Surveillance and Democracy

CHILLING TALES FROM AROUND THE WORLD

INCLO

INTERNATIONAL NETWORK OF
CIVIL LIBERTIES ORGANIZATIONS

Surveillance and Democracy

CHILLING TALES FROM AROUND THE WORLD

Cover photo: A security camera is mounted on the side of a building overlooking an intersection in midtown Manhattan, on 31 July 2013 in New York.
Photo: Mark Lennihan/AP

ABOUT INCLO

The International Network of Civil Liberties Organizations (INCLO) is a group of independent, national human rights organisations working to promote fundamental rights and freedoms by supporting and mutually reinforcing the work of the member organisations working in their respective countries, and by collaborating on a bilateral and multilateral basis. Each organisation is multi-issue, multi-constituency, domestic in focus, independent of government, and advocates on behalf of all persons in their respective countries through a mix of litigation, legislative campaigning, public education and grassroots advocacy. The members of INCLO that participated in this report are: the American Civil Liberties Union (ACLU), the Association for Civil Rights in Israel (ACRI), the International Human Rights Group Agora (Agora) in Russia, the Canadian Civil Liberties Association (CCLA), the Centro de Estudios Legales y Sociales (CELS) in Argentina, the Egyptian Initiative for Personal Rights (EIPR), the Human Rights Law Network (HRLN) in India, the Hungarian Civil Liberties Union (HCLU), the Irish Council for Civil Liberties (ICCL), the Kenya Human Rights Commission (KHRC), and the Legal Resources Centre (LRC) in South Africa.

table of contents

ACKNOWLEDGEMENTS

The report has been a collaborative effort on the part of ten organisations of INCLO. The primary chapter authors are:

UNITED STATES
Larry Siems, writer, and Brett Max Kaufman, staff attorney in the ACLU's Center for Democracy

ISRAEL
Avner Pinchuk, senior attorney, ACRI

RUSSIA
Damir Gainutdinov, attorney, and Pavel Chikov, executive director, Agora

CANADA
Brenda McPhail, director, Privacy, Technology and Surveillance Project, CCLA

ARGENTINA
Ignacio Bollier, project officer, Democratic Security and State Violence Programme, Ximena Tordini, director of Communications, and Paula Litvachky, director of the Justice and Security Area, CELS

INDIA
Saikat Datta, independent journalist, and Eliza Relman, paralegal, ACLU, with the support of the HRLN

HUNGARY
Fanny Hidvegi, director, Data Protection and Freedom of Information Programme, and Rita Zagoni, programme officer, Data Protection and Freedom of Information Programme, HCLU

IRELAND
Stephen O'Hare, senior research and policy programme manager, ICCL

KENYA
Andrew Songa, programme manager, Transformative Justice, KHRC

SOUTH AFRICA
Avani Singh, attorney, Constitutional Litigation Unit, and Michael Laws, researcher, Constitutional Litigation Unit, LRC

The primary editor of the report was Larry Siems. Lucila Santos (programme coordinator, INCLO), Brett Max Kaufman (staff attorney in the ACLU's Center for Democracy), and Steven Watt (senior staff attorney, ACLU Human Rights Program) also contributed edits.

Jameel Jaffer (deputy legal director of the ACLU and director of the Center for Democracy) reviewed and edited the final report.

Mariana Migueles and Carolina Marcucci were in charge of the report's design and layout. Jazmin Tesone was the report's photo editor. Hilary Burke copyedited the report.

INCLO also thanks the Open Society Foundations, the Ford Foundation and the Oak Foundation for their generous support of its work in this area.

introduction

This report offers a ground-level view of some of the ways surveillance, and digital electronic surveillance in particular, is impacting on the lives of citizens and residents in ten countries in Africa, the Americas, Asia, Europe and the Middle East.

