remote operation of a device's functions such as its camera or microphone.[8] In civilian contexts, spyware was originally foreseen as a law enforcement/crime prevention tool and was used principally in criminal investigations in a highly regulated manner. Over time, however, its use and scope of focus have expanded to include the surveilling of journalists, activists, political opponents, international non-government organizations and even general population groups.[9] Between 2011 and 2023, at least seventy-four governments contracted with commercial firms to obtain spyware or digital forensics technology.[10]

- **Pegasus spyware** represents the archetype of intrusive surveillance technology and is sold to governments worldwide. Unlike most hacking utilities that require a level of engagement from the intended victim – such as activating a hyperlink or opening an email attachment – Pegasus uses 'zero-click' infiltration, preventing the victim from obstructing the software's installation. Once installed, the software gains unmitigated access to all of the target device's sensory and data components including photographs, geolocation markers, electronic correspondence, text messages, visual and audio files and installed applications.[11] This provides a hacker with in-depth insight into a user's personal and/or professional life, including behavioural proclivities, occupation, political ideologies, health status, financial circumstances and interpersonal interactions.

- Comparable software, for example **Predator**, is developing rapidly.[12] In October 2023, the Vietnamese Government used the social media platform X to attempt to install Predator on the telephones of key figures including members of the US Foreign Affairs and Foreign Relations Committees, Asia experts at Washington think tanks and Asia-based journalists from CNN.[13] Critically, Predator can activate the microphones and cameras of Apple iPhones and devices running on Google's Android software, retrieve all files and read private messages, even when they are end-to-end encrypted.

REAL-TIME SURVEILLANCE

Satellites, drones, closed-circuit (and networked) cameras and digital interception tools enable the real-time surveillance of both online and offline spaces.[14] Such surveillance can serve a range of ends, from enabling rapid response to intelligence gathering.

- **Signals intelligence** (**SIGINT**) is an older form of electronic surveillance that involves the interception, decoding and analysis of (often encrypted) communications, radar and other electronic systems.[15] Importantly, SIGINT harvests both content data and metadata, the combination of which is pivotal for deep intelligence analyses and situational awareness.[16] One of the fastest-growing subsets of SIGINT is **foreign instrumentation signals intelligence** (**FISINT**). This intelligence is gleaned from the interception of electromagnetic data emissions that follow the testing or deployment of aerospace, surface and subsurface systems. Such data can be transmitted by both military assets (e.g. unmanned aerial vehicles or missile systems) and civilian assets (e.g. satellites or traffic control systems) and can give insight into a range of activities, from weapons development to political unrest or human rights abuses.

- **Facial recognition systems** rely on advanced machine learning algorithms that scan, recognize and match facial features against existing data.[17] The software is increasingly used in law enforcement and urban settings, ostensibly as a public safety tool.[18] A development that warrants particular scrutiny is live facial recognition technology, which is the systematic visual documentation of individuals participating in assemblies, protests or other forms of civic activism. These technologies operate in real time by comparing a digitally captured facial image, or 'template', against stored data based on criteria set by the system's operators.[19]

LOCATION TRACKING

Electronic systems that identify an individual's location – usually through their mobile phone but increasingly through other 'wearables' – have proliferated into law enforcement and intelligence agencies across the globe.[20] Such technologies have become highly pervasive, being able to track an individual's movements, their associates and their associates' movements.[21] Moreover, design improvements (e.g. that allow them to be easily transported or affixed to unmanned aerial vehicles) mean that the scope of implementation has widened,[22] increasing the potential for mass public surveillance.[23]

- Generically known as **'Stingrays', International Mobile Subscriber Identity (IMSI) catchers** are electronic surveillance tools that simulate a cell phone tower/mobile phone traffic base station, thereby forcing smartphones, watches, tablets etc. to connect to them.[24] Once connected, information specific to a phone and SIM card can be identified and linked to an individual user. The primary function is to pinpoint an individual's location and/or movements. Modern IMSI catchers, however, can also block communications, intercept data transmitted and received (including the content of calls, text messages and websites visited) and communicate with devices, for example by sending messages directing a user to a website enabled with malware.[25]

- The increasing use of WiFi in smartphones has offered new ways to monitor individual/group mobility with relatively inexpensive hardware installations, such as **WiFi sniffers**.[26] Importantly, such approaches enable monitoring even when a user sets their phone to airplane mode or turns it off completely.

- Over the past two decades, information and communication technologies such as Global Navigation Satellite Systems (GNSS), Bluetooth, and WiFi have increasingly been embedded into wearable personal devices such as **smartwatches, fitness trackers, neuro-monitoring headsets and medical devices**. While popular for delivering essential services (e.g. real-time health emergency alerts) and connecting people within communities (e.g. Strava),[27] the technology simultaneously facilitates the detection of an individual's location and proximity to others in real time with a high degree of accuracy.[28]

- Meta's platforms such as **Facebook and Instagram**,[29] along with **TikTok, Snapchat and X**, all collect location data and profile user patterns of mobility.[30] Importantly, users have largely acquiesced to this; they value the utility of being able to reach out and engage with peers in their immediate vicinity. Indeed, several of the earliest platforms using location tracking, such as Foursquare[31] and the (now defunct) messaging app Yik Yak,[32] openly publicized this feature.

- Applications specifically designed to locate an individual are both built into devices' operating systems and/or are available for installation (e.g. **Location Tracker**). During the COVID-19 pandemic, for example, contact-tracing applications were developed (and in certain jurisdictions made compulsory to use) with the primary objective of determining individuals' movements and patterns of association.

THE LEVERAGING OF MONITORING AND SURVEILLANCE TECHNOLOGIES IN IRAN, UGANDA AND RUSSIA

THE ISLAMIC REPUBLIC OF IRAN: STATE PATERNALISM IN THE DIGITAL AGE

Summary: Described as a ‘pioneer of digital authoritarianism’,[33] the Islamic Republic of Iran illustrates the increasing willingness of states to employ advanced technology for monitoring and surveilling citizen activity. Aware of the threats and opportunities that digital communications and the internet carry, the government has taken a dual approach centered around innovation on the one hand, and blocking what it deems inappropriate content on the other.[34] While the government has justified the use of such surveillance and monitoring as a means to gather ‘key indicators related to general culture, lifestyles, media influence, and communications’,[35] it also leverages it to track protesters and suppress dissenting voices.[36] Most recently, the surveillance system has been instrumental in enforcing coercive regulations, notably the hijab law, which compels women to adhere to veiling practices. This will and capability to use digital advances to enforce gender-specific laws signals a dangerous trend towards weaponizing technology to restrict fundamental rights.

During the 1979 Islamic Revolution, Iran’s approach to media and communications technology was to embrace its potential insofar as this did not contradict Islamic values and principles.[37] Ever since its rapid expansion in the mid-1990s, however, authorities have come to view the internet more as a threat to state control and security, particularly in terms of its potential to mobilize people and communicate dissent. In 2017, the government blocked internet access and imposed a temporary ban on Instagram and Telegram, justifying the restrictions as necessary steps to quell riots, which they considered to be largely organized through the internet and social networks.[38]

Over time, the clerical establishment came to directly oppose the integration of the internet into Ali Khamenei’s vision for the nation, repeatedly describing social media as a ‘weapon’.[39] In 2012, by order of the Ayatollah, the Supreme Council of Cyberspace (SCC) was established and tasked with managing the state surveillance system, including monitoring people’s online behaviour.[40] According to Khamenei, network planning and coordination by a government authority was needed to protect individuals from the harms caused by the internet,[41] and he urged the judicial authorities to address the cyberspace issue.[42]

> Iran’s leadership has persistently resisted the idea of providing citizens with unrestricted internet access, claiming that its enemies are engaging in a hybrid warfare against ‘Islam and the Islamic Republic’, trying to ‘distort and destroy’ the clerical establishment in Iran through its media empire and the use of social media. In 2022, Ali Khameneicalled for the initiation of ‘an enlightenment jihad’.[43]

Most recently, the regime’s response to the digital age has become one of stringent control – an ‘iron veil’[44] – instrumentalized by a range of censorship techniques targeting both physical and digital domains.[45] First, the government has restricted internet access by reducing connectivity and prohibiting social media platforms in the country.[46] Individuals have somewhat circumvented such measures by using virtual private networks (VPNs) to access the internet, including to voice opposition, disseminate information and coordinate protests. The government, however, capitalized on this trend to augment domestic surveillance, enabling it to collect information on individuals and groups, as well as track their movements, internet communications and online activities.[47]

In parallel, over the past two decades, Iran has been working to establish a government-controlled secure national network named the National Information Network (NIN). Modelled on China’s Great Firewall and Russia’s RuNet,[48] the project would allow Iran to bypass the vulnerabilities associated with an internet overseen by companies based in countries that it considers to be hostile.[49] Indeed, the NIN has been described by the government as ‘completely undetectable and impenetrable by foreign sources’.[50] Moreover, by nationalizing internet services and infrastructure, the system would facilitate the filtering of online content accessible to Iranians, liberating them from ‘immoral, corrupt, and violent’ material.[51]

The digital nationalization initiative has been accompanied by efforts to pass the Cyberspace Users Rights Protection and Regulation of Key Online Services legislation (also known as the Protection Bill). The Bill proposes placing Iran’s internet infrastructure and gateways under the control of the armed forces and security agencies. It would also drive users onto national platforms by prohibiting VPN use[52] (users and distributors would risk being imprisoned for up to two years)[53] and throttling bandwidth.[54] Finally, if approved, the Bill would empower the Supreme Regulatory

Commission (SRC) with the authority and responsibility to execute and uphold its regulations.[55] This would likely streamline the implementation of internet shutdowns and online censorship,[56] arguably completing Iran's digital isolation.[57]

State officials justified the VPN ban as a means to promote domestic products, arguing that VPNs drive users away from domestic platforms to the detriment of Iranian companies. Banning VPNs also combats 'soft warfare waged by enemies', who 'seek to promote Western culture and values and undermine Iran through cyberspace'.[58]

