**Watchers in the Dark: an overview of State security policies in the age of AI**

**Iacopo Brini**

Law School, Università Commerciale L. Bocconi, Milan, Italy

E-mail: iacopo.brini@studbocconi.it

Published: 27th of January, 2025

**Abstract**

The rise of new and powerful Artificial Intelligence technologies is beginning to present, as their development seems to become ever more exponential, extremely urgent questions on worldwide governmental reliance on their use, and whether something should (or indeed can) be done to limit their prevalence.

Through a panoramic view on the general structure of security frameworks, this paper will analyse what kinds of technologies have been implemented by different states, with a focus on the People’s Republic of China and the Russian Federation and their embracing of new developments in surveillance, as well as a brief contrast with the United States, to try and paint the current state of affairs in security policy, and what may lie ahead in the uncertain seas of the digital age.

The paper will review the national security frameworks of China, Russia and the United States, emphasizing how each state has shown varying degrees of enthusiasm towards AI integration, and will then suggest that specific, rule of law-oriented regulation seems unlikely in the face of a State’s interest to better its surveillance capabilities. Limitations are instead likely to come as results of bargaining processes between world powers.

Keywords: AI, State Security, Surveillance

1. Introduction

National Security is, at its heart, the science and praxis of handling threats to the State. A menace of this sort is essentially any sort of force that positions itself against the interests and priorities of the State, whether through military means or with any other instrument that is suitable to harm the State’s three cornerstones of territory, sovereignty and people.

These forces working to the State’s detriment may come from abroad, from foreign players and known or unknown enemies, but the trickiest and often the most subtle and vicious threats come from within the confines of the State itself; sometimes, perhaps, from the citizens themselves.

The duty of a national security apparatus is thus of a far more preventative nature than it is reactive. A State has its army to react to aggressions, and its police forces and criminal justice system to enforce its laws and punish (and, hopefully, reform) its citizens. The State security apparatus exists to act before these instruments become necessary, to act upon threats far before they materialise and ideally before they even gain the potential to do so.

The obvious primary instrument for this preventative purpose is one that allows the security forces to have a clear, dynamic picture of whatever is currently happening inside and outside of the State’s borders: surveillance. While a general definition would sound something like the “*collection, recording, and classification of information about people, processes, and institutions*”,[[1]](#footnote-1) the aspect that has truly come to the fore in the Digital Age is the interplay between traditional systems of surveillance[[2]](#footnote-2) and the plethora of technological developments in the last two decades. The possibilities of integrating novel technologies, such as Artificial Intelligence, to streamline, improve, expand or even run a State’s security apparatus are endless, and endlessly growing, endowing governments with more and more powers they are sure to enjoy and which they are unlikely to shed voluntarily. The new and rising question thus becomes just how much governments are reliant on the use of AI-powered intelligence gathering and surveillance, and what avenues of control and regulation, if any, can be undertaken in order to limit its prevalence.

II. *Qui Custodes*? State security frameworks across the world

To better understand this interplay, the first question to be answered is who are the players behind surveillance programs and the main drivers of their integration with ever more sophisticated instruments: in short, who are the custodians of the State, charged with its proactive defence?

In the People’s Republic of China, the security of the communist political regime is entrusted to a specific agency, which acts as an organic constituent of the State Council, the Ministry for State Security (MSS). The MSS functions as China's intelligence, security and secret police agency in one, and “*can be described as an institution similar to the FBI and the Central Intelligence Agency (CIA) combined under one intelligence directorate* […]”.[[3]](#footnote-3)

While most China’s foreign intelligence and surveillance operations remain under the general purview of the MSS, the Ministry of Public Security (MPS) also plays a central role in national security and public safety within, and often without,[[4]](#footnote-4) the State’s borders: together, the MSS and the MPS compose most of the People’s Police, the civilian equivalent to the People’s Armed Police, which instead reports to and is part of the People’s Liberation Army, China’s armed forces. Specifically, while the Ministry of Public Security handles the vast majority of officers under the moniker of the ‘Public Security Police’,[[5]](#footnote-5) the Ministry of State Security runs its own ‘State Security Police’ as the secret police within China itself. This compact, unitary structure of interwoven pieces owing ultimate loyalty to the Party administrators in the State Council makes the Chinese framework uniquely suitable for in-house development of AI technologies, with great potential for speedy and uniform implementation across all forces involved once they are developed.

In the Russian Federation, the main agencies that oversee the State’s security are the Federal Security Bureau (FSB), the Ministry of the Interior (MVD) and the recently created National Guard (more commonly referred to as ‘Rosgvardiya’). Despite being ostensibly separate institutions with a separate focus on internal or external security, the Russian tendency is to treat them as a unitary field, where all players need to be well-versed both in ‘offensive’ intelligence and ‘defensive’ counterintelligence, *domi bellique*.[[6]](#footnote-6)

This philosophy is espoused in particular by an old guard of so-called ‘securocrats’, more or less the same age as President Vladimir Putin and often sharing his intelligence background, who began their careers in the waning days of the Soviet golden age. The FSB is by all means the direct successor of the infamous Soviet KGB, and is thus responsible for counterintelligence and counterterrorism operations both abroad and at home, as well as being tasked with the Russian Federation’s border security. According to the securocrat philosophy, it often operates with broad authority in monitoring internal political opposition and handling internal security threats.

The National Guard, on the other hand, was created in 2016 by concentrating the paramilitary public order force (the ‘interior troops’) previously under the Ministry of the Interior with the formerly separate OMON and SOBR, respectively the riot police and SWAT teams. It answers directly to the President, and is tasked with maintaining public order, quelling domestic unrest, acting as a territorial defence force and thus broadly to ensure regime security from foreign infiltration and homegrown insurrection.[[7]](#footnote-7) The MVD was thus left mostly with the task of handling the police forces of the country and helping with day-to-day crime.

A final mention should be made for the Main Intelligence Directorate (GRU), the military’s SIGINT arm, and the Investigative Committee of the Russian Federation (SKRF), which was spun off in 2011 from the Prosecutor General Office (GPRF) and is responsible for investigating serious crimes and inspecting government agencies, a move widely regarded as a power grab by the old-guard General Alexander Bastrykin.[[8]](#footnote-8)

The securocrat-run system of parallel, personalistic agencies discourages development and uniform implementation and use of new AI applications for surveillance, as every moving part within the system is incentivized to keep its achievements and improvements for itself to ensure pleasing the leader, President Putin, at the expense of both Russia’s enemy and the agency’s own rival securocrats.