The ten author organisations are members of the International Network of Civil Liberties Organizations (INCLO), and their dispatches are rooted in their experiences as civil and human rights litigators and advocates in their respective countries. Their stories are distinct, reflecting local and national political realities, but their concerns, like the surveillance technologies themselves, are transnational, interconnected and, increasingly, shared.

In the United States, a Marine Corps veteran tries to board a plane and learns he is on a secret no-fly list, apparently based on innocuous private email communications.

In Israel, state security agents summon peaceful political activists for 'warning conversations' that make clear their lives and communications are being monitored.

In Russia, a respected human rights advocate learns after repeated detentions that he is listed in the "human rights activists" section of the national surveillance database.

In Canada, a conscientious judge discovers that his country's intelligence services have been circumventing the law and the courts to spy on Canadian citizens.

In Argentina, the investigation of its worst terrorist attack included illegal surveillance and intelligence activities to cover up the truth, leaving the attack unsolved to this day.

In India, a journalist on the brink of exposing government surveillance of opposition politicians becomes the target of surveillance himself.

In Hungary, the residents of a multiethnic neighbourhood in Budapest find themselves living under the gaze of cameras that can recognise their faces.

In Ireland, the office of the independent ombudsman charged with overseeing the country's national police suspects it has become the target of national police surveillance.

In Kenya, a radical imam is gunned down on the street, and investigations point to state-sanctioned death squads operating on the basis of information gathered through transnational intelligence sharing.

In South Africa, the head of an internationally renowned environmental organisation is the subject of a request for "specific security assessments" from a foreign government to the South African government, and the South African organisation Legal Resources Centre (LRC) learns that it has been subject to unlawful surveillance by the United Kingdom's Government Communications Headquarters (GCHQ).

Separately, these stories describe concrete instances in which governments have used surveillance to violate civil and human rights. Together, they challenge the notion that digital and more traditional surveillance operations are harmless intrusions and that these tools are being used in democratic countries with adequate restraint and oversight.

This publication is by no means a comprehensive survey of the digital and traditional surveillance programmes operating in these countries. Rather, INCLO member organisations have focused on specific cases in their countries where abusive government surveillance has come to light, and where member organisations and other civil and human rights groups have sought to challenge or curtail these practices. While the nature and purpose of these operations differ significantly from country to country, these organisations have faced – and still face – a common set of obstacles in seeking to confront the abuses: most significantly, poorly defined legal frameworks delimiting surveillance powers and safeguarding individual rights; lack of transparency in regard to laws and practices governing surveillance; feeble or insufficient mechanisms for overseeing intelligence agencies and their intelligence operations;

and limited avenues for pursuing accountability when intelligence services misuse surveillance tools.

These are not new challenges. Surveillance, a cornerstone of oppressive states, has always posed a particular test for open, democratic societies; almost by definition, clandestine intelligence gathering strains democratic structures and stretches fundamental commitments to due process, transparency and citizen oversight. But there is something new in the scope and intrusiveness of the surveillance, which is the product of breathtaking technological advances that have opened entirely new windows into citizens' activities and private lives. This exponential expansion of digital electronic surveillance powers has brought widespread anxiety that intelligence gathering may be harming democracy itself, weakening democratic processes and institutions in countries where they are often taken for granted, and impeding or undermining the development of democratic structures in countries that have only recently emerged from more authoritarian systems and abusive surveillance regimes.

Nothing dramatised the magnitude of new surveillance technologies more clearly than the trove of classified US National Security Agency (NSA) documents that Edward Snowden turned over to reporters in May 2013. For years, some INCLO member organisations had sought, largely in vain, to learn how their countries were using new surveillance technologies and powers domestically and internationally. But freedom of information requests and litigation challenging specific surveillance initiatives have too often been impeded by secrecy and thwarted by vague governmental claims of national security. Now the world could see that several intelligence agencies possessed the capacity to monitor electronic communications originating anywhere on Earth, and that the agencies believed they were entitled to gather what the former director of the NSA called 'the whole haystack' of global communications, regardless of domestic and international due process requirements.