The NIN needs to be understood as working in complement with Iran's mobile phone surveillance infrastructure. By regulation, all telecommunications providers operating in Iran are mandated to grant the Communication Regulatory Authority (CRA) direct access to their systems, allowing it to store user data, access user history and control access to mobile services.[59] Additionally, the CRA's Legal Intercept system (known by its Persian acronym SIAM[60]) integrates directly into mobile service provider systems, allowing it to directly manage independent mobile networks (including throttling cell phone connection speeds) and determine which users make use of VPNs.[61] This integration of surveillance and censorship capacities allows the government to collect detailed information on citizens and non-citizens from the moment they purchase SIM cards, including the content of their communications, their locations,[62] as well as personal identifiers such as birth certificates, passport numbers and home addresses.[63] If fully realized, the system would enable the CRA to directly oversee, intercept, redirect or block the mobile communications of all Iranians.[64]

Many of these tensions were brought into the spotlight on 16 September 2022, when 22-year-old Mahsa Amini died in a hospital in Tehran after being detained by Iran's Guidance Patrol for allegedly violating the *hijab* rule.[65] Amini's death ignited widespread protests, often referred to as the 'Woman, Life, Freedom Uprisings', which were ostensibly about the mandatory *hijab*, but also police brutality and lack of accountability. Since September 2022, social media platforms have been inundated with videos depicting unveiled women resisting the Guidance Patrol, as well as unveiled women in malls, restaurants, shops and streets. Security forces have responded harshly, including with arbitrary detentions and executions, torture, rape and sexual and gender-based violence.[66] This has been complemented by the blocking of social media platforms, throttling web traffic (to halt the dissemination of videos and communication among protesters) and leveraging Iran's digital surveillance system – which combines facial recognition, online activity monitoring and movement tracking[67] – to identify and punish dissidents.[68] According to Amnesty International, between April and July 2023, nearly one million women were notified by SMS for being unveiled inside their private vehicles.[69]

The disproportionate impact of such surveillance on women is linked to new legislation presented to the Iranian parliament in May 2023: the Bill to Support the Family by Promoting the Culture of Chastity and Hijab. The Bill proposes the installation of surveillance cameras in public places to identify women who are not wearing the veil, and outlines harsh penalties for transgressors.[70] Additionally, it imposes strict sanctions on public figures, celebrities, businesses and service providers who support activists and fail to enforce the *hijab* requirement.[71] These penalties include fines, the seizure of vehicles and communication devices, termination of employment and restrictions on accessing banking services, medical treatment and public transportation.[72] Repeat offenders can be sentenced to lengthy incarceration or be forced to attend 'morality schooling'.[73]

The practice of hijab, deeply rooted in the Islamic faith, remains a subject of contention even within Islamic scholarly circles.[74] While Quranic directives on modesty serve as the foundation for its legal obligation in Iran, they do not explicitly mention the hijab.[75] Moreover, the implementation and enhancement of artificial intelligence systems to enforce dress code violations may itself conflict with the Quran's emphasis on the sanctity of personal privacy.[76]

UNDER WATCH: MASS SURVEILLANCE AND PRIVACY RIGHTS IN UGANDA

Summary: In 2021, the Ugandan government launched the Intelligent Transport Monitoring System (ITMS), requiring the installation of surveillance cameras and cellular-network-connected tracking devices in all vehicles.[77] The government asserts that the ITMS is designed to 'protect diligent drivers and inform law enforcement about violators and criminals',[78] without encroaching on privacy rights. Human rights organizations, however, have expressed skepticism.[79] Specific concerns include the ITMS' potential to erode privacy rights, restrict freedom of movement, expression and association, and hinder access to information. Moreover, there is general concern that this represents a further proliferation of mass digital surveillance driven by national security imperatives and that it aims to suppress political dissent.[80] Such a fear has been exacerbated by the introduction of complementary legislation that, while not explicitly restricting online freedoms, includes broad and ambiguously defined provisions that could be exploited to curtail such freedoms.[81]

The Intelligent Transport Monitoring System

In 2018, following a spate of killings by individuals riding motorcycles targeting prominent political and government figures, the government of Uganda introduced the Nine-Point Security Plan aimed at preventing crime and safeguarding public security.[82] At the centre of the plan is the introduction of electronic license plates, which would allow the police to track, monitor and identify the owners of vehicles found at crime scenes.[83] To this end, on 23 July 2021,[84] the government signed a 10-year partnership agreement with a Moscow-based company to establish the Intelligent Transport Monitoring System (ITMS).[85] Over the next decade, the company will work with the government to install digital trackers on every public and private vehicle,[86] after which the ITMS will be locally operated.[87] Over time the system's surveillance capabilities will be augmented, including with facial recognition and traffic density cameras.

By January 2025,[88] every vehicle in the country (including foreign vehicles in Uganda temporarily[89]) will undergo registration for new plates at the owner/driver's expense. These will be equipped with a SIM card device supplied by the state-owned Uganda Telecommunications Corporation Ltd (UTL).[90] The SIM-enabled plates work like a Global Positioning System (GPS) tracker, delivering real-time information on a vehicle's whereabouts and owner to the national police command centre.[91]

Against growing criticism, the government has maintained that the aim of ITMS is to reduce vehicle theft and improve road safety,[92] while the Ministry of Security has committed to the initiative not surveilling people's movements generally.[93] Specifically, it has asserted that the trackers operate like regular surveillance cameras, and will only be activated in the event of a criminal incident to detect, track and identify which vehicles were present at the scene.[94] In terms of safeguards, the contract stipulates that all data collected, processed or stored shall comply with the Data Protection and Privacy Act of 2019.[95]

Critics, however, have noted that the government has not detailed concrete plans for oversight, nor measures to address human rights concerns.[96] Moreover, its lack of transparency regarding the technical details of the ITMS has raised questions around the scope for unmonitored mass surveillance, including of political opponents and dissidents.[97] Indeed the government has been accused of misusing security technologies in the past.[98] Most recently, in November 2020, the Uganda Police Force (UPF) used a combination of surveillance cameras, license plate readers and facial recognition technologies to locate and apprehend protesters in the lead-up to the 2021 elections.[99] This was enabled by a 2019 partnership valued at USD 126 million between the UPF and the Chinese telecommunications company Huawei to install closed-circuit and networked television cameras in public spaces.[100] These cameras were also used to intercept the encrypted communications of opposition politicians and monitor their activities.[101] Much like the ITMS, the system was justified by the government as a tool to strengthen law and order,[102] and as representing a reasonable limitation on the non-absolute right to privacy.[103]

Legislation and Digital Surveillance in Concert

The ITMS is not an outlier when it comes to citizen surveillance. Uganda's legal framework – specifically the Anti-Terrorism Act of 2002, the Regulation of Interception of Communications Act of 2010 and the Data Protection and Privacy Act of 2019 – grants the government extensive discretion in this regard. Article 19 of the Anti-Terrorism Act allows for the interception of communications and surveillance – without a court warrant[104] – not only of persons suspected of being involved in terrorism, but also for such purposes as safeguarding the public interest and the national economy.[105] The nature of such interception and surveillance is wide in scope, encompassing phone calls, emails, letters and postal packages, electronic surveillance, monitoring of meetings and access to bank accounts.[106]

In 2010, the Regulation of Interception of Communications Act (RICA) was passed, with Article 2 requiring that Ugandan intelligence and security agencies, including the UPF, be 'authorized by warrant' to conduct digital surveillance.[107] The regulation does not, however, supersede the Anti-Terrorism Act (2002), and it is reported that surveillance continues to take place in the absence of a warrant.[108] Further, Section 8 of the Act requires telecom companies and communication service providers to install surveillance and interception technology – broadly described as 'hardware and software facilities and devices' – in order to have the technical capability to support 'lawful interceptions at all times'.[109] Such deficits are mimicked in the Computer Misuse Act (2011),[110] which allows data to be collected and processed without the subject's consent when it is for the purposes of national security or law enforcement.[111]

The Data Protection and Privacy Act (2019) is perhaps the most vague. Section 7(2)(b) allows for the collection and processing of personal data, without consent, 'where it is necessary for the proper performance of a public duty by a public body, for national security and for the prevention, detection, investigation, prosecution or punishment of an offence or breach of law'.[112] The Act did charge the National Information Technology Authority Uganda (NITA-U) with responsibility for ensuring that 'every data collector, data controller, data processor or any other person collecting or processing data complies with the principles of data protection and this Act',[113] however did not grant it the power to impose penalties for non-compliance.[114]

A further area of concern is the work of the Uganda Communications Commission (UCC), the main regulator of broadcasting services in Uganda.[115] The UCC enjoys particularly broad discretionary powers during states of emergency where it may 'direct any operator to operate a network in a specified manner' and 'take temporary possession of any communication station within Uganda'.[116] A 2017 amendment to the Uganda Communications Act expanded the UCC's authority further by removing it from the oversight of the minister of telecommunications.[117]

Implications of Government Surveillance on Rights and Freedoms

As set out above, under the pretext of national security, Uganda has leveraged vague legislative provisions to conduct mass digital surveillance and communication interception. Arguably unconstitutional,[118] these measures directly affect the right to privacy, and create a corollary impact on other freedoms, such as the right to freedom of movement, freedom of expression and association and access to information. From an international law perspective, while freedom of expression and speech are not absolute rights and can be restricted by the state, vague provisions, a lack of sanctions and a paucity of empirical evidence that mass digital surveillance reduces criminal activity, would arguably fail to meet the conditions of legality and necessity. Further, the all-encompassing nature of the surveillance system, which potentially monitors the movements of all individuals at all times without exception, contradicts the universal standard of targeted surveillance and cannot be considered proportionate, even if restrictions on freedom of expression were deemed necessary.[119] Finally, the chilling impacts of surveillance regimes must be considered. The real-time tracking of vehicles introduced by the ITMS, for example, may cause individuals to hesitate to visit specific locations, interact with particular individuals or assemble to express certain viewpoints.[120] More generally, the sense of being constantly watched can promote conformity and compliance, discourage dissent and compel people to censor their behaviour and interactions.