As for the United States of America, the answer is rather ample and vague, since the country does not have a unified ‘ministry of the interior’ or a comparable unitary institution tasked with the management of security within the State’s borders, nor does it have a single intelligence agency entrusted with surveillance of foreign enemies.

The U.S.’s history as an initially loose federation meant that “police power”, under the Tenth Amendment, was entrusted solely with the constituent States of the Union. The deceptively-named Department of the Interior’s original field of competence was essentially anything that was not covered by a more specific Department (e.g. War, Justice, Treasury Depts.), but this never included law enforcement, which at the federal level remained a minor affair until the 20th Century, and which until 9/11 and the creation of the Department of Homeland Security, had no real bureau of its own.

As such, it is no surprise that the United States currently presents a set of seventeen federal agencies composing an ‘Intelligence Community’ placed under the leadership of a Director of National Intelligence (DNI) and his Office,[[9]](#footnote-9) for a total of eighteen disparate entities which on their own belong and report to a series of federal Executive Departments. The DNI’s role is to coordinate cooperation between these components, though he does not have executive authority over them, which exacerbates the obvious concerns about cross-agency interference, competence disputes and excessive overlapping of surveillance activities[[10]](#footnote-10)

Within the overlaps and fragmentation of the Intelligence Community, the agencies most involved with surveillance and general preventative internal security are the Federal Bureau of Investigations’ Intelligence Branch and the Department of Homeland Security’s Office of Intelligence and Analysis, whilst the National Security Agency, which conducts counterintelligence operations by focusing on ‘signals intelligence’ (SIGINT),[[11]](#footnote-11) maintains that it relies on the FBI to collect information on foreign intelligence activities within the borders of the United States.

The very different characteristics of all three systems are key factors in understanding policies and decisions on the adoption of AI-powered surveillance systems and similar tools, which a centralised and heavily top-down system like the Chinese one is more likely to seamlessly adopt and integrate, as opposed to the difficulties which the Russian intelligence ecosystem is likely to face; in contrast, the United States’ fragmentary galaxy of intelligence agencies presents a more difficult path to predict, owing to the larger degree of autonomous decision making on matters of AI use and implementation.

**III. *Quomodo custodes custodient?* New and old instruments of surveillance**

The novelties in surveillance mostly regard the meteoric rise of ‘artificial intelligence’, more widely known as AI. The term itself encompasses a number of technological developments, each building on the other and on the less broad concept of AI as “*giving computers behaviours which would be thought intelligent in human beings*” [[12]](#footnote-12) These novelties mostly involve the fields of ‘machine learning’, i.e. computers creating mathematical algorithms based on accumulated data, thus coming to solutions for inputs they were not specifically programmed to resolve, and ‘big data’, i.e. the enormous volumes of information that are stored and fed into machine learning programs to refine the ‘thinking’ of an AI. Digital tools are increasingly being implemented with trained AIs to allow them to perform more complex tasks, requiring decisions and actions in addition to mere observation.[[13]](#footnote-13)

From around 2012 onwards, improvements in raw computing power and the spread of training datasets for machine learning led to a significant improvement in the quantity of big data that can be analysed by systems, allowing them to directly learn from the data how to perform complex tasks.[[14]](#footnote-14) From then on, AI has been on a constant improvement streak that in some cases has been self-sustaining: ever-better AI models have become ever more efficient at sifting through ever-bigger datasets, improving machine learning. An obstacle remains in that data still needs to be ‘labelled’ for AI to have context in its decision-making; this labelling usually involves sensitive, personal data which contextualises broader mundane datasets.[[15]](#footnote-15)

As stated in the foregoing section, State security frameworks of various complexity are all set in place to protect internal order from incoming threats, and the most efficient way to do so is through surveillance. In this current digital age, this set of practices has expanded to include acts “*of real-time and retrospective viewing, processing and cataloguing of online footprint against the will and/or knowledge of the actor(s) to whom such data belong”*[[16]](#footnote-16)

Digital surveillance extends over a number of domains, among which the main ones are data collection, imagery collection, Internet monitoring, geolocation and biometrics: all tools whose main task is to “*intercept external and domestic communication, data transfers and network monitoring*”,[[17]](#footnote-17) in essence pertaining to the more traditional definition of SIGINT practices. Specifically, bulk data interception has radically improved through the Internet’s development and spread throughout the world, whilst Internet Communication Technology (ICT) monitoring is the old surveillance of human activity, including networks of friends, locations visited and other habits, merely transposed onto our modern social media platforms (Twitter, Facebook or Instagram) and communication apps (Whatsapp, Telegram, Messenger or even the old SMS)

More specifically, States and their agencies employ AI (in the broadest sense) within a few relevant groups[[18]](#footnote-18) of surveillance systems: facial recognition devices and their incorporated data gathering and processing capabilities,, smart (i.e. predictive) policing of communities and individuals, as well as ‘internet of things’ networks which avail the aforementioned with even more reach into mundane household appliances, and general cloud computing which allows for sizeable increments in processing power.[[19]](#footnote-19) This AI-supported surveillance network forms *“part of a suite of digital repression tools—information and communications technologies used to surveil, intimidate, coerce, and harass opponents […] that challenge the State*”: they are thus meant to coadiuvate and reinforce the already existing State security infrastructure, more than any kind of replacement.

As an example of the potential for integration of the “*digital repression suite”* in everyday life, one need not look further than smart cities, which conceptually could be equipped with arrays of tracking sensors transmitting real-time data on all aspects of the city’s operations, from directing emergency vehicles through traffic congestion to monitoring energy overuse and waste management, as well as of course, overseeing public safety. The command centre would gather this information and react immediately to any perceived emergency (or threat); within this, AI is implemented as an early-warning system of sorts, pre-screening the massive amounts of data for anything suspicious. The data is likely to come mainly from facial recognition biometric technologies, which match camera footage with vast databases or aggregate demographic trends, and may already pre-interpret general crowd movements and opinions in the same way. The ‘smart police’ will then have clearer records and patterns on which to base predictions provided by algorithms, and act consequently.[[20]](#footnote-20) It should be no wonder that the People’s Republic of China is the world's foremost leader in smart city development, with the National New-Type Urbanization Plan for 2014-2020 explicitly including smart city development, with a focus on information network and broadband expansion, as well as the digitization of planning management and what it called “*sophisticated social governance*”.[[21]](#footnote-21)

**IV. China and Russia: affinities and divergences under an ‘authoritarian’ approach**

China and Russia can be, and often are, described as illiberal regimes. The aforementioned structure of the security apparatuses of both countries shows that, whilst having some differences in how security is handled, both states broadly adhere to the principle that security necessities trump the rule of law. Whilst Russia however follows the unitary securocrat philosophy which sees any foreign threat as a domestic issue and *vice versa*, China espouses the concept of ‘social supervision’, i.e. mobilising the whole of society by turning citizens into watchers and monitors, reporting suspicious activity in the digital field, whilst being watched and monitored themselves by the State entities.[[22]](#footnote-22)

Most importantly, though, the People’s Republic of China’s authoritarian approach to the new technologies in surveillance is rather positive and welcoming: the upsides to implementing these upgrades into the current state security structures are apparent and manifold for the ruling CCP, starting with AI-powered selective restriction of the free flow of information on the Internet, with an ever-more “*selective censorship of specific topics, and selective targeting of specific behaviours*”[[23]](#footnote-23) which in China is currently embodied in what is called the ‘Great Firewall’.