But it was not just that the US intelligence services and their so-called 'Five Eyes' partners in the United Kingdom, Canada, Australia and New Zealand possessed and were deploying these novel and far-reaching powers; it was that these countries were sharing information they gathered through these powers with one another, often circumventing laws limiting domestic surveillance in their own countries. These countries have also collaborated with intelligence services in other countries to form surveillance coalitions known as, 'Nine Eyes,' '14 Eyes,' 'Rampart A (or 33 Eyes)' and '41 Eyes,' creating transnational networks to gather, store and share intelligence that not only defy national laws but also challenge concepts of national sovereignty and distort fundamental notions of government accountability to the citizenry and the consent of the governed.

All of these trends are illustrated in this report. In most countries profiled here, domestic intelligence services have employed new surveillance tools on their own populations. In Canada, India, Ireland, Israel, Russia and the United States, they have done so by circumventing legal restrictions meant to act as bulwarks against domestic spying. In Argentina, Hungary, Kenya and South Africa – countries that have struggled in recent years to build stronger and more transparent democratic institutions – the spying has replicated or perpetuated intelligence structures from previous oppressive regimes. In Canada, Hungary, Kenya, South Africa and the United States, the surveillance includes some degree of transnational surveillance and intelligence sharing.

Since well before the Snowden leaks, INCLO members have worked to expose and challenge the abuses described here; in some cases, Snowden's revelations have enabled them to litigate more effectively and to communicate more clearly the ways surveillance powers are affecting the lives of citizens and residents in their countries. But as the South African chapter describes, those revelations also dramatically exposed how our own member organisations, many of them historically targeted for surveillance in their home countries, face new vulnerabilities in the age of transnational digital surveillance – as when the LRC, our South African member organisation, learned its communications had been illegally intercepted by GCHQ in the United Kingdom.

For INCLO members, there could be no more vivid demonstration of how, in this brave new world of transnational digital surveillance, we truly are all in this together.

surveillance in ten countries

the cases

We’re watch-listing you

1
UNITED STATES

A TSA officer checks a passenger's ticket, boarding pass and passport as part of security screening at John F. Kennedy International Airport in New York, on 30 October 2014.
Photo: Mark Lennihan/AP

UNITED STATES

We're watching-listing you

the case

For Ibraheim 'Abe' Mashal, the trip was another sign of the success of Marine Corps Dog Training, the business he launched when he returned to Illinois after serving as a dog handler in the US Marines. He now had customers not just around Chicago but in 20 other states, and on 20 April 2010 he was heading to Spokane, Washington to meet a new client who was willing to fly him that far to have him train her two dogs.

Abe flew often, and it seemed strange that this time he could not check in online. He called the airline. He was told he could collect his boarding pass at the ticket counter in Chicago's Midway airport before his flight.

At the airport, when he handed the ticket agent his driving licence, she gave him a look and disappeared. She returned just as he sensed a scene developing around him. As some 30 Transportation Security Administration (TSA) agents and Chicago Police officers pressed in, the airline representative informed Abe that he was on the US government's 'No Fly List' and that he could not board this, or any other, flight.

The US government's No Fly List is a subset of the Terrorist Screening Database (TSDB), the master 'Watchlist' that the Federal Bureau of Investigation's Terrorist Screening Center has compiled and administered since 2003. The watchlist is drawn from an even larger central Terrorist Identities Datamart Environment (TIDE) database, which a classified 2014 government report boasted had just 'passed a milestone of one million persons.' The government says it includes someone in the TSDB if it has a 'reasonable suspicion' based on 'articulable facts' that the person 'is known or suspected to be, or has been engaged in conduct constituting, in preparation for, in aid of or related to, terrorism and terrorist activities.' Somewhere between 500,000 and 800,000 people were in the TIDE database, and as many as 10,000 of them were on the No Fly List, the morning Abe Mashal found himself surrounded by a posse of police and federal agents at Midway airport's Southwest Airlines ticket counter.