BUILDING A MASS SURVEILLANCE SOCIETY IN THE RUSSIAN FEDERATION

Summary: Starting around 2011–2012, following a spate of mass protests that were largely coordinated and mobilized online, the Russian Government began to respond to the risks associated with a free and uncontrolled internet space. It introduced a complex array of restrictions led by different government ministries and empowered by broad (and at times draconian) legislation. Over time, however, it realized that a semi-restricted cyberspace offered a different kind of opportunity, namely the scope to glean granular information about anti-government threats, their content and the individuals leading them. This incentivized Russia to invest in a sophisticated system of mass and invasive surveillance. The government is unapologetic about this; the broad roll-out of facial recognition systems, for example, is an integral part of the Ministry of Digital Development's Data Economy Project, which aims to consolidate existing tools and data 'to create a holistic picture of citizens and their activities'.[121] The upshot is that in Russian society today, scrutiny by the state is ubiquitous, with the government actively monitoring social media accounts, intercepting private communications and using surveillance cameras to track the behaviour and activities of citizens.

In Russia, the internet (and social media in particular) is viewed as a form of soft power that can both influence the opinion of the masses and serve as a platform for intelligence gathering.[122] This is showcased in how Russia's cyber infrastructure has been built, the programmes the government runs and the technologies it is seeking to develop.

Russia's internet, commonly referred to as RuNet or its Russian acronym SORM, was built with wide surveillance capabilities. The system requires that all ISPs (internet service providers) install special interception devices that enable surveillance through deep packet inspection (DPI).[123] Moreover, SORM's hardware was developed with functionality to, for example, listen in on phone conversations, intercept emails and text messages and track internet communications.

To leverage this architecture, the government empowered Roskomnadzor, Russia's principal internet oversight body and an organ of the Ministry of Digital Development, to assist the domestic intelligence service (FSB) to monitor government opponents and identify potential emergent threats. Specifically, since 2020, it has been running a national surveillance programme to monitor online protest activities. In cooperation with the Ministry of the Interior and prosecution service, the programme surveils around 3,500 local and national accounts on the social networks VKontakte and Odnoklassniki, in addition to YouTube and Telegram channels. Increasingly, the project has used fake profiles and bot farms to gain access to member-only chat rooms and closed messaging services on social networks such as Vkontakte. At the local level, Roskomnadzor tracks 'points of tension' and events that could drive unrest, with the broader aim of identifying individuals perceived as a threat to the government and feeding this information back to the FSB and Interior Ministry. For example, in the eastern region of Bashkortostan, Roskomnadzor has compiled dossiers on critics, influencers and independent media outlets that share unfavourable views of the government that might gain traction with the public.[124]

Intelligence services have particularly homed in on the importance of monitoring encrypted cyber activity, such as WhatsApp and Signal, and to more precisely locate and monitor the movements of individuals of concern. Such demand has stoked a cottage industry of domestic tech contractors specializing in novel forms of digital surveillance. For example, the surveillance system used by the FSB was built by the technology company MFI Soft; it provides real-time information on the subscribers to telecommunications services, including data analytics of their internet traffic. A further MFI Soft tool, NetBeholder, maps the movements of mobile phones in a way that can suggest meetings between individuals,[125] or if an individual is switching between different phones to mask their activities.[126] Another Russian surveillance enterprise, Protei, sells software that automates the transcribing of intercepted phone calls from voice to text, facilitating the further profiling of individuals.[127]

Importantly, Russia's internet surveillance is not geared solely towards individuals, but equally to detect general behaviours and content that it deems undesirable. In February 2023, Oculus[128] was integrated into the domestic surveillance system, allowing intelligence services to scan the internet for unlawful content and 'destabilizing subjects', including unsanctioned protests, illegal assemblies, content that promotes drugs and LGBTQI+ propaganda.[129] The AI-based system makes this 'scraping' process very efficient; Oculus is capable of scanning text and recognizing visually-depicted illegal actions at a rate of around 200,000 images per day.[130]

THE CHALLENGE AND COMPLEXITY OF CORPORATE RESPONSIBILITY

NetBeholder software utilizes deep-packet inspection, a technique employed by ISPs to analyze data traffic to determine where communications should be routed. This allows it to detect when a user shares a file or makes a voice call on encrypted apps such as Signal, WhatsApp or Telegram. Critically, there is little that developers of Signal, Telegram and WhatsApp can do to prevent this sort of activity. The interception methods used by Russian authorities to surveil citizens leverage the data that service providers capture to monitor their own system's performance. As such, although the content of a specific message is obscured, records of exchanges are, by necessity, retained.[131]

Complementing internet restrictions and monitoring, Russia has introduced robust and invasive systems of video surveillance. In 2017, the Moscow city administration launched a video-enabled facial recognition initiative,[132] comprising more than 160,000 cameras, 3,000 of which were networked to the government's facial recognition database.[133] In 2018, during the FIFA World Cup, authorities had the opportunity to conduct large-scale testing of the new technology. It was reported that around 500 cameras were connected to the FindFace Security system developed by NtechLab, leading to around 180 people being apprehended and detained.[134] By 2020, the facial recognition system had been rolled out en masse, and extended to at least 10 other Russian cities.[135] A review of more than 2,000 court cases from this period concluded that the introduction of cameras was linked closely to protestor arrests, most of which concerned anti-government demonstration participation.[136]

A further 12,300 cameras with facial recognition capabilities have been integrated into the Moscow metro as part of its fare payment system. Images of passengers are captured and retained as they pass through the gates and an algorithm compares the biometric features of the individual against the faces of persons wanted by authorities. The time taken between a system identification alert and the arrival of local law enforcement is generally a few minutes.[137] It has been reported that, of those detained, most are not in the process of travelling to a protest but rather commuting to work or attending a social event. Moreover, detainees are frequently required to sign a document promising not to protest or acknowledging that they have received a warning against protesting.[138]

Importantly, since the full-scale invasion of Ukraine in February 2022, Russian authorities seem to have pivoted away from using facial recognition to detect and arrest protestors, to preventing protests from occurring in the first instance. Leveraging laws that prohibit 'public actions aimed at discrediting the use of the armed forces of the Russian Federation', [139] facial recognition has been used to identify and arrest government opponents pre-emptively, likely as part of a broader effort to prevent public displays of dissent and suppress anti-war sentiment.

LEVERAGING TECH COLLABORATIONS

Importantly, despite efforts to automate its intelligence gathering on its citizens, Russia still relies on outside companies to both undertake monitoring and to improve the technologies being used, such as by training facial recognition systems. For example, NTechLab and Tevian (which were sanctioned by the EU in July 2023 for their role in the detention of Russian protesters), have provided software to Moscow that continuously scans faces to match with a watchlist. In 2024, the government used facial recognition algorithms trained by Toloka (a platform run by companies in the Netherlands, Switzerland and Russia), to identify and arrest at least 19 individuals participating in ceremonies commemorating Alexei Navalny, the opposition leader who died in a Russian prison in February 2024.[140]

Bringing these findings together, indicators suggest that civilian monitoring and surveillance in Russia is set to grow. As of the time of writing, the facial recognition system has been rolled out in 62 regions and traffic lights with facial recognition are set for pilot testing. Finally, to close the circle on internet monitoring, Russia is in the process of creating a 'Super App' (modelled on China's WeChat) that will bring social networking, messaging, services and e-government into a single unifying application.[141] Russia sees this as an opportunity to both filter content and monitor and enable the dissemination of propaganda, as it creates a single entry point into a user's network.[142]

CONCLUSIONS

As set out above, the past two decades have witnessed a vast increase in the prevalence and sophistication of technological tools used to collect data on the communications, associations, location and movements of both individuals and groups. This has been fast-tracked by advancements such as 5G-enabled services,[143] edge computing, artificial intelligence and machine learning techniques, which together have widened the scope of data collection, increased the speed by which it can be assessed and deepened the complexity of analysis for various ends. This has enabled a trend towards the mass monitoring of activity, movement and social interactions.[144] Indeed, cases brought before the European Court of Human Rights increasingly reflect states' propensity to develop ubiquitous programmes of surveillance for use by intelligence services, law enforcement and other public authorities.[145]

The outcomes from a rights perspective are broad-reaching. When states misuse surveillance technologies to monitor not only the content of civil society activity but also those who organize and participate in it, the result can be to hinder civic participation and/or quash political dissent.[146] It can also repress emergent civil society groups, leading to a contraction of the democratic space. Monitoring people's communications in particular can create a chilling effect on debate and the interchange of ideas, both of which are critical to enabling a plurality of opinions to be expressed. When such monitoring categorizes behaviours and preferences into pre-existing frameworks, the result can be to promote social conformity and control. This marginalizes those who deviate from the norm, creating particular risks for minorities and other vulnerable groups.[147]

Trends in monitoring also have implications for privacy. Indeed, in modern society, the groups that form to associate or assemble extend far beyond the political realm to include, for example, sexual identity groups, groups advocating for gender equality, environmental human rights defenders, etc. Especially for younger generations, online platforms (such as social media and messaging apps) are widely used as a means to build community and mobilize, both online and offline.[148] The upshot is that as individuals become more connected, their lives are intermeshed with fora that can be surveilled. Even for those not engaged in civil society movements, the massive 'dragnets' (widespread, indiscriminate data collection) used in many surveillance systems have widened the scope for unwarranted mass surveillance.