The possibility of predictive policing of dissent by AI-extrapolated trends in individual or group bulk data accumulated by conventional means is an enticing means to reduce the economic and social burden of the repressive State security apparatuses. These AI implements will be made accurate and precise thanks to the unrestricted use of ‘ground truth’ data from personal data such as tax returns, medical records, criminal records, police records, sexual health clinics, bank statements, genetic data, physical monitoring (e.g., location, biometrics, CCTV face monitoring) to ‘label’ the bulk data accumulated through surveillance.[[24]](#footnote-24) In the People’s Republic of China, the Ministry of State Security operates under the National Security Law and Counterespionage Law, which already authorize broad surveillance and information gathering and stockpiling under the guise of counter-espionage activities. The Counterespionage Law in particular was amended in 2023 to extend to information on “*national* *security and interests*” the same protection granted to State secrets.[[25]](#footnote-25)

Additionally, the National Intelligence Law of 2017 empowered both the MSS and the Ministry of Public Security’s Internal Security Bureau with expansive authority to collect any and all digital citizen and company data at will, without any warrant.[[26]](#footnote-26) owing to the secrecy of Court proceedings in China, especially over State matters, there is little to no accessible caselaw over the implementation of the Security, Intelligence or Counterespionage Laws, though some examples of people being brought up on “espionage charges”[[27]](#footnote-27) most likely refer to one or more components of the trifecta.

The only oversight over surveillance operations remains thus solely of a centralised political nature, and integration of AI technology into this system can be found in the ‘Next Generation Artificial Intelligence Development Plan’ of July 2017. The plan laid out the infamous ‘Social Credit’ system, which among other implications, empowers State agencies to monitor and rate individual’s behaviour through big-data collection and analysis. Such efforts are of course spurred and enabled by the aforementioned developments in facial recognition and data accumulation, since the ultimate aim of the program is “*a broader political control process known as ‘social management’*”.[[28]](#footnote-28)

While the topic of social management could warrant, and indeed it has, its own series of papers and reviews, a broad summary could frame it as the pursuit of a “holistic” or “comprehensive” State security,[[29]](#footnote-29) the buzzword slogan for an organised micro- and macro-management system of Party leadership control over the CCP and the general citizenry, to optimize interactions “*vertically (within the Party), horizontally (between agencies), and holistically, between the Party and society*”.[[30]](#footnote-30)The potential for automation or heavy integration, through AI, of such a system is lost on no one in China.[[31]](#footnote-31)

The case of the Russian State is indeed both similar and different. The Russian Federation is still an illiberal regime, but it features less oppressive characteristics to a Western observer’s eye; the populace is generally less constricted in its daily life, and the perceived need by the Kremlin’s ruling clique of securocrats and technocrats (the younger élites, who are less defence-oriented than their older peers and more open to reforming current power structures) is that the population ought to be kept reasonably happy and unaware, so to speak, of the boot that quashes them. As such, the authoritarian approach of the Russian regime in terms of surveillance and manipulation of online discourse does not pass through “*systemic technical censorship*”[[32]](#footnote-32) such as the ‘Great Firewall’ and instead relies on a mix of “le*ss overt means, more plausibly deniable, legalistic, and often nontechnical mechanisms to manipulate online information flows, narratives, and framings to affect and shape public opinion without resort to universal censorship*”.[[33]](#footnote-33)

Specifically, the main instruments reside in a slew of legislation which began in 2012 with the establishment of a blacklist of censored sites and grew rapidly to include the 2013 anti-piracy provisions[[34]](#footnote-34) (which burdened Internet providers with liability for violations) and anti-LGBT propaganda law[[35]](#footnote-35) (which extended the 2012 blacklist to almost anything having to do with sexual orientation), as well as the 2014 “Law on Pre-Trial Blocking of Websites” (which provided for immediate blocking of sites that are deemed to contain ‘incitement to extremism or riots’).[[36]](#footnote-36) A suicide prevention site, Pobedish.ru,[[37]](#footnote-37) was among the domains affected by the blacklisting provisions, as well as Wikipedia.ru, whose editors had to conform and reword the Russian-language entry for “cannabis” in order to have the page unblocked.[[38]](#footnote-38)

The ‘System Operational-Investigatory Measure’ (SORM) in particular has long been the legal basis of lawful surveillance of digital communications and telecommunication networks.[[39]](#footnote-39) It lays out a set of requirements that define the legal limits of surveillance, namely allowing tracking and storage of metadata without a warrant, but requiring it for access to the data itself. A SORM law has been in force in Russia since 1995, first providing for obligatory instalment of Federal Security Bureau hardware to all telecom operators, then extended to Internet Service Providers’ servers in 1998 and finally with the current SORM-3[[40]](#footnote-40) layout developed in 2014 to include all social media platforms.[[41]](#footnote-41) Further enabling came with the ‘Anti-Encryption Law’ of 2016, which required all encrypted services to provide the FSB with encryption keys or other means of decoding their data.

These laws are not enforced so thoroughly or with the same zeal as, for example, the Chinese would; they instead serve more to create a “*chilling effect both for content producers and intermediaries as well as providing legal grounds for subsequent blockings or prosecutions*”.[[42]](#footnote-42) This system presents a “*plausible, lower-tech alternative to the tech-heavy Chinese approach*”, which replaces the massive filtering devices of the MSS and the MPS with intimidation, self-censorship for fear of reprisal, complex laws subject to arbitrary application and general information manipulation through AI-supported government propaganda.[[43]](#footnote-43) Replacing filtering with oversight, the Russian digital authoritarianism model still necessitates communications to be pervasively collected, with little to no limit to what law enforcement can do once a SORM probe allows them access.