Mashal was led into a back room. An FBI agent rechecked his ID, left the room to make a call, and then started questioning Mashal about the reason for his trip and his religious faith. Mashal answered the agent's questions, and he asked a few of his own. How had he ended up on such a list? The agent said he didn't know – and even if he knew, he couldn't say. How could Abe correct the obvious mistake? The agent told him to look up the Department of Homeland Security's 'TRIP' programme when he got home.

Advertised as a 'One-Stop Traveler's Redress Process' for those 'who have inquiries or seek resolution regarding difficulties they experienced during travel screening at transportation hubs,' the DHS's Traveler Redress Inquiry Program (TRIP) was not much of a programme. It essentially consisted in submitting an online complaint form and then waiting for a 'Determination Letter' – a letter that, if and when it came, often determined nothing. The letter would neither confirm nor deny that the applicant was on the TSDB or No Fly List. It provided no information about why the person may be on the list. It didn't even make clear whether, after the government's review, the person was now able to board a plane.

Mashal submitted his TRIP complaint as soon as he got home from the airport. That same afternoon, two more FBI agents visited him and questioned him in his living room, drilling deeper into his religious beliefs and practices, his family background (his Palestinian father had immigrated to the United States and worked for years as a distribution manager for a well-known candy company; his mother is Catholic and Italian-American), and the training he had received in

the Marines. Again Mashal answered everything, and the exchange seemed to go well; the agents called a few days later to say they were sending his answers to Washington with a recommendation that he be removed from the No Fly List.

Two months later, those same agents called with 'great news,' and asked Mashal to meet them in a Chicago-area hotel. But in a room of the hotel, they delivered 'bad news and good news' instead – the bad, that Mashal was indeed on the No Fly List; the good, that they could have him removed from the list if he would become one of their paid informants. They hinted that they had a large network of informants like him in Muslim communities throughout the Midwest. They also hinted at why Mashal might have ended up on the list, suggesting he had emailed someone who was under surveillance. They asked if he had ever emailed any American imams for advice on raising children in an interfaith household. Mashal, whose wife is Christian and with whom he had three young children, had done just that.

'At that point, I had enough,' Mashal later recalled.

I told them I would not answer any more questions without a lawyer present. None of this made sense to me. Was it even legal for them to go into my email? If I did email someone who was under surveillance, how would I have even known that person was under surveillance? Was it legal for them to blackmail me, by putting me on the No Fly List, in exchange for becoming an informant? Once I told them I wanted a lawyer present, the agents shook my hand, and told me I had to leave.

Mashal contacted the American Civil Liberties Union (ACLU), which had just filed suit in federal district court in Oregon on behalf of a group of clients who were ensnared in similar No Fly ordeals; he became one of 13 plaintiffs suing the Justice Department, the FBI

A protester holds a banner as he attends a demonstration against secret monitoring programmes PRISM, TEMPORA, INDECT and showing solidarity with whistleblowers Edward Snowden, Bradley Manning and others in Berlin, on 27 July 2013.
Photo: Reuters/Latinstock

Ibraheim 'Abe' Mashal in 1999. Photo: Courtesy of Ibraheim Mashal.

and the Terrorist Screening Center in *Latif v. Holder* for violating their due process rights under the US Constitution. Six of those plaintiffs had learned they were on the No Fly List while travelling or living abroad, and had been stranded overseas; seven, including Mashal, found out when they tried to board flights in their home cities and towns in the United States. Like Mashal, three others were veterans of the US armed services. And like Mashal, several of the other plaintiffs reported that FBI agents had tried to recruit them as informants in exchange for removing their names from the No Fly List. In their lawsuit, the plaintiffs sought a court injunction directing the government to remove them from the No Fly List, or else to provide them with a fair process to find out whether and why they were on the list – and if they were, to challenge their blacklisting.