A further area of risk concerns the pooling and cross-analysis of surveillance data with other open-source information (observed behaviours, financial and commercial transactions, installed applications in a smartphone, social network profiles, etc.) using methods such as social graph analysis. This can deliver a complex and informative profile of an individual,[149] including their political beliefs, religion or sexual orientation.[150] Such data can be leveraged for constructive ends, for example detecting and solving crime,[151] or to forecast risks around violence or public safety that may extend from civic activism.[152] Indeed, it is under such aims that most surveillance is authorized from a legal standpoint. However, malign uses also exist, such as the monitoring of protest movements and political opposition groups, and the identification of minorities such as LGBTQI+ or human rights defenders. Such data can also be used to undertake profiling, i.e. classifying attributes of an individual's behaviour and/or their associations to draw conclusions on likely future behaviour. This is a particular concern insofar as it compromises autonomy and agency. Moreover, when profiling draws linkages based on gender, race, religion etc., existing biases can be exacerbated and individual rights to equality and protection against discrimination infringed.[153]

Finally, the risks associated with technical errors need to be acknowledged. For example, while advances have been made in the accuracy of facial recognition technology, false positives remain a concern. Such problematics are rooted in biases and non-representativeness in the datasets underpinning such technologies, making the technology less accurate in identifying individuals with darker skin tones and women.[154] This creates scope not only for discriminatory outcomes but also to amplify existing racial and gender biases. Such risks carry over to other technologies, such as crowd management software and the use of social network analysis by law enforcement. Here the issue is that individuals whose lifestyles are less 'datafied' vis-à-vis the general population (due to poverty, geography or because they live on the margins of society) are not included in the data that feed the technology.[155] As such, the Big Data sets collected contain 'dark zones' where certain citizens or communities are overlooked or underrepresented, creating scope for discrimination.[156]

In terms of international human rights law, information gathering, whether by public or private entities, including through surveillance or the interception of communications, must be consistent with standalone rights, including the right to privacy and protection from discrimination, as well as interdependent human rights, such as freedom of assembly and freedom of movement. The principle of proportionality requires that the effects of monitoring should not be excessive and that authorities should minimize the resulting interference caused by the surveillance activity. Monitoring, whether conducted covertly or overtly, should never be aimed at intimidation, harassment or limiting people's freedom of expression. Surveillance practices must be regulated by appropriate and publicly accessible domestic legal frameworks and allow for sufficient transparency and scrutiny by the courts.[157]

Only in exceptional circumstances are more invasive forms of surveillance permitted, for example to protect national security or safeguard rights and liberties (such as the right to life) in situations where public order is at risk.[158] Such limits must be set out in law and be sufficiently accessible to the public, clear and precise so that any individual may without difficulty review the legislation and determine who is authorized to conduct surveillance activities, and under what circumstances. Limitations must not breach core rights protections and must be both necessary and proportionate to serving a legitimate purpose and the least intrusive option available.[159] Moreover, the limitation must be shown to be plausible and to have a reasonable chance of achieving its objective. The onus is on the authorities seeking to limit the right to show that the limitation is clearly connected to achieving a legitimate aim.[160] States are also responsible for protecting individuals' rights from abuse by non-state entities, including companies engaged in surveillance and monitoring and their collection, processing and retention of personal data.[161] States' obligations also include ensuring that personal information held by public authorities is not leaked or misused, and transparency with respect to what information is collected and retained.[162]

END NOTES

[1] See S Lockwood, 'Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators', 18 Harvard Journal of Law and Technology (2004) 313–14.

[2] S. Barocas and A. D. Selbst, 'Big Data's Disparate Impact', 104 California Law Review (2016) 685.

[3] 'Dual-use technology' typically refers to technology that can be used for both civilian and military purposes.

[4] See I. D. Constantiou and J. Kallinikos, 'New Games, New Rules: Big Data and the Changing Context of Strategy', 30 Journal of Information Technology (2015) 44.

[5] M. Land and J. Aronson, 'Human Rights and Technology: New Challenges for Justice and Accountability', 16 Annual Review of Law and Social Science (2020) 223–226.

[6] See generally, M. Brunati, M. Conti and A. Tezza, 'SNIFFO: Security of Networks and Intelligence for Field Operations', in 2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE, 2017.

[7] L. Vomfell, W. K. Härdle and S. Lessmann, 'Improving Crime Count Forecasts Using Twitter and Taxi Data', Decision Support Systems 113 (2018), 73.

[8] T. Kaldani and Z. Prokopets, 'Pegasus Spyware and Its Impacts on Human Rights', DGI (2022) 04 Council of Europe, 2022, p 7; Amnesty International, 'German-Made FinSpy Spyware Found in Egypt, and Mac and Linux Versions Revealed', 25 September 2020, https://www.amnesty.org/en/latest/research/2020/09/german-made-finspy-spyware-found-in-egypt-and-mac-and-linux-versions-revealed/ (last accessed 24 January 2025).

[9] Kaldani, and Prokopets, 'Pegasus Spyware', supra fn 8, p 18.

[10] OHCHR, The right to privacy in the digital age, A/HRC/51/17, 4 August 2022, Available at: https://documents.un.org/doc/undoc/gen/g22/442/29/pdf/g2244229.pdf , at para. 5. See also: Carnegie Endowment for International Peace, Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses, March 2023. Available at: https://carnegie-production-assets.s3.amazonaws.com/static/files/Feldstein_Global_Spyware.pdf

[11] Kaldani, and Prokopets, 'Pegasus Spyware', supra fn 8, pp 7–8.

[12] The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights, UN doc A/HRC/51/17, 4 August 2022, §6. See further Amnesty International, The Predator Files: Caught in the Net. The Global Threat From 'EU Regulated' Spyware, 2023, https://www.amnesty.org/en/documents/act10/7245/2023/en/ (last accessed 24 January 2025).

[13] J. Menn, M. Hoppenstedt, M. Birnbaum, Y. Philippin, R. Buschmann and N. Naber, 'Vietnam Tried to Hack U.S. Officials, CNN With Posts on X, Probe Finds', The Washington Post, 9 October 2023, https://www.washingtonpost.com/technology/2023/10/09/vietnam-predator-hack-investigation/.

[14] See generally, C. Fontes, E. Hohma, C. C. Corrigan and C. Lütge, 'AI-Powered Public Surveillance Systems: Why We (Might) Need Them and How We Want Them', 71 Technology in Society (2022).

[15] See generally C. Weinbaum, S. Berner and B. McClintock, SIGINT for Anyone: The Growing Availability of Signals Intelligence in the Public Domain, RAND Corporation, 2017, https://www.rand.org/pubs/perspectives/PE273.html (last accessed 24 January 2025).

[16] U. Uebler and H-J. Kolb, 'Signals Intelligence – Processing – Analysis – Classification', MEDAV GmbH Uttenreuth (Germany), Tech. Rep., 2009.

[17] F. Palmiotto and N. Menéndez González, 'Facial Recognition Technology, Democracy and Human Rights', 50 Computer Law & Security Review (2023): 4.

[18] P. Kaur, K. Krishan, S. K. Sharma and T. Kanchan, 'Facial-Recognition Algorithms: A Literature Review', 60 Medicine, Science and the Law 2 (2020) pp. 131–133.

[19] Impact of New Technologies, supra fn 10, §30.

[20] American Civil Liberties Union, 'Stingray Tracking Devices: Who's Got Them?', November 2018, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices.

[21] Impact of New Technologies, supra fn 10, §28.

[22] V. Acuna, A. Kumbhar, E. Vattapparamban, F. Rajabli and I. Guvenc, 'Localization of WiFi Devices Using Probe Requests Captured at Unmanned Aerial Vehicles', in 2017 IEEE Wireless Communications and Networking Conference (WCNC), IEEE 2017, pp 1-6.

[23] See generally, P. F. Scott, 'Secrecy and Surveillance: Lessons from the Law of IMSI Catchers', 33 International Review of Law, Computers & Technology 3 (2019) 349.

[24] See generally, R. Butler, 'Stingray Stung? Analyzing Cellphones as Effects Provides Fourth Amendment Treatment', 34 Harvard Journal of Law & Technology 2 (2020) 733.

[25] See further K. Zetter, 'How Cops Can Secretly Track Your Phone – A Guide to Stingray Surveillance Technology, Which May Have Been Deployed at Recent Protests', The Intercept, 31 July 2020, https://theintercept.com/2020/07/31/protests-surveillance-stingrays-dirtboxes-phone-tracking/.

[26] Technology researcher Anas Basalamah notes on this point: 'WiFi-enabled devices periodically broadcast management frames called probes in search for nearby access points. These probes are sent in clear text and carry useful data such as device MAC address, which acts as a unique identifier for this particular device. Reading these over-the-air packets using low-cost sniffers enables us to identify the presence of people at the 50-100 metre range … Placing several sniffers around the city (or monitored spaces) allows us to understand the mobility of crowds by the observing the density of probes, dual times, and mobility traces across multiple sniffers.' See A. Basalamah, 'Crowd Mobility Analysis Using WiFi Sniffers', 7 International Journal of Advanced Computer Science and Applications 12 (2016) 374.

[27] G. Danezis, S. Lewis and R. Anderson, 'How Much is Location Privacy Worth?', 4th Annual Workshop on the Economics of Information Security, WEIS 2005, Harvard University, June, p 2, https://infosecon.net/workshop/pdf/location-privacy.pdf (last accessed 24 January 2025); S. E. Henderson, 'Carpenter v. United States and the Fourth Amendment: The Best Way Forward', 26 William & Mary Bill of Rights Journal (2017); K. Martin and H. Nissenbaum, 'What Is It About Location?', 35 Berkeley Technology Law Journal (2020) 101.

[28] See generally: P. Klasnja, S. Consolvo, T. Choudhury, R. Beckwith and J. Hightower, 'Exploring Privacy Concerns About Personal Sensing', in H. Tokuda, M. Beigl, A. Friday, A. J. Bernheim Brush and Y. Tobe (eds), Pervasive Computing: 7th International Conference, Pervasive 2009, Nara, Japan, May 11-14, 2009, Proceedings, Springer, 2009; T. Althoff, R. Sosič, J. L. Hicks, A. C. King, S. L. Delp and J. Leskovec, 'Large-Scale Physical Activity Data Reveal Worldwide Activity Inequality', Nature 547 (2017): 336).