Owing to this, the Russian approach to AI-implementation is ultimately less focused on developing new and innovative tools for active control, looking instead to utilise AI to better surveil the relatively free-flowing Internet through SORM-compliant devices. Russian intelligence, however, is still a child of the securocrat approach to State security, and is thus characterized by a proactive and offensive posture that sees attack as the best form of defence; so-called Russian ‘trolls’, bot farms and a series of other tools for disinformation and hacking campaigns, which are set to become AI-managed or even AI-run,[[44]](#footnote-44) are all already employed abroad by the Russian Federation’s security agencies against its geopolitical enemies, with more abandon than at home, where a lighter approach is employed and the need for modernisation[[45]](#footnote-45) and constant updating of technological instruments of surveillance is perhaps not so heartily felt.

V. The United States: hypocrisy and deceit in the struggle for privacy

In the face of such potent and widespread integration of digital and AI surveillance technologies by its main geopolitical rivals, the US has found itself at some disadvantage: it has strived to close the gap with its competitors on the global stage while simultaneously needing to balance a set of liberal, democratic principles enshrined at its cultural and legal core, acknowledging the need for espionage abroad and surveillance for counterterrorism domestically, but having to contend with existing checks and balances that at least attempt to constrain the State’s domestic security apparatus. Faced with this struggle and almost impossible balancing act, the United States Intelligence community has often faltered to the side of convenience, rather than taking the more principled high road.[[46]](#footnote-46)

Ever since Justice Brandeis’s dissent[[47]](#footnote-47) in *Olmstead v. United States*, Fourth Amendment jurisprudence has been thoroughly sceptical of surveillance operations, though the exception of ‘national security’ has always proved a potent enemy.[[48]](#footnote-48) In 1967, Katz v. United States established the legal precedent that enforcement agencies were mandated to procure a warrant before intercepting personal communications.[[49]](#footnote-49) However, this did not stop projects such as MINARET and SHAMROCK, both US Government exercises spanning from 1967 to 1978, which that intercepted and collected exorbitant numbers of electronic communications of US citizens in a *“coordinated FBI-CIA, and DoD effort to serve as domestic counterespionage against the USSR"*.[[50]](#footnote-50) The Federal Bureau of Investigations simultaneously ran the COINTELPRO initiative, amassing over 500,000 dossiers on American citizens, while the Central Intelligence Agency oversaw Operation CHAOS and built a database that tracked 300,000 people. These infamous examples, combined with the more recent and well known NSA wiretapping scandals, provide concrete evidence of the willingness of U.S. intelligence agencies to disregard, evade or otherwise bend existing caselaw and statutes in the pursuit of a higher perceived need, that of safeguarding the State at all costs.

Currently, the Federal electronic surveillance statutes[[51]](#footnote-51) are commonly referred to collectively as "Title III" and present a series of restrictions[[52]](#footnote-52) on the use of most electronic surveillance devices and techniques, including the requirement that a high-level Department official specifically approve the use of many of these types of electronic surveillance prior to an Assistant United States Attorney obtaining a court order authorizing interception. Chapter 7 in particular contains the specific mechanisms, including applicable approval requirements, for the use of wiretaps, "bugs" (oral interception devices), roving taps, video surveillance, and the consensual monitoring of wire or oral communications, as well as emergency interception procedures and restrictions on the disclosure and evidentiary use of information obtained through electronic surveillance.

However, perhaps providing the best evidence of the power of the “national security” exception over the general tendency of American privacy law, interceptions conducted pursuant to the Foreign Intelligence Surveillance Act of 1978[[53]](#footnote-53) were specifically excluded from the coverage of Title III.[[54]](#footnote-54)

The Foreign Intelligence Surveillance Act of 1978[[55]](#footnote-55) in fact established separate procedures for the surveillance and collection of foreign intelligence on American soil; its foremost requirement is for federal law enforcement and intelligence agencies to obtain an authorization to proceed with surveillance operations from a Foreign Intelligence Surveillance Court (FISC), which operates inaudita altera parte and whose proceedings are held in secret. The FISC was immediately subjected to heavy criticism and decried as a rubber-stamp for its characteristics, and the fact that denials of a warrant are subject to review from a Foreign Intelligence Surveillance Court of Review (FISCR), essentially making it impossible for a surveillance warrant to be denied.

Additionally, in the aftermath of 9/11, surveillance practices like bulk metadata collection, biomedical surveillance and network interception were essentially liberalised and encouraged with a sweeping series of legislation, most notably within Title II of the Patriot Act,[[56]](#footnote-56) aptly named ‘Enhanced Surveillance Procedures’; among other provisions, it removed distinctions between surveillance in criminal investigations and surveillance for the purposes of gathering foreign intelligence, and authorised[[57]](#footnote-57) the use of a type of administrative subpoena known as ‘National Security Letter’ (NSL), which authorised the FBI and other domestic agencies to forcibly gather information for national security purposes, while also adding a non-disclosure obligation on the disclosing party, without any prior judicial review.

Infamously, following the legal erasure of surveillance safeguards in 2001 the National Security Agency’s Terrorist Surveillance Program was authorised to collect and store US citizens’ phone calls, emails and other digital activities, without a FISA warrant and within the territory of the United States;[[58]](#footnote-58) under mounting public pressure the practice waned after 2007, when the NSA started seeking FISA warrants again, and it came to the fore again after the 2013 Snowden leaks.

Given this tortuous and narrow path between the requirements of the Fourth Amendment and the historical practice of the State security apparatus within the United States, it is no wonder that the reception to implementing new technologies has been rather more lukewarm, at least in public, than it has been with its direct rivals. The Intelligence Community itself, however, has steadied its course and weathered most of the storm of the last decades of opposition to surveillance with its powers intact: the Freedom Act of 2015[[59]](#footnote-59) reinstated most of the Patriot Act’s provisions, though with some more safeguards and increased FISA oversight and involvement.