In the months before the case was heard in court, the FBI continued to pressure Mashal, first by phoning him directly and then by questioning a number of his relatives and friends. One of those friends, an employee of another federal agency, called Mashal after the FBI's visit to pass along the message that he would not be removed from the No Fly List unless he dropped the ACLU suit and resumed his conversation with the FBI agents. And then the DHS TRIP Determination Letter arrived. 'After consulting with other federal agencies, as appropriate,' it read, 'it has been determined that no changes or corrections are warranted to any applicable records at this time.' The message to Mashal was clear: he was still on the No Fly List.

In May 2011 a federal judge in Portland, Oregon dismissed the 13 No Fly plaintiffs' lawsuit, saying that the court lacked jurisdiction in the case. The ACLU appealed, and the Ninth Circuit Court of Appeals unanimously reversed that decision and ordered the district court to hear the case. In that order, the Court of Appeals highlighted the Kafkaesque question at the heart of the case. 'At oral argument,' the panel noted, 'the government was stymied by what we considered a relatively straightforward question: what should United States citizens and legal permanent residents do if they believe they have been wrongly included on the No Fly List?'

In August 2013 the district court ruled that American citizens and residents have a constitutionally protected liberty interest in international travel. A year later, in June 2014, the court struck down the existing DHS TRIP redress procedure as unconstitutional, finding that the process was 'wholly ineffective' and that 'without proper notice or opportunity to be heard, an individual could be doomed to indefinite placement on the No-Fly list.' It ordered the government to tell the 13 plaintiffs if they were on the list and why, and give them the opportunity to challenge their status consistent with constitutional due process rights.

Finally, on 10 October 2014 – four and a half years after Abe Mashal was told he was banned from air travel – the ACLU received a letter stating that Mashal and six of his co-plaintiffs 'are not on the No Fly List as of the date of this letter.' Mashal described the impact of the news a few hours later:

More than four years ago, I was denied boarding at an airport, surrounded by TSA agents, and questioned by the FBI. That day, many freedoms that I took for granted were robbed from me. I was never told why this happened, whether I was officially on the list, or what I could do to get my freedoms back. Now, I can resume working for clients who are beyond driving distance. I can attend weddings, graduations and funerals that were too far away to reach by car or train. I can travel with my family to Hawaii, Jamaica, or anywhere else on vacation. Today, I learned I have my freedoms back.

For six of the other plaintiffs, though, the ordeal continues. They have since received unclassified 'summaries' of some of the reasons they were placed on the No Fly List, but those summaries are far from a full explanation. The government still has not given them a meaningful hearing. For these men and women, and for many more who have filed complaints through the DHS TRIP process, the saga continues. For that reason, the ACLU has challenged the

government's new redress process as falling far short of constitutional fair process requirements.

And scores of new names are added to the No Fly List every day. The list doubled in size in 2012, from around 10,000 to 21,000; it more than doubled again the following year, to almost 50,000; and as of September 2014, it contained approximately 64,000 names. Like Abe Mashal, most of these men and women may never know they are on the US government's lists until they try to board what they thought would be a routine business or vacation flight.

the context

The United States' ever-expanding watchlists are fuelled by surveillance powers of breathtaking capacity and reach.

In early June 2013 The Guardian newspaper published a leaked, secret order of the US Foreign Intelligence Surveillance Court that revealed that the National Security Agency was collecting the telephone records of millions of Americans on an ongoing, daily basis, giving the world its first glimpse of the most sprawling domestic surveillance programme in US history. Just days later, The Washington Post reported on PRISM, a programme that allows the NSA to receive data directly from US companies like Google and Facebook, including the contents of the emails, text messages, video chats, photographs and more of the NSA's foreign targets and anyone in communication with those targets. Only then did we learn that the source of these stunning revelations was Edward Snowden, a contract employee of the NSA who had fled the United States with a trove of documents exposing the staggering scope of the NSA's digital surveillance power. Over the next days and weeks the revelations kept coming, and they haven't stopped.