[29] See further R. Wilken, 'Places Nearby: Facebook as a Location-Based Social Media Platform', 16 New Media & Society 7 (2014). See also E. Williams and J. Yerby, 'Google and Facebook Data Retention and Location Tracking Through Forensic Cloud Analysis' (2019), SAIS 2019 Proceedings, https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1002&context=sais2019 (last accessed 24 January 2025).

[30] L. Humski, D. Pintar and M. Vranić, 'Analysis of Facebook Interaction as Basis for Synthetic Expanded Social Graph Generation', 7 IEEE Access (2019), https://ieeexplore.ieee.org/abstract/document/8573573 (last accessed 24 January 2025). See also the early identification of location as a means to draw inferences in social relations between users in N. Akhtar, H. Javed and G. Sengar, 'Analysis of Facebook Social Network', in Proceedings of the 5th International Conference and Computational Intelligence and Communication Networks, Mathura, 2013.

[31] Business Foursquare differentiated itself by its location feature to encourage

live 'check-ins', self-identify and share patterns of users' movements. See, for example, J. Cranshaw, R. Schwartz, J. Hong and N. Sadeh, 'The Livehoods Project: Utilizing Social Media to Understand the Dynamics of a City', 6 Proceedings of the Sixth International AAAI Conference on Weblogs and Social Media 1 (2012), https://ojs.aaai.org/index.php/ICWSM/article/view/14278/14127 (last accessed 24 January 2025).

[32] See further V. Safronova, 'The Rise and Fall of Yik Yak, the Anonymous Messaging App', The New York Times, 27 May 2017, https://www.nytimes.com/2017/05/27/style/yik-yak-bullying-mary-washington.html. See also N. C. Russell, F. Schaub, A. McDonald and W. Sierra-Pambley, APIs and Your Privacy, Fordham Center on Law and Information Policy (Fordham CLIP) and University of Michigan, January 2019, http://dx.doi.org/10.2139/ssrn.3328825.

[33] S. Akbarzadeh, A. Naeni, I. Yilmaz and G. Bashirov, 'Cyber Surveillance and Digital Authoritarianism in Iran', 4 Global Policy (2024) 4. Digital authoritarianism is understood as 'the use of digital information technology by authoritarian regimes to monitor, suppress and manipulate both domestic and foreign populations' (see ibid). See also M. Alimardani, 'Aggressive New Digital Repression in Iran in the Era of the Woman, Life, Freedom Uprisings', in New Digital Dilemmas: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms, Carnegie Endowment for International Peace, 2023; A. Taghati, 'Iran News: Iranian Regime's New Push to Launch National Web Raises Concerns Over Internet Restrictions', National Council of Resistance of Iran (NCRI), 17 April 2024, https://www.ncr-iran.org/en/news/anews/iran-news-iranian-regimes-new-push-to-launch-national-web-raises-concerns-over-internet-restrictions/ (last accessed 24 January 2025).

[34] Iran's government refers to internet filtering, not internet censorship, describing it as 'a preventive policy pursued by governments based on their value structures meant to purify the cyberspace'. See A. Hashemzadegan and A. Gholami, 'Internet Censorship in Iran: An Inside Look', 6 Journal of Cyberspace Studies 2 (2022) 186–187, https://doi.org/10.22059/JCSS.2022.349715.1080.

[35] 'Iranian Parliament Orders Surveillance on Citizens' Private Lives', Iran International, 11 August 2023, https://www.iranintl.com/en/202311086719.

[36] See Alimardani, 'Aggressive New Digital Repression in Iran', supra fn 33, p 9.

[37] Hashemzadegan and Gholami, 'Internet Censorship in Iran', supra fn 34, 185.

[38] See 'Iranian Parliament Orders Surveillance on Citizens' Private Lives', supra fn 35; Hashemzadegan and Gholami, supra fn 34, 196.

[39] K. S. Isfahani, 'Tehran Cooked up a Conspiracy Theory Blaming Israel for US TikTok ban', IranSource, Atlantic Council, 5 April 2024, https://www.atlanticcouncil.org/blogs/iransource/iran-tiktok-ban-israel-adl-greenblatt-conspiracy-theory/ (last accessed 24 January 2025).

[40] See Akbarzadeh et al, 'Cyber Surveillance and Digital Authoritarianism in Iran', supra fn 33, 2–4; Hashemzadegan and Gholami, 'Internet Censorship in Iran', supra fn 34, 188.

[41] Decree on the Formation and Appointment of Members of the Supreme Council of Cyberspace, 2012, https://farsi.khamenei.ir/message-content?id=19225 (in Persian, last accessed 24 January 2025).

[42] 'Ali Khamenei Once Again Demanded to Deal with Cyberspace: "If You Don't Have a Law, Get One Quickly"', Radio Farda, 28 June 2022, https://www.radiofarda.com/a/ali-khamenei-attack-social-media-iran/31919702.html (in Persian, last accessed 24 January 2025.

[43] S. Isfahani, 'The Internet Has No Place in Khamenei's Vision for Iran's Future', IranSource, Atlantic Council, 25 July 2022, https://www.atlanticcouncil.org/blogs/iransource/the-internet-has-no-place-in-khameneis-vision-for-irans-future/ (last accessed 24 January 2025).

[44] See Isfahani, 'Tehran Cooked up a Conspiracy Theory', supra fn 39.

[45] See Akbarzadeh et al, 'Cyber Surveillance and Digital Authoritarianism in Iran', supra fn 33, 2; 'Iranian Parliament Orders Surveillance on Citizens' Private Lives', supra fn 35.

[46] 'Iranian Parliament Orders Surveillance on Citizens' Private Lives', supra fn 35.

[47] See Akbarzadeh et al, 'Cyber Surveillance and Digital Authoritarianism in Iran', supra fn 33, 6-8. Authorities created 'fake VPNs' that prevent users from accessing international webpages while also enabling a close monitoring of people's activities online, including revealing their true identity.

[48] Additionally, it is believed that both governments have provided Iranian authorities with surveillance technologies and mechanisms of detection. China has assisted in developing the infrastructure and surveillance algorithms for the NIN, while Russia has provided Iran with 'communication-surveillance capabilities as well as eavesdropping devices, advanced photography devices and lie detectors'. See Digital Watch Observatory, 'Iran to Implement National Information Network to Keep People off the Internet', 11 September 2023, https://dig.watch/updates/iran-to-implement-national-information-network-to-keep-people-off-the-internet (last accessed 24 January 2025); R. Stone, 'Iran's Researchers Increasingly Isolated as Government Prepares to Wall Off Internet', Science, 11 September 2023, https://www.science.org/content/article/iran-s-researchers-increasingly-isolated-government-prepares-wall-internet; 'Report: Russia Provides Iran With Digital Surveillance Capabilities', IranWire, 28 March 2023, https://iranwire.com/en/technology/115074-report-russia-provides-iran-with-digital-surveillance-capabilities/.

[49] R. Kumar, 'As the World Focuses on Ukraine, Iran is on the Verge of Becoming an Internet Black Hole', Reuters Institute for the Study of Journalism, 5 April 2022, https://reutersinstitute.politics.ox.ac.uk/news/world-focuses-ukraine-iran-verge-becoming-internet-black-hole (last accessed 24 January 2025).

[50] S. A. Williams, 'Iranian National Information Network', Master of Operational Arts and Sciences Research Report, Air Command and Staff College, Air University, 2019, p 7, https://apps.dtic.mil/sti/pdfs/AD1107324.pdf (last accessed 24 January 2025).

[51] See Kumar, 'As the World Focuses on Ukraine, Iran is on the Verge of Becoming an Internet Black Hole', supra fn 49.

[52] See also S. Kia, 'Deciphering Iran's Regime Backpedaling of VPN Ban and Exploring Future Motives', NCRI, 28 February 2024, https://www.ncr-iran.org/en/news/society/deciphering-irans-regime-backpedaling-of-vpn-ban-and-exploring-future-motives/ (last accessed 24 January 2025); M. Motamedi, 'Iran Unveils Plan for Tighter Internet Rules to Promote Local Platforms', Al Jazeera, 24 February 2024, https://www.aljazeera.com/news/2024/2/24/iran-unveils-plan-for-tighter-internet-rules-to-promote-local-platforms.

[53] See Alimardani, 'Aggressive New Digital Repression in Iran', supra fn 33. See also M. Alimardani, 'New "Protection" Bill on Internet Freedom', United States Institute of Peace, 23 February 2022, https://iranprimer.usip.org/blog/2021/oct/14/internet-freedom-iran-and-new-protection-bill (last accessed 24 January 2025).

[54] The latter provision represents a notable shift in that while throttling has been employed in the past, it has never been a recognized government policy. See ARTICLE 19, 'Iran: Parliament Moves to Ratify Central Elements of Oppressive Internet Bill', 23 February 2022, https://www.article19.org/resources/iran-parliament-ratifies-central-elements-of-oppressive-internet-bill/ (last accessed 24 January 2025).

[55] See Alimardani, 'New "Protection" Bill on Internet Freedom', supra fn 53.

[56] See ARTICLE 19, 'Iran: Parliament Moves to Ratify Central Elements of Oppressive Internet Bill', supra fn 54.

[57] G. Miller, N. Aljizawi, K. Ermoshina, M. Michaelsen, Z. Pandey, G. Plumptre, A. Senft and R. Deibert, 'You Move, They Follow: Uncovering Iran's Mobile Legal Intercept System', The Citizen Lab, 16 January 2023, https://citizenlab.ca/2023/01/uncovering-irans-mobile-legal-intercept-system/ (last accessed 24 January 2025).

[58] See Kia, 'Deciphering Iran's Regime Backpedaling', supra fn 52.

[59] The Communication Regulatory Authority (CRA) operates under the supervision of the Ministry of Information and Communications Technology and is responsible for overseeing and regulating various aspects of communication and telecommunications within the country.