Progressive technological development and Artificial Intelligence implementation is thus still happening, though mostly under wraps and without much fanfare, owing to the need of preserving a façade of rule-of-law and Fourth Amendment preservation whilst not falling behind with rivals less concerned with keeping up appearances: thus, the Federal Bureau of Investigations was reported[[60]](#footnote-60) to be using AI technologies through a system it calls the “Complaint Lead Value Probability”, which serves to “*prioritize tips by conducting algorithm scores and triaging*”, i.e. to preliminarily evaluate which complaints should be addressed further. The Department of Homeland Security instead unveiled an agency-wide roadmap called ‘Innovation, Research and Development (IRD) Strategic Plan’ for pursuing emerging technologies, including Advanced Sensing, AI and Autonomous Systems, Biotechnology, Cybersecurity, Data Integration, Analytics, Modelling and Simulation and Digital Identity and Trust.[[61]](#footnote-61) Finally, and perhaps most worryingly, the private company SpaceX has been developing a network of hundreds of advanced, top-of-the-line spy satellites for the National Reconnaissance Office (NRO), raising additional questions regarding the involvement of private contractors in such delicate surveillance matters; this issue seems poised to be uniquely American, given the nature of Russian and especially Chines companies as formal subjects of private law, but in actuality enduring a level of State oversight or even direct control that is alien to U.S. companies.[[62]](#footnote-62)

VI. Conclusions

State surveillance is not inherently unlawful.[[63]](#footnote-63) There is legitimate justification in resorting to surveillance, but all legitimacy truly rests in the characteristics of the State that performs it, and in the predisposition and mentality of its agents in the various State security frameworks: a democracy is bound to at least attempt to use it under the tenets and constraints of the rule of law, while an authoritarian partocracy cannot but employ it to serve its own needs, and perhaps reap more benefits from it because of its lack of restraint. Indeed, for example, China does not have an advantage in terms of number of electronic device users, given the global user bases for the U.S.’s tech giants like Facebook or Google, but it does have an advantage in terms of integration and combination of data both across platforms and with personal, private ‘ground truth’ data for AI training, something the US simply cannot replicate with the same level of efficacy.

Unfortunately, little can be done to “fix” this disadvantage that modern digital democracies find themselves without utterly betraying the fundamental principles these States stand for. The United States’ history of Fourth Amendment violations in pursuit of State security perhaps best exemplifies how intelligence agencies will have little to no qualms in resolving this conundrum on the side of increasing surveillance, resorting to any new technology and improvement with all possible speed: to a State agent, their utility far outweighs any concern over preserving rights, which could not exist if the State itself is at risk. In this, one could be tempted to draw some parallels with the securocrat mindset of the Russian “old guard”, which focuses on safeguarding Russia from external or internal threats at all costs, often resorting to less subtle means of enforcement that guarantee results at the expense of public image.

AI-integration cannot, however, be allowed to run rampant. As with its development in other fields, Artificial Intelligence in surveillance is uniquely poised to encourage recourse to this instrument, which will become ever-easier, ever-faster and ever more precise.

Additionally, AI development is a self-monopolising field: the more a purveyor of this technology improves it, the more the technology itself will help in its own improvement, expansion and increase of capabilities. A private actor which enters this cycle will see its bargaining power against States multiply tenfold, which is an outcome of unimaginable damaging potential, but a State that runs its own AI development will simply have little to no checks over its direction and pace, and will encourage itself to develop more, which will lead to even more usage and even more surveillance.

As such, there is a distinct lack of incentives for States with a stake in this AI ‘arms race’ to limit themselves and their development capability, lest they find themselves at a disadvantage, and there is a plethora of motivating factors for all players involved to engage in relentless competition.

The European attempt at legislation and regulation, the recently approved AI Act of 2024,[[64]](#footnote-64) should be seen more as a sign that the European Union and its constituent states are not real parties to the competition over integrating AI in the security and surveillance fields, owing to a combination of industrial weakness, technological reliance on US firms, and a lack of political willingness to craft a joint strategy over the matter. The ‘regulatory approach’, as it has been often named, cannot be reproduced anywhere else: surely not in the People’s Republic of China, which stands to gain the most from these new technologies and has set them as cornerstones of its five-year plans towards economic development and control of the population, and neither in the Russian Federation, whose employment of AI for its online disinformation and manipulation campaigns has proven vastly successful.

If the United States aims to reduce the threat of Artificial Intelligence in the surveillance field, it will have to contend with three main obstacles: the first, as mentioned above, is that its competitors are not willing to slow down their operations, and their objective is precisely to put the U.S. and its allies on the back foot of the global surveillance field; the second is that owing to the lack of incentives, the only approach that can produce any sort of result is enticing its geopolitical enemies through concession and compromise in other fields, where the United States may still hold an edge; the third is the strong internal opposition it is certain to face.

As such, some prudent, well-formulated regulation will certainly need to exist to curb the worst cases of excess and abuse, but any outright bans or forcible restrictions in the implementation of AI and similar techniques into democratic security systems would certainly result in these systems availing themselves clandestinely, and still suffering a competitive disadvantage against models of outright control such as the Chinese one, and hybrid authoritarianism like the one currently holding sway in Russia.

To address the first and second obstacles, the U.S. might have to rely on concessions in trade or, possibly, in geopolitical influence, allowing its opponents some added liberties when dealing, e.g., with proxy conflicts such as the Ukrainian War and the Syrian Civil War. This, however, poses a secondary question: is such a sacrificial move even worth trying, in order to limit the spread of AI and digital surveillance? The answer the Intelligence Community of the U.S. will give is most certainly a resounding ‘no’, which will have dangerous implications when taking a look at the history of covert, unauthorised, grey-zone operations its component agencies have shown themselves to be willing to engage in over the last century, despite all legal infrastructure currently standing guard over the right to Privacy.

In the end, we already know the answer to the age-old question, *quis custodiet ipsos custodes?* The most sincere response is that our custodians ‘watch themselves’, so to speak, and thus the answer cannot truly be found in attempting to control them; the aim should instead be to create the necessary conditions, in the global exchequer, for it to be convenient and hopefully necessary for our watchers to quell their paranoia and begin to limit themselves.

Bibliography

Books and Journal Articles:

* Bendett, Samuel. “The Development of Artificial Intelligence in Russia.” In *Artificial Intelligence, China, Russia, and the Global Order*, edited by Nicholas D. Wright, Air University Press, 2019.
* Brayne, Sarah. “Big Data Surveillance: The Case of Policing.” *American Sociological Review* 82, no. 5 (2017): 977–1008.
* Corff, Oliver. “‘Rich Country, Strong Army’: China’s Comprehensive National Security.” *Federal Academy for Security Policy*, 2018.<http://www.jstor.org/stable/resrep22151>.
* Donohue, Laura K. “Anglo-American Privacy and Surveillance.” *The Journal of Criminal Law and Criminology* 96, no. 3 (2006): 1059–1208.
* Feldstein, Steven. “AI Surveillance Enabling Technologies.” In *The Global Expansion of AI Surveillance,* Carnegie Endowment for International Peace, 2019.

<http://www.jstor.org/stable/resrep20995.6>.