Despite all that we've learned, and despite legal challenges and legislative reforms, the basic physical and legal infrastructures of NSA spying remain intact. The government continues to conduct dragnet surveillance under two legal authorities – a 2008 law called the FISA Amendments Act, or FAA, and a Ronald Reagan-era executive order – that permit the NSA to monitor vast streams of internet traffic by siphoning off huge amounts of it, often in bulk, for copying and searching in its own communications databases. The government accomplishes this dragnet, in part, through secret collaborations with telecommunications companies that operate the internet 'backbone' – the global network of high-capacity cables that carry digital communications around the world. It also relies on partner intelligence agencies, both inside and outside the so-called Five Eyes, for access to various massive data streams all around the world.

Inside the United States, this dragnet surveillance is conducted under the FAA, a law that vastly expanded the NSA's power to acquire a huge amount of international communications from internet and telecommunications providers within the United States. Under the government's interpretation of the law, virtually every international communication – that is, every communication going into or out of the United States – is within the reach of the NSA's surveillance. What's more, under its interpretation of the law, the NSA is permitted to hold on to the communications of Americans that the agency intercepts 'incidentally' – meaning that whenever the NSA targets the communications of foreigners (either individually or in bulk), it is entitled to copy, review and save communications involving Americans, all without ever seeking a warrant as the Fourth Amendment of the US Constitution requires. (In fact, in hearings before the passage of the law, government officials admitted that this sort of end run around the Fourth Amendment's warrant requirement was precisely the point of the new legislation.)

Outside the United States, the government's dragnet relies on an executive order over which no court has any supervisory authority and on which congressional oversight is scant. The government argues that whenever a federal statute or the Constitution does not regulate its surveillance conduct, the only authority that does is the executive order – meaning, in the government's view, that surveillance conducted abroad is more or less a free-for-all. The order creates sprawling permissions to conduct surveillance that does not involve Americans and does not take place on US soil, effectively permitting the US government to monitor any foreigner for the purpose of gathering 'foreign intelligence' – a broadly defined term – including journalists, human rights activists or lawyers.

Reports have indicated that the scope of global surveillance conducted by the NSA under the order is enormous: it includes the collection of buddy lists and address books, the hacking of system administrators, the installation of malware and, perhaps most astoundingly, the recording and retention of virtually every telephone call taking place on the phone networks of several foreign countries. In addition, documents have shown that the NSA has used the order to target European Union institutions, state-run corporations in Brazil, and world leaders at the 2009 G20 summit. Most strikingly, under what is termed 'about' surveillance, the government believes it may monitor the internet backbone for communications using keywords – in other words, that it may search through the contents of messages that traverse the wire all around the world.

All of the NSA's own activities are compounded by its co-operation with, and reliance on, foreign

> Under what is termed 'about' surveillance, the government believes it may monitor the internet backbone for communications using keywords – in other words, that it may search through the contents of messages that traverse the wire all around the world.

governments. An unprecedented 2015 ruling by the United Kingdom's Investigatory Powers Tribunal determined that the UK Government Communications Headquarters (GCHQ) had for years acted unlawfully in accessing millions of people's personal communications after they had been collected by the NSA, and the sharing of information between the NSA and GCHQ appears to be rampant. That sharing reportedly includes the feeding of GCHQ-obtained information – including private videos obtained under a programme called 'Optic Nerve' – into the NSA's signals-intelligence database, XKeyScore. The NSA also receives data from various signals-intelligence collection points around the world, including many sites in the United Kingdom and Australia. And the NSA routinely shares intelligence data – even raw data, which includes identifying information about Americans and others – with foreign intelligence agencies, including Israel's SIGINT Unit.