[60] The SIAM consists of several functional components working in concert: the Legal Intercept (LI) System, directly interfacing with mobile service providers, in

charge of conducting usage surveillance; the Control Illegal Devices (CID) System, responsible for controlling and detecting changes in a user's service profile or SIM cards; the SHAHKAR System, tasked with storing information about mobile subscribers; and the SHAMSA, which collects information for data analysis.

[61] S. Biddle and M. Hussain, 'Hacked Documents: How Iran Can Track and Control Protesters' Phones', The Intercept, 28 October, 2022, https://theintercept.com/2022/10/28/iran-protests-phone-surveillance/.

[62] Utilizing the 'LocationCustomerList' command enables SIAM operators to observe which phone numbers have been linked to designated cell towers, alongside their associated IMEI numbers (a distinct string of digits assigned to each mobile phone globally). Hence, if there is a location experiencing a protest, SIAM can furnish a list of all phone numbers currently present at that site.

[63] T. Starks and A. Schaffer, 'Iran Sought a Surveillance Project with "Unprecedented" Reach', The Washington Post, 17 January 2023, https://www.washingtonpost.com/politics/2023/01/17/iran-sought-surveillance-project-with-unprecedented-reach/.

[64] See Miller et al, 'You Move, They Follow', supra fn 57; Biddle and Hussain, 'Hacked Documents', supra fn 61. Using the 'ApplySuspIp' command, SIAM is able to completely sever the internet connection of any mobile phone on the network for specified durations or indefinitely. Comparable commands would enable SIAM to prohibit a user from making or receiving calls.

[65] 'Iran Installs Cameras in Public Places to Identify, Penalise Unveiled Women', Reuters, 11 April 2023, https://www.reuters.com/world/middle-east/iran-installs-cameras-public-places-identify-penalise-unveiled-women-police-2023-04-08/.

[66] See Amnesty International, 'Iran: Executions of Tortured Protesters Must Trigger a Robust Reaction From the International Community', 19 May 2023, https://www.amnesty.org/en/latest/news/2023/05/iran-executions-of-tortured-protesters-must-trigger-a-robust-reaction-from-the-international-community/; Amnesty International, 'Iran: Security Forces Used Rape and Other Sexual Violence to Crush "Woman Life Freedom" Uprising With Impunity', December 6, 2023, https://www.amnesty.org/en/latest/news/2023/12/iran-security-forces-used-rape-and-other-sexual-violence-to-crush-woman-life-freedom-uprising-with-impunity/; Amnesty International, 'Iran: Executions of Protester with Mental Disability and Kurdish Man Mark Plunge into New Realms of Cruelty', 24 January 2024, https://www.amnesty.org/en/latest/news/2024/01/iran-executions-of-protester-with-mental-disability-and-kurdish-man-mark-plunge-into-new-realms-of-cruelty/ (all accessed 24 January 2025).

[67] See Alimardani, 'Aggressive New Digital Repression in Iran', supra fn 33. See also K. Johnson, 'Iran Says Face Recognition Will ID Women Breaking Hijab Laws', Wired, 10 January 2023, https://www.wired.com/story/iran-says-face-recognition-will-id-women-breaking-hijab-laws/.

[68] E. Gibson, 'Dissidents and Women Are Targeted by Iran's High-Tech Surveillance', Fair Observer, 30 September 2023, https://www.fairobserver.com/world-news/iran-news/dissidents-and-women-are-targeted-by-irans-high-tech-surveillance/. The utilization of technology for this purpose was initially mentioned in September 2022, when the leader of an Iranian government agency responsible for enforcing morality laws discussed plans to employ technology to detect 'inappropriate and unusual movements', such as instances of non-compliance with hijab regulations. See Johnson, 'Iran Says Face Recognition Will ID Women Breaking Hijab Laws', supra fn 67.

[69] Amnesty International, 'Iran: International Community Must Stand With Women and Girls Suffering Intensifying Oppression', 26 July 2023, https://www.amnesty.org/en/latest/news/2023/07/iran-international-community-must-stand-with-women-and-girls-suffering-intensifying-oppression/ (last accessed 24 January 2025).

[70] A. Bajec, 'As Iran Doubles Down on Hijab Laws, Women Fight Back', The New Arab, 14 August 2023, https://www.newarab.com/analysis/iran-doubles-down-hijab-laws-women-fight-back.

[71] See Gibson, 'Dissidents and Women Are Targeted by Iran's High-Tech Surveillance', supra fn 68; C. Alkhaldi and N. Ebrahim, 'Iran Proposes Long Jail Terms, AI Surveillance and Crackdown on Influencers in Harsh New Hijab Law', CNN, 2 August 2023, https://edition.cnn.com/2023/08/02/middleeast/iran-hijab-draft-law-mime-intl/index.html.

[72] Amnesty International, 'Iran: International Community Must Stand With Women and Girls Suffering Intensifying Oppression', supra fn 69.

[73] See Johnson, 'Iran Says Face Recognition Will ID Women Breaking Hijab Laws', supra fn 67.

[74] T. Alkiek, 'Is Hijab Religious or Cultural? How Islamic Rulings Are Formed', Yaqeen Institute for Islamic Research, 25 March 2021, https://yaqeeninstitute.org/read/paper/is-hijab-religious-or-cultural-how-islamic-rulings-are-formed (last accessed 24 January 2025). A. Piela, 'Muslim Women and the Politics of the Headscarf', JSTOR Daily, 6 April 2022, https://daily.jstor.org/muslim-women-and-the-politics-of-the-headscarf/ (last accessed 24 January 2025). The diverse array of definitions results in differing interpretations regarding the necessity of head-covering; some assert it as obligatory, while others consider it discretionary.

[75] T. Alkiek, 'Is Hijab Religious or Cultural?', supra fn 74.

[76] Quran 24:27 reads: 'Enter not houses other than your own houses until you have obtained the permission of the inmates'. Quran 49:12 reads: 'Believers, avoid being excessively suspicious, for some suspicion is a sin. Do not spy'. See also, for example, M. A. Hayat, 'Privacy and Islam: From the Quran to Data Protection in Pakistan', 16 Information & Communications Technology Law 2 (2007).

[77] F. Kisakye, 'New Vehicle Tracking Raises Alarm Over Privacy Violations', The Observer, 29 November 2023, https://observer.ug/news/new-vehicle-tracking-raises-alarm-over-privacy-violations/.

[78] See Art. Lebedev Studio, 'Uganda Intelligent Transport Monitoring System Brand Platform and Identity', https://www.artlebedev.com/uganda/itms/ (last accessed 24 January 2025).

[79] S. Neiman, 'Uganda Could Be Adding a New Tool for Repression to Museveni's Kit', World Politics Review, 5 January 2024, https://www.worldpoliticsreview.com/uganda-museveni-human-rights/.

[80] D. Mukasa, 'A GPS Tracker on Every "Boda Boda": A Tale of Mass Surveillance in Uganda', Center for Human Rights & Global Justice, 13 October 2021, https://chrgj.org/2021/10/13/a-gps-tracker-on-every-boda-boda-a-tale-of-mass-surveillance-in-uganda/ (last accessed 24 January 2025).

[81] L. Nitsche, 'Digital Rights: Civic Space Continues to be Constrained', DW Akademie, 4 May 2018, https://akademie.dw.com/en/digital-rights-civic-space-continues-to-be-constrained/a-43625163.

[82] Human Rights Watch, 'Uganda: Rights Concerns Over License Plate Tracking', 14 November 2023, https://www.hrw.org/news/2023/11/14/uganda-rights-concerns-over-license-plate-tracking (last accessed 24 January 2025).

[83] Ibid.

[84] Even though the roll-out of the project was supposed to be 1 March 2024, it had to be postponed to 1 July 2024, due to logistical challenges; see Republic of Uganda, Joint Media Statement on Implementation of the Intelligent Transport Monitoring System Project by the Minister for Security and the Minister for Works and Transport on 4th July 2024, at the Uganda Media Center, 4 July 2024, p 3, Uganda Media Centre | MINISTRY OF ICT AND NATIONAL GUIDANCE | REPUBLIC OF UGANDA (last accessed 24 January 2025).

[85] Eagle Online, 'Russian Firm to Make Vehicle Trackers in Uganda', 10 March 2022, Russian firm to make vehicle trackers in Uganda - Eagle Online.

[86] Parliament of the Republic of Uganda, Report of the Joint Committee of the Committees of Defence and Internal Affairs; and Physical Infrastructure on Investigations on the Implementation of the Intelligent Transport Monitoring System by M/S Joint Stock Company Global Security, May 2023, Section 8.3, 'Observation', p 14.

[87] See Neiman, 'Uganda Could Be Adding a New Tool for Repression to Museveni's Kit', supra fn 79.

[88] See Republic of Uganda, Joint Media Statement on Implementation of the Intelligent Transport Monitoring System Project, supra fn 84, p 6.

[89] See Human Rights Watch, 'Uganda: Rights Concerns Over License Plate Tracking', supra fn 82.

[90] Ibid: 'As part of the system, all vehicle owners will, after February 1, 2024, be required to pay between 50,000 and 714,300 Uganda shillings (about US$13 to US$190) to register their vehicles for new plates'.

[91] S. Beeghly, 'HRW: Uganda Surveillance System Threatens Rights to Privacy, Expression and Association', Jurist, 14 November 2023, https://www.jurist.org/news/2023/11/hrw-uganda-surveillance-system-threatens-rights-to-privacy-expression-and-association/.

[92] See ibid.

[93] The Independent, 'Vehicle surveillance system to monitor criminals – Gen Muhwezi', 23 February 2022, Vehicle surveillance system to monitor criminals - Gen Muhwezi.

[94] See also Parliament of the Republic of Uganda, Report of the Joint Committee of the Committees of Defence and Internal Affairs, supra fn 86, Section 5.1, 'Specific objectives of ITMS', p 4: 'The specific objectives of the project are: crime management through detection, tracking, identification and recognition of all vehicles and motorcycles operating in the country.'