* Feldstein, Steven. “Distinguishing Between Legitimate and Unlawful Surveillance.” In *The Global Expansion of AI Surveillance,* Carnegie Endowment for International Peace, 2019.<http://www.jstor.org/stable/resrep20995.6>.
* Feldstein, Steven. “Types of AI Surveillance.” In *The Global Expansion of AI Surveillance*, Carnegie Endowment for International Peace, 2019.<http://www.jstor.org/stable/resrep20995.6>.
* Galeotti, Mark. “The Law Enforcement Agencies: Russian Domestic Security and International Implications.” *Security Insights,* no. 45 (February 2020).
* Goldberg, Adam, et al. “China Amends the Counter-Espionage Law.” *Pillsbury Law*, May 15, 2023.<https://www.pillsburylaw.com/en/news-and-insights/china-counter-espionage-law.html>.
* Hoffman, Samantha. “Managing the State: Social Credit, Surveillance, and the Chinese Communist Party’s Plan for China.” In *Artificial Intelligence, China, Russia, and the Global Order*, edited by Nicholas D. Wright, Air University Press, 2019.
* Kerr, Jaclyn. “The Russian Model of Digital Control and Its Significance.” In *Artificial Intelligence, China, Russia, and the Global Order*, edited by Nicholas D. Wright, Air University Press, 2019.
* Miglio, Michela. “SpaceX’s Spy Satellites and the Future of Space Warfare.” *Praesidium* 1 (October 2024), p. 33.
* Morgus, Robert. “The Spread of Russia’s Digital Authoritarianism.” In *Artificial Intelligence, China, Russia, and the Global Order*, edited by Nicholas D. Wright, Air University Press, 2019.
* Ünver, H. Akın. “Politics of Digital Surveillance, National Security and Privacy.” *Centre for Economics and Foreign Policy Studies,* 2018.
* Wright, Nicholas D., ed. “Artificial Intelligence and Domestic Political Regimes: Digital Authoritarian, Digital Hybrid, and Digital Democracy.” In *Artificial Intelligence, China, Russia, and the Global Order*. Air University Press, 2019.
* Wright, Nicholas D., ed. “The Technologies: What Specifically Is New?” In *Artificial Intelligence, China, Russia, and the Global Order*. Air University Press, 2019.

Cases and Legal Documents:

* 18 U.S.C. § 2510 et seq.
* 50 U.S.C. § 1801 et seq., 92 Stat. 1783.
* 18 U.S.C. § 2511(2)(a)(ii), (2)(e), and (2)(f).
* Executive Order 12333 of December 4, 1981, “United States Intelligence Activities.” 46 FR 59941, *Code of Federal Regulations*, Title 3 (1981): 200.
* Federal Law No. 187-FZ, *Rossiyskaya Gazeta*, July 2, 2013, No. 187.
* Federal Law No. 135-FZ, *Rossiyskaya Gazeta*, July 2, 2013, No. 6117.
* FISA Act, 50 U.S.C. ch. 36, Pub. L. 95–511, 92 Stat. 1783.
* Ministry of Communications of the Russian Federation, Order n. 83 (16 April 2014).
* *Olmstead v. United States*, 277 U.S. 438 (1928).
* *PATRIOT Act*, Pub. L. 107–56, 115 Stat. 272.
* *Protect America Act of 2007*, Pub. L. 110–55, 121 Stat. 552.
* Regulation (EU) 2024/1689.
* Section 505 of the Act.
* *United States v. Claiborne*, 1:17-cr-00069 (D.D.C.).
* *USA Freedom Act*, Pub. L. 114-23, 129 Stat. 268 (2015).

Web Articles:

* Gallardo, Cristina. “Secret Chinese ‘Police Stations’ to Be Investigated Around Britain.” *Politico*, November 1, 2022.<https://www.politico.eu/article/uk-police-china-london-glasgow-investigating-unacceptable-chinese-police-stations-in-britain/>.
* Heilweil, Rebecca. “The FBI Is Using AI to Mine Threat Tips, but Isn’t Sharing Much Detail.” *Fedscoop*, October 17, 2024.<https://fedscoop.com/fbi-ai-tool-threat-tips>.
* Neely, Jason, and Elaine Hardcastle. “Japan’s Astellas Says Employee Indicted by China’s Prosecutors.” *Reuters*, August 21, 2024.<https://www.reuters.com/business/healthcare-pharmaceuticals/japans-astellas-says-employee-indicted-by-chinas-prosecutors-2024-08-21/>.
* Omidi, Maryam. “Blackout: Why Russian Internet Sites Are Going Dark Over Anti-Piracy Laws.” *New East Digital Archive*, August 1, 2013.<https://www.new-east-archive.org/articles/show/1273/blackout-why-russian-internet-sites-are-going-dark-over-anti-piracy-laws>.
* Soldatov, Andrey. “What Did Russia Block This Autumn?” *Index on Censorship*, November 22, 2013.<https://www.indexoncensorship.org/2013/11/russia-censored-autumn-2013/>.
* The Society for the Study of Artificial Intelligence and Simulation of Behaviour. “What Is Artificial Intelligence.” *AISB Website*.<http://www.aisb.org.uk/public-engagement/what-isai>.
* Yellig, John. “Homeland Security Unveils Emerging Technologies Road Map.” *IoT World* *Today*, June 4, 2024.<https://www.iotworldtoday.com/security/homeland-security-unveils-emerging-technologies-road-map>.

1. ### Brayne, Sarah. “Big Data Surveillance: The Case of Policing” *American Sociological Review* 82, no. 5 (2017): 977–1008.

   [↑](#footnote-ref-1)
2. ### And the regulatory framework they operate under

   [↑](#footnote-ref-2)
3. ### According to a criminal complaint filed in *United States v. Claiborne*, 1:17-cr-00069, (D.D.C.).