The ACLU has spent much of the past several years challenging the NSA's dragnet in court. Just days after The Guardian published the previously secret FISC order concerning the NSA's bulk phone-records collection, the ACLU filed a lawsuit challenging the bulk collection programme on statutory and constitutional grounds. While the suit remains pending in the US Court of Appeals for the Second Circuit, in May 2015 the appellate court ruled that the government's use of Section 215 of the Patriot Act for bulk phone-records surveillance was both 'unprecedented and unwarranted.' That legal victory coincided with the passage, in Congress, of the USA Freedom Act, legislation that repudiated the government's phone-records programme and made other changes – however minor – to other government collection authorities and to government transparency rules.

The ACLU has also challenged the FAA in court, both through participation in various criminal cases in which defendants were given notice of the use of the statute in their prosecutions, and in a civil case filed in March 2015, *Wikimedia v. NSA*, brought on behalf of nine civil society organisations. (Because of various legal doctrines developed by the Supreme Court, legal challenges on behalf of foreigners, or even Americans, to surveillance conducted under the executive order are exceedingly difficult to pursue.) The ACLU argues that the FAA violates the Fourth Amendment's prohibition on unreasonable searches and seizures by dispensing with any individualised judicial review of targeting decisions, and that it violates the First Amendment by intruding on the rights to free association and free speech. Those cases are ongoing, as is a similar challenge, *Jewel v. NSA*, brought by the Electronic Frontier Foundation.

These legal challenges face enormous obstacles. First, it is difficult to establish 'standing' to sue – essentially, the legal right to be in court at all – in surveillance cases. Since the Supreme Court's decision in an earlier ACLU case, *Clapper v. Amnesty International USA*, filed in 2008 and challenging the same law, plaintiffs taking on government surveillance must demonstrate that the government's collection of their communications is not based on speculation or unproven assumptions about the ways in which government surveillance works; in essence, plaintiffs must show that they have been targeted under what is, by definition, a top secret programme. Fortunately, the vast amounts of information gained directly from the Snowden revelations and indirectly through, for example, official government disclosures, cast the 'standing' question relating to NSA surveillance in a much different light than in the original *Amnesty* lawsuit, and cases like *Wikimedia* may finally succeed in prying open the courthouse doors for an NSA challenge.

But even if they establish standing to sue, plaintiffs will face a formidable challenge at trial, where a government-invoked 'state secrecy' privilege is often fatal in surveillance cases. The 'state secrets' doctrine effectively allows the government to put a stop to litigation by claiming that allowing the lawsuit to proceed jeopardises national security secrets.

Finally, it is critical to note that Edward Snowden himself – the whistleblower whose courage jump-

started the renewed global debate about government surveillance, both by the United States and others, and whose actions have directly led to surveillance reforms at home and abroad – remains unable to return home to the United States. The US government has charged Snowden with violations of the Espionage Act, among the most serious felonies in American law. During any trial for these crimes, Snowden would be barred, under US law, from mounting a defence rooted in the First Amendment that highlights his intent to inform the American public about the NSA's activities, the lack of harm that his leaks caused to American interests, and the benefits of those leaks to a public debate that the government itself acknowledges would never have happened without him. While Snowden continues to lead a meaningful life in exile in Russia and to participate in the global surveillance debate, it is high time for the US government to find a path for him to return home.

conclusion

A government has ears everywhere. It overhears a man's private conversation and puts that man on a list. Doors close for that man because he is on the list. When he runs into one of those doors and discovers he is on a government list, he cannot learn why. When he tries to remove his name from the list, he is told the only way to do so is to become another set of government ears – the ears that are overhearing private conversations and putting people on lists.

In many ways Abe Mashal's story reads like a parable of the conventional security state transposed to the digital age: if Edward Snowden's revelations have illuminated the staggering scope of the United States' digital surveillance powers, the experiences of the ACLU's No Fly plaintiffs point to how deeply that surveillance reaches into the private lives of US citizens and residents. The Kafkaesque difficulties they have had in trying to extricate themselves from the list underscore how self-protective and self-perpetuating secret and pervasive surveillance systems tend to be. Abe Mashal and his co-plaintiffs won an important victory in their challenge to the No Fly List. But when it comes to the new surveillance-fuelled list-making in the United States, it is just a start.