[95] Ibid, Section 8.1, 'Observations', para iii, p 9: 'Article 7.1 of the ITMS Agreement provides that "The Parties shall ensure that Personal Data is collected, processed and stored in accordance with the Data Protection and Privacy Act, 2019. No party shall use any personal data collected, processed or stored for purposes other than for the objects of this Agreement. Therefore, the ITMS is mindful of the Data protection and privacy Laws of the Country.'

[96] Section 20 of this Act requires that the data collector, in this case, the ITMS, 'secure[s] the integrity of personal data' in its possession by adopting appropriate measures to prevent the 'loss, damage, or unauthorised destruction and unlawful access to or unauthorised processing of the personal data'. See Neiman, 'Uganda Could Be Adding a New Tool for Repression to Museveni's Kit', supra fn 79. See also Unwanted Witness, 'Uganda's Facial Recognition Technology Threatens Privacy', 7 November 2018. https://www.unwantedwitness.org/ugandas-facial-recognition-technology-threatens-privacy/ (last accessed 24 January 2025).

[97] L. Nitsche, 'Digital Rights', supra fn 81; N. Konde, 'No to Big Brother: The Legality and Implications of Mass Digital Surveillance in Uganda', 1 African Journal of Legal Issues in Technology and Innovation 1 (2023) 194–213.

[98] See, Unwanted Witness, State of Security for Human Rights Defenders in a Digital Era. Ugandan Case: Perception and Practices, n.d., https://www.unwantedwitness.org/download/uploads/State-of-Security-for-HRDs-In-a-Digital-Era.pdf (last accessed 24 January 2025).

[99] Mukasa, 'A GPS Tracker on Every "Boda Boda"', supra fn 80.

[100] Ibid.

[101] E. R. Sekyewa, 'What Ugandan Authorities Are Doing to Limit the Impact of Online Opposition Voices', D+C, 8 October 2019, https://www.dandc.eu/en/article/what-ugandan-authorities-are-doing-limit-impact-online-opposition-voices (last accessed 24 January 2025); J. Parkinson, N. Bariyo and J. Chin, 'Huawei Technicians Helped African Governments Spy on Political Opponents', Wall Street Journal, 15 August 2019, https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017.

[102] W. Kamusiime, 'Police Refutes Claim of Spying on Opposition', Uganda Police Force, 20 2019, August, https://www.upf.go.ug/police-refutes-claim-of-spying-on-opposition/ (last accessed 24 January 2025).

[103] See Neiman, 'Uganda Could Be Adding a New Tool for Repression to Museveni's Kit', supra fn 79.

[104] Section 19(1), Anti-Terrorism Act 2002: 'Subject to this Act, an authorised officer shall have the right to intercept the communications of a person and otherwise conduct surveillance of a person under this Act'.

[105] Section 19(4), ibid.

[106] Section 19(5), ibid.

[107] Sections 2(1)(a)(iii) and (b)(ii), Regulation of Interception of Communications Act 2010.

[108] See Sekyewa, 'What Ugandan Authorities Are Doing to Limit the Impact of Online Opposition Voices', supra fn 101.

[109] Section 8(1), Regulation of Interception of Communications Act, 2010.

[110] In 2011, the Ugandan Parliament passed the Computer Misuse Act 'for the safety and security of electronic transactions and information systems' as well as 'to prevent unlawful access, abuse or misuse of information systems including computers'.

[111] See, for instance, Section 25, Computer Misuse Act 2011, according to which an 'offensive communication' refers to any repeated electronic interaction which 'attempts to disturb the peace, quiet or right of privacy of any person with no purpose of legitimate communication whether or not a conversation ensues'. Likewise, Section 24 defines 'cyber harassment' as 'the use of a computer for ... making any request, suggestion or proposal which is obscene, lewd, lascivious or indecent; threatening to inflict injury or physical harm to the person or property of any person'.

[112] Also mentioned in Sections 11(2)(e)(v) and 17(3)(c)(v).

[113] Section 3(2), Data Protection and Privacy Act 2019. Subsequently, in 2020, the Personal Data Protection Office was established within the NITA-U as the oversight body for data protection as required under Section 3, 'Establishment of Personal Data Protection Office', Data Protection and Privacy Regulations 2021.

[114] Unwanted Witness, Data Protection and Privacy Act, 2019, Section 5.0, 'Key Gaps in the Law': 'Failure to provide power for the Authority to impose penalties', p 9. https://www.unwantedwitness.org/download/uploads/Data-Protection-and-Privacy-Law-Analysis.pdf (last accessed 24 January 2025). See also Section 33, Data Protection and Privacy Act 2019, 'Compensation for failure to comply with this Act'.

[115] The UCC was established under Section 4 of the Uganda Communications Act 2013. Among the functions of the Commission is 'to monitor, inspect, licence, supervise, control and regulate communications services' (Section 5(1)(b)).

[116] Section 86(1)(a and b), ibid.

[117] See Nitsche, 'Digital Rights', supra fn 81.

[118] Art 27(2), Constitution of the Republic of Uganda 1995 states that '[n]o person shall be subjected to interference with the privacy of that person's home, correspondence, communication or other property'.

[119] For the argument, see Konde, 'No to Big Brother', supra fn 97, 202–205.

[120] Ibid.

[121] See also J. Sherman, 'Russia's Internet Censor is Also a Surveillance Machine', Council on Foreign Relations, 28 September 2022, https://www.cfr.org/blog/russias-internet-censor-also-surveillance-machine (last accessed 24 January 2025); 'In Russia, 'More than 60 Regions Have Implemented Facial Recognition Systems', TASS, 24 October 2023, Available https://tass.ru/ekonomika/19096823 (in Russian).

[122] Roskomnadzor is, then, more of a policing agency that not only monitors but also operates in a way that facilitates the persecution of oppositionists, activists and the independent media. See further P. Mozur, A. Satariano, A. Krolik and A. Aufrichtig, '"They Are Watching": Inside Russia's Vast Surveillance State', The New York Times, 22 September 2022, Available https://www.nytimes.com/interactive/2022/09/22/technology/russia-putin-surveillance-spying.html.

[123] DPI, a sophisticated technique for the examination and management of a network's traffic, can be leveraged to eavesdrop on personal communications and facilitate censorship-related activities. See, 'The State Duma has adopted a law on fines for operators that fail to install data traffic retention systems', 23 May, 2023, https://roskomsvoboda.org/en/post/shtrafy-za-ne-sorm/ (in Russian, last accessed

24 January 2024).

[124] Mozur et al, '"They Are Watching"', supra fn 122.

[125] A subsidiary of Citadel, the company MFI Soft is notable for its development of NetBeholder, a powerful surveillance tool that allows for detailed tracking and analysis of telecom subscriber data. This technology is employed to monitor the communications and movements of individuals. See further A. Popova, 'Russia Exports Digital Surveillance, Despite Sanctions', Center for European Policy Analysis (CEPA), 26 August 2022, Available https://cepa.org/article/russia-exports-digital-surveillance-despite-sanctions/ (last accessed 24 January 2025).

[126] Finally, with access to the data of subscribers to the telecom network through SORM, NetBeholder can identify the geographic area where a user inside Russia is based, or in the case of a foreigner, their country of residence.

[127] See further A. Krolik, P. Mozur and A. Satariano, 'Cracking Down on Dissent, Russia Seeds a Surveillance Supply Chain', The New York Times, 6 July 2023, https://www.nytimes.com/2023/07/03/technology/russia-ukraine-surveillance-tech.html.

[128] The system is maintained by the Main Radio Frequency Center, an entity overseen by Roskomnadzor. See 'Russian System to Scan Internet for Undesired Content and Dissent', Reuters, 13 February 2023, https://www.reuters.com/world/europe/russian-system-scan-internet-undesired-content-dissent-2023-02-13/.

[129] 'The Oculus Automatic Search System for Prohibited Content Has Been Launched in the Russian Federation', Interfax, 13 February 2023, https://www.interfax.ru/russia/885877 (last accessed 24 January 2025). See further Mozur et al, '"They Are Watching"', supra fn 122.

[130] See further C. Castro, 'Russia Launches AI Monitoring Tool Oculus to Beef Up Its Censorship Machine', TechRadar, 17 February 2023, https://www.techradar.com/news/russia-launches-ai-monitoring-tool-oculus-to-beef-up-its-censorship-machine (last accessed 24 January 2025).

[131] See 'Telecommunications Breakdown: How Russian Telco Infrastructure was Exposed', UpGuard, 18 September 2019, https://www.upguard.com/breaches/mts-nokia-telecom-inventory-data-exposure (last accessed 24 January 2025). See also Krolik et al, 'Cracking Down on Dissent' supra fn 127; Z. Whittaker, 'Documents Reveal How Russia Taps Phone Companies for Surveillance, TechCrunch, 18 September 2019, https://techcrunch.com/2019/09/18/russia-sorm-nokia-surveillance/.

[132] Moscow's facial recognition system is powered by software utilizing algorithms developed by one Belarusian company and three Russian firms. See further A. Semivolos, 'The Advent of Facial Recognition and the Erosion of the Rule of Law in Moscow Smart City', 29 Cardozo Journal of Equal Rights & Social Justice (2022); S. Ross, D. Serebrennikov, E. Minaeva and V. Netyaev, 'Surveillance Technologies in Autocratic Regimes: The Moscow AI Experiment and its Implications for Crime Control and Police Effectiveness', April 2024, http://dx.doi.org/10.2139/ssrn.4789135.

[133] L. Masri, 'Facial Recognition is Helping Putin Curb Dissent With the Aid of U.S. Tech', Reuters, 28 March 2023, https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-detentions/.

[134] 'Facial Recognition System at the 2018 World Cup Helped Detain More Than 180 People', Vedomosti, 26 July 2018, https://www.vedomosti.ru/politics/news/2018/07/26/776624-sistema-raspoznavaniya-na-chm-2018 (in Russian).