   [↑](#footnote-ref-3)
4. ### Gallardo Cristina, ‘Secret Chinese ‘police stations’ to be investigated around Britain‘, November 1, 2022, <https://www.politico.eu/article/uk-police-china-london-glasgow-investigating-unacceptable-chinese-police-stations-in-britain/>

   [↑](#footnote-ref-4)
5. ### Whose 1st Bureau is tasked with maintaining social and political stability and handling threats to ‘national unity’

   [↑](#footnote-ref-5)
6. ### “*In Russia, the foreign and domestic dimensions of security are viewed essentially as two sides of the same coin”*, Galeotti Mark, ‘The Law Enforcement Agencies: Russian Domestic Security and International Implications’, *Security Insights*, No. 45 (February 2020), p.1

   [↑](#footnote-ref-6)
7. ### *“The National Guard has a specific mission over and above simply supporting the regular military in territorial defense, and it has wargamed operations against insurgents backed by foreign special forces”,* Galeotti Mark, ‘The Law Enforcement Agencies: Russian Domestic Security and International Implications’, *Security Insights*, No. 45 (February 2020)

   [↑](#footnote-ref-7)
8. ### Galeotti Mark, ‘The Law Enforcement Agencies: Russian Domestic Security and International Implications’, *Security Insights*, No. 45 (February 2020)

   [↑](#footnote-ref-8)
9. ### Executive Order 12333 of December 4, 1981, ‘United States Intelligence Activities’, 46 FR 59941, *Code of Federal Regulations*, Title 3 (1981), p. 200

   [↑](#footnote-ref-9)
10. ### Not necessarily to the knowledge of the agencies themselves, which might both put a suspect under surveillance without knowing of the other’s activities.

    [↑](#footnote-ref-10)
11. ### I.e. surveillance, as opposed to ‘human intelligence gathering’, or HUMINT, which is more the CIA and DIA’s purview

    [↑](#footnote-ref-11)
12. ### The Society for the Study of Artificial Intelligence and Simulation of Behaviour. What is Artificial Intelligence. AISB Website. http://www.aisb.org.uk/public-engagement/what-isai Accessed 6th november 2024

    [↑](#footnote-ref-12)
13. ### Wright, Nicholas D., ed. “The Technologies: What Specifically Is New?” *Artificial Intelligence, China, Russia, and the Global Order*. Air University Press, 2019, p.3

    [↑](#footnote-ref-13)
14. ### *Ibid.*, p.5

    [↑](#footnote-ref-14)
15. ### *Ibid.,* p.6-7

    [↑](#footnote-ref-15)
16. ### Ünver, H. Akın. “Politics of Digital Surveillance, National Security and Privacy.” Centre for Economics and Foreign Policy Studies, 2018.

    [↑](#footnote-ref-16)
17. ### Ünver, H. Akın. “Politics of Digital Surveillance, National Security and Privacy.” Centre for Economics and Foreign Policy Studies, 2018.

    [↑](#footnote-ref-17)
18. ### Feldstein, Steven. “Types of AI Surveillance.” *The Global Expansion of AI Surveillance*. Carnegie Endowment for International Peace, 2019.

    [↑](#footnote-ref-18)
19. ### *As one expert put it, if video surveillance is the “eyes” then cloud services are the “brains” that “connect cameras and hardware to the cloud computing models via 5G networks.”*, Feldstein, Steven. “AI Surveillance Enabling Technologies.” *The Global Expansion of AI Surveillance*. Carnegie Endowment for International Peace, 2019.

    [↑](#footnote-ref-19)
20. ### Feldstein, Steven. “Types of AI Surveillance.” *The Global Expansion of AI Surveillance*. Carnegie Endowment for International Peace, 2019

    [↑](#footnote-ref-20)
21. ### Richard Hu, Reinventing the Chinese City, Columbia University Press, 2023.

    [↑](#footnote-ref-21)
22. ### Ünver, H. Akın. “Politics of Digital Surveillance, National Security and Privacy.” Centre for Economics and Foreign Policy Studies, 2018.

    [↑](#footnote-ref-22)
23. ### Wright, Nicholas D., ed. “Artificial Intelligence and Domestic Political Regimes: Digital Authoritarian, Digital Hybrid, and Digital Democracy.” *Artificial Intelligence, China, Russia, and the Global Order*. Air University Press, 2019.

    [↑](#footnote-ref-23)
24. ### *Ibid.,* p. 29-31

    [↑](#footnote-ref-24)
25. ### Goldberg, Adam et al., “China Amends the Counter-Espionage Law”, Pillsbury Law, May 15, 2023, https://www.pillsburylaw.com/en/news-and-insights/china-counter-espionage-law.html

    [↑](#footnote-ref-25)
26. ### Ünver, H. Akın. “Politics of Digital Surveillance, National Security and Privacy.” Centre for Economics and Foreign Policy Studies, 2018.

    [↑](#footnote-ref-26)
27. ### Neely, Jason, and Elaine Hardcastle. “Japan’s Astellas Says Employee Indicted by China’s Prosecutors | Reuters.” Reuters, August 21, 2024. https://www.reuters.com/business/healthcare-pharmaceuticals/japans-astellas-says-employee-indicted-by-chinas-prosecutors-2024-08-21/.

    [↑](#footnote-ref-27)
28. ### Hoffman, Samantha. “Managing the State: Social Credit, Surveillance, and the Chinese Communist Party’s Plan for China.” Edited by Nicholas D. Wright. *Artificial Intelligence, China, Russia, and the Global Order*. Air University Press, 2019.

    [↑](#footnote-ref-28)
29. ### Corff, Oliver. “‘Rich Country, Strong Army’: China’s Comprehensive National Security.” Federal Academy for Security Policy, 2018. http://www.jstor.org/stable/resrep22151.

    [↑](#footnote-ref-29)
30. ### Hoffman, Samantha. “Managing the State: Social Credit, Surveillance, and the Chinese Communist Party’s Plan for China.” Edited by Nicholas D. Wright. *Artificial Intelligence, China, Russia, and the Global Order*. Air University Press, 2019, p.49

    [↑](#footnote-ref-30)
31. ### “*In the construction of the social credit system, current research and development is largely focused on areas such as big-data analysis and integration to support the collection of information and ensure its effective use for intelligence.”, Ibid. p.52*

    [↑](#footnote-ref-31)
32. ### *Ibid.* p. 31

    [↑](#footnote-ref-32)
33. ### Kerr, Jaclyn. “The Russian Model of Digital Control and Its Significance.” Edited by Nicholas D. Wright. *Artificial Intelligence, China, Russia, and the Global Order*. Air University Press, 2019.

    [↑](#footnote-ref-33)
34. ### Federal Law No.187-FZ, Rossiyskaya Gazeta , July 2, 2013 , No. 187

    [↑](#footnote-ref-34)
35. ### Federal Law 135-FZ, Rossiyskaya Gazeta , July 2, 2013 , No. 6117

    [↑](#footnote-ref-35)
36. ### Kerr, Jaclyn. “The Russian Model of Digital Control and Its Significance.” Edited by Nicholas D. Wright. *Artificial Intelligence, China, Russia, and the Global Order*. Air University Press, 2019.