[135] R. Dixon, 'Russia's Surveillance State Still Doesn't Match China. But Putin is Racing to Catch Up', The Washington Post, 17 April 2021, https://www.washingtonpost.com/world/europe/russia-facial-recognition-surveillance-navalny/2021/04/16/4b97dc80-8c0a-11eb-a33e-da28941cb9ac_story.html.

[136] Masri, 'Facial Recognition is Helping Putin Curb Dissent With the Aid of U.S. Tech', supra fn 133. See further Amnesty International, 'Russia: Police Target Peaceful Protesters Identified Using Facial Recognition Technology, 27 April 2021, https://www.amnesty.org/en/latest/news/2021/04/russia-police-target-peaceful-protesters-identified-using-facial-recognition-technology-2/ (last accessed 24 January 2025). See also, for reference, L. F. M. Ramos, 'Evaluating Privacy During the COVID-19 Public Health Emergency: The Case of Facial Recognition Technologies', in Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance (ICEGOV '20), Association for Computing Machinery, October 2020, https://doi.org/10.1145/3428502.3428526.

[137] 'Moscow Metro Introduces "World's First" Pay-by-Face System', The Moscow Times, 15 October 2021, https://www.themoscowtimes.com/2021/10/15/moscow-metro-introduces-worlds-first-pay-by-face-system-a75300; I. C. Cambell, 'Moscow Adds Facial Recognition Payment System to More Than 240 Metro Stations', The Verge, 15 October 2021, https://www.theverge.com/2021/10/15/22728667/russia-face-pay-system-moscow-metro-privacy.

[138] Masri, 'Facial Recognition is Helping Putin Curb Dissent With the Aid of U.S. Tech', supra fn 133.

[139] See further: Introducing criminal liability for public dissemination of deliberately misleading information under the guise of credible reports on the use of Russia's Armed Forces - On Amendments to the Criminal Code of the Russian Federation and Articles 31 and 151 of the Criminal Procedure Code of the Russian Federation, 4 March 2022. Available at: http://en.kremlin.ru/events/president/news/67908

[140] N. McIntyre, L. Kijewski, H. Munzinger, C. Huppertz and L. Kotkamp, 'Paid Pennies to Train Tools of Repression: The Humans Behind Moscow's State Surveillance', The Bureau of Investigative Journalism, 27 March 2024, https://www.thebureauinvestigates.com/stories/2024-03-27/paid-pennies-to-train-tools-of-repression-the-humans-behind-moscows-state-surveillance/ (last accessed 24 January 2025).

[141] T. Evdokimova, 'Russia Wants Citizens to Like, Comment, Subscribe for More Surveillance', Slate, 14 September 2022, https://slate.com/technology/2022/09/russia-domestic-surveillance.html.

[142] P. Dietrich, The Key Player in Russia's Cybersphere: What the West Needs to Know about VK Company, German Council on Foreign Relations, DGAP Analysis No. 4, September 2023, https://dgap.org/system/files/article_pdfs/DGAP%20Analysis%20No.%204_September_20_2023_20pp.pdf (last accessed 24 January 2025).

[143] See further G. Ianni, F. Capineri, P. Vanni, G. Forcina, F. Manca, G. Marinelli, C. Molinari, G. Mucciaccio and M. Vidoni, '5G Technology: New Challenges for Law Enforcement Agencies to Face', 22 European Law Enforcement Research Bulletin (2022). See also J. S. Hollywood, D. Woods, A. Lauland, S. E. Goodison, T. J. Wilson and B. A. Jackson, Using Future Broadband Communications Technologies to Strengthen Law Enforcement, RAND Corporation, 2016,

https://www.rand.org/content/dam/rand/pubs/research_reports/RR1400/RR1462/RAND_RR1462.pdf (last accessed 24 January 2025); C. Chen, G. Zhou, and C. Chen, 'Research on Intelligent Mobile Police Application Based on 5G Technology', in 2022 IEEE International Conference on Electrical Engineering, Big Data and Algorithms (EEBDA), IEEE, 2022.

[144] See, for example, R. Kitchin, 'The Real-Time City? Big Data and Smart Urbanism', 79 GeoJournal (2014); Z Allam and Z. A. Dhunny, 'On Big Data, Artificial Intelligence and Smart Cities', 89 Cities (2019); J-P. Onnela, S. Arbesman, M. C. González, A-L. Barabási and N. A. Christakis, 'Geographic Constraints on Social Network Groups' 6 PLoS ONE 4 (2011).

[145] For precedents established in respect of earlier forms of mass surveillance at the European Court of Human Rights, see, for example, ECtHR, Rotaru v Romania, Judgment, App no 28341/95, 4 May 2000; ECtHR, Weber and Saravia v Germany, Admissibility Decision, App no 54934/00, 29 June 2006; ECtHR, Liberty and Others v United Kingdom, Judgment, App no 58243/00, 1 July 2008.

[146] Land and Aronson, 'Human Rights and Technology', supra fn 5, 226.

[147] See B. E. Harcourt, Against Prediction: Sentencing, Policing, and Punishing in an Actuarial Age, Chicago Public Law and Legal Theory Working Paper No 94, 2005, p 36,

https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1021&context=public_law_and_legal_theory (last accessed 24 January 2025).

[148] See further UN Human Rights Committee (HR Committee), General Comment No. 37 (2020) on the Right of Peaceful Assembly (Article 21), UN doc CCPR/C/GC/37, 17 September 2020, §2.

[149] N. Jiang, J. Wen, J. Li, X. Liu and D. Jin, 'GATrust: A Multi-Aspect Graph Attention Network Model for Trust Assessment in OSNs', 35 IEEE Transactions on Knowledge

and Data Engineering 6 (2023). See further K. J. Strandburg, 'Surveillance of Emergent Associations: Freedom of Association in a Network Society', in A. Acquisti, S. Gritzalis, C. Lambrinoudakis and S. di Vimercati (eds), Digital Privacy: Theory, Technology, and Practices, Auerbach Publications, 2007, p 437; See also Impact of New Technologies, supra fn 10.

[150] K. J. Strandburg, 'Surveillance of Emergent Associations', supra fn 148, p 438.

[151] See Appendix to the Recommendation Rec(2001)10 of the Committee of Ministers to Member States on the European Code of Police Ethics, 19 September 2001.

[152] This is done based on extrapolating trends and patterns from assembled data retained from previous assemblies using crowd management software. See further C. McCue, Data Mining and Predictive Analysis: Intelligence Gathering and Crime Analysis Elsevier, 2007; T. Scassa, 'Law Enforcement in the Age of Big Data and Surveillance Intermediaries: Transparency Challenges', 14 SCRIPTed (2017); R. Montasari, 'The Potential Impacts of the National Security Uses of Big Data Predictive Analytics on Human Rights', in R. Montasari,Countering Cyberterrorism: The Confluence of Artificial Intelligence, Cyber Forensics and Digital Policing in US and UK National Cybersecurity, Springer, 2023.

[153] See , Arts 2(1) and 26, UN International Covenant on Civil and Political Rights (ICCPR).

[154] V. L. Raposo, 'When Facial Recognition Does Not "Recognise": Erroneous Identifications and Resulting Liabilities', 39 AI & SOCIETY 4 (2024).

[155] J. Lerman, 'Big Data and its Exclusions', 66 Stanford Law Review Online (2013).

[156] See K. Crawford, 'Think Again: Big Data', Foreign Policy, 10 May 2013, https://foreignpolicy.com/2013/05/10/think-again-big-data/.

[157] See further UN HR Committee, General Comment No. 37, supra fn 147, §61. See also Joint Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association and the Special Rapporteur on extrajudicial, summary or arbitrary executions on the Proper Management of Assemblies, UN doc A/HRC/31/66, 4 February 2016, §73. See also HR Committee, Concluding Observations on the Fourth Periodic Report of the Republic of Korea, UN doc CCPR/C/KOR/CO/4, 3 December 2015, §§42–43.

[158] UN HR Committee, CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988, §7. See also UN HR Committee, General Comment No. 37, supra fn 147, §§41–47 and Article 22(2), ICCPR.

[159] Where authorities place a constraint on citizens' enjoyment of a particular right, such a limitation must be sufficiently narrow and, crucially, prove to be a necessity in protecting the permissible purposes of applying the restriction. The principle of proportionality maintains that the law in place effectively enables the least intrusive instrument amongst those that might achieve the desired result. See General Comments Adopted by the Human Rights Committee Under Article 40, Paragraph 4, of the International Covenant on Civil and Political Rights, UN doc CCPR/C/21/Rev.1/Add.9, 1 November 1999, §§11–16.

[160] For further guidance see UNGA Res 68/1670, 21 January 2014, §23.

[161] UN HR Committee, General Comment No. 37, supra fn 147, §10

[162] UN HR Committee, General Comment No. 16, supra fn 157, §10.

THE GENEVA ACADEMY

The Geneva Academy provides post-graduate education, conducts academic legal research and policy studies, and organizes training courses and expert meetings. We concentrate on branches of international law that relate to situations of armed conflict, protracted violence, and protection of human rights.

DISCLAIMER

The Geneva Academy of International Humanitarian Law and Human Rights is an independent academic centre. Our publications seek to provide insights, analysis and recommendations, based on open and primary sources, to policymakers, researchers, media, the private sector and the interested public. The designations and presentation of materials used, including their respective citations, do not imply the expression of any opinion on the part of the Geneva Academy concerning the legal status of any country, territory, or area or of its authorities, or concerning the delimitation of its boundaries. The views expressed in this publication represent those of the authors and not necessarily those of the Geneva Academy, its donors, parent institutions, the board or those who have provided input or participated in peer review. The Geneva Academy welcomes the consideration of a wide range of perspectives in pursuing a well-informed debate on critical policies, issues and developments in international human rights and humanitarian law.

**The Geneva Academy
of International Humanitarian Law
and Human Rights**

Villa Moynier
Rue de Lausanne 120B
CP 1063 - 1211 Geneva 1 - Switzerland
Phone: +41 (22) 908 44 83
Email: info@geneva-academy.ch
www.geneva-academy.ch