    [↑](#footnote-ref-36)
37. ### Soldatov, Andrey, “What did Russia block this Autumn?”, Index on Censorship, November 22, 2013, https://www.indexoncensorship.org/2013/11/russia-censored-autumn-2013/

    [↑](#footnote-ref-37)
38. ### Omidi, Maryam, “Blackout: why Russian internet sites are going dark over anti-piracy laws”, New East Digital Archive, August 1st, 2013, https://www.new-east-archive.org/articles/show/1273/blackout-why-russian-internet-sites-are-going-dark-over-anti-piracy-laws

    [↑](#footnote-ref-38)
39. ### Ünver, H. Akın. “Politics of Digital Surveillance, National Security and Privacy.” Centre for Economics and Foreign Policy Studies, 2018.

    [↑](#footnote-ref-39)
40. ### Ministry of Communications of the Russian Federation, Order n.83 (16th April 2014)

    [↑](#footnote-ref-40)
41. ### Ünver, H. Akın. “Politics of Digital Surveillance, National Security and Privacy.” Centre for Economics and Foreign Policy Studies, 2018.

    [↑](#footnote-ref-41)
42. ### Kerr, Jaclyn. “The Russian Model of Digital Control and Its Significance.” Edited by Nicholas D. Wright. *Artificial Intelligence, China, Russia, and the Global Order*. Air University Press, 2019, p.66

    [↑](#footnote-ref-42)
43. ### Morgus, Robert. “The Spread of Russia’s Digital Authoritarianism.” Edited by Nicholas D. Wright. *Artificial Intelligence, China, Russia, and the Global Order*. Air University Press, 2019.

    [↑](#footnote-ref-43)
44. ### *“Specifically, the Russian government and military are investing heavily in creating the intellectual and physical infrastructure necessary to facilitate AI development across the country, pushing for results in certain civilian and weapons platforms”.*

    ### Bendett, Samuel. “The Development of Artificial Intelligence in Russia.” Edited by Nicholas D. Wright. *Artificial Intelligence, China, Russia, and the Global Order*. Air University Press, 2019

    [↑](#footnote-ref-44)
45. ### *Ibid*., p.168

    [↑](#footnote-ref-45)
46. ### Wright, Nicholas D., ed. “Artificial Intelligence and Domestic Political Regimes: Digital Authoritarian, Digital Hybrid, and Digital Democracy.” *Artificial Intelligence, China, Russia, and the Global Order*. Air University Press, 2019.

    [↑](#footnote-ref-46)
47. ### “*The makers of our Constitution [conferred, as against the government, the right to be let alone - the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment […]”.* Olmstead v. United States, 277 U.S. 438 (1928)

    [↑](#footnote-ref-47)
48. ### *“Attorney General Jackson responded to the decision by reinstating the general ban on wiretapping. But within months President Roosevelt overturned Jackson's policy. A May 21, 1940 memorandum indicated that ‘in the President's view the Supreme Court did not intend to have its decision apply to grave matters involving the defense of the nation’*”, Donohue, Laura K. “Anglo-American Privacy and Surveillance.” *The Journal of Criminal Law and Criminology (1973-)* 96, no. 3 (2006): 1059–1208.

    [↑](#footnote-ref-48)
49. ### Ünver, H. Akın. “Politics of Digital Surveillance, National Security and Privacy.” Centre for Economics and Foreign Policy Studies, 2018.

    [↑](#footnote-ref-49)
50. ### *Ibid., p.7*

    [↑](#footnote-ref-50)
51. ### 18 U.S.C. § 2510, *et seq*.

    [↑](#footnote-ref-51)
52. ### U.S. Department of Justice, *Justice Manual*, (2018), 9.7000 *et seq.*, <https://www.justice.gov/jm/jm-9-7000-electronic-surveillance>, accessed Nov. 3rd 2024.

    [↑](#footnote-ref-52)
53. ### 50 U.S.C. § 1801, *et seq*, 92 Stat. 1783

    [↑](#footnote-ref-53)
54. ### 18 U.S.C. § 2511(2)(a)(ii), (2)(e), and (2)(f).

    [↑](#footnote-ref-54)
55. ### ‘FISA Act’, 50 U.S.C. ch. 36, Pub. L. 95–511, 92 Stat. 1783

    [↑](#footnote-ref-55)
56. ### ‘PATRIOT Act’, 18 USC § 2712, 31 USC § 5318A, 15 USC § 1681v, 8 USC § 1226A, 18 USC § 1993, 18 USC § 2339, 18 USC § 175b, 50 USC § 403-5b, 51 USC § 5103a, Pub. L. 107–56, 115 Stat. 272

    [↑](#footnote-ref-56)
57. ### Section 505 of the Act

    [↑](#footnote-ref-57)
58. ### The ‘Protect America Act of 2007’, Pub. L. 110–55, 121 Stat. 552, instead allowed warrantless wiretapping when foreign intelligence targets were "*reasonably believed*" to be outside the United States

    [↑](#footnote-ref-58)
59. ### ‘USA Freedom Act’, 12 U.S.C. § 3414; 15 U.S.C. § 1681u; 18 U.S.C. § 2709; 18 U.S.C. § 3511; 50 U.S.C. § 1881a, Pub. L. 114-23, 129 Stat. 268 (2015)

    [↑](#footnote-ref-59)
60. ### Heilweil, Rebecca. ‘The FBI is using AI to mine threat tips, but isn’t sharing much detail’, *Fedscoop*, (October 17, 2024), available at <https://fedscoop.com/fbi-ai-tool-threat-tips/#:~:text=The%20Federal%20Bureau%20of%20Investigation,how%20the%20system%20actually%20works>. (accessed 3rd Nov. 2024)

    [↑](#footnote-ref-60)
61. ### Yellig, John. ‘Homeland Security Unveils Emerging Technologies Road Map’, *IoT World Today,* (June 4, 2024), available at <https://www.iotworldtoday.com/security/homeland-security-unveils-emerging-technologies-road-map>

    [↑](#footnote-ref-61)
62. ### Miglio, Michela. ‘SpaceX’s Spy Satellites And The Future Of Space Warfare’, *Praesidium* 1, October 2024, p.33

    [↑](#footnote-ref-62)
63. ### Feldstein, Steven. “Distinguishing Between Legitimate and Unlawful Surveillance.” *The Global Expansion of AI Surveillance*. Carnegie Endowment for International Peace, 2019. http://www.jstor.org/stable/resrep20995.6.

    [↑](#footnote-ref-63)
64. ### Regulation (EU) 2024/1689

    [↑](#footnote-ref-64)