Surveillance at a glance in the United States

Do citizens know more now than they did three years ago about the government's surveillance activities?
Yes

Did the Snowden disclosures lead to meaningful public debate in your country about the proper limits on government surveillance?
Yes

Since the Snowden disclosures, have any whistleblowers come forward to inform the public about government surveillance activities?
Yes

In the last three years, have the government's national-security surveillance authorities been narrowed, expanded, or neither?
Narrowed in some respects, expanded in others

In the last three years, have new structural checks (e.g. new transparency requirements) been imposed on intelligence agencies?
Yes

If the legislature/parliament is considering new legislation relating to government surveillance, would that legislation narrow the government's surveillance powers or expand them?
Narrow

If the legislature/parliament is considering new legislation relating to government surveillance, would that legislation impose new structural checks?
Yes

Over the last three years, have the government's national-security surveillance authorities been the subject of domestic litigation, including in constitutional courts?
Yes

Over the last three years, have the courts rejected as incompatible with constitutional or human rights law any aspect of government surveillance?
Yes

Over the last three years, do you think the public has come to trust the intelligence agencies more, less, or neither?
Less

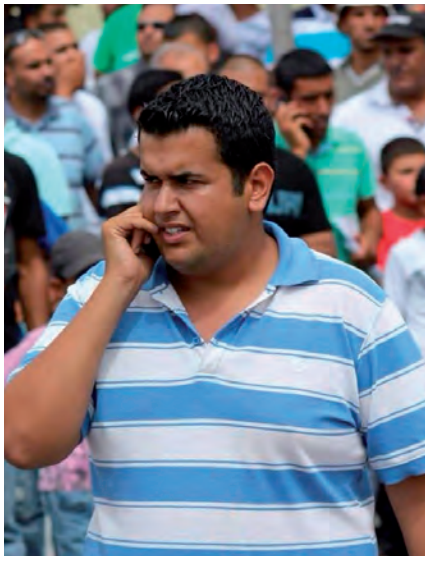
Warning conversations: an intimidation approach to activism?

2
ISRAEL

Demonstrators shout slogans during a protest against the Prawer-Begin Plan in Haifa, on 30 November 2013.
Photo: Mareike Lauken/Active Stills

ISRAEL

Warning conversations: an intimidation approach to activism?



Rateb Abu-Krinat during one of the demonstrations against the Prawer Plan in 2013.
Photo: Eslam Alsana

the case

As a field worker for the NGO 'Negev Coexistence Forum for Civil Equality,' Rateb Abu-Krinat was active in promoting full civil rights and equality for Arab-Bedouin citizens in the Negev region of southern Israel. Between 2012 and 2013, his activism included participating in public protests against the 'Prawer Plan,' a controversial government initiative to regulate the land ownership structures of the Negev Bedouin.

In June 2012, Rateb received a call requesting that he report to the local police station as part of an investigation. Rateb, an Arab-Israeli citizen, voluntarily complied. When he arrived, he was subjected to a humiliating body search and then taken to a room and introduced to a man who identified himself as 'Jamil' from Shin Bet, the General Security Service (GSS). Insisting that this was just a 'regular conversation,' Jamil proceeded to question Rateb for two and a half hours about his studies and his work, and pressed him to provide details about his family and his friends. Towards the end of the conversation, Jamil asked him about his position on the Prawer Plan. The GSS official concluded this session by making it clear to Rateb that he already knew a great deal about his life and activities and that while he was currently 'untainted,' he should be wary of participating in activities that could harm the security of the state; Jamil told him that he should 'pray' that there would be no need for them to meet again.

Eight months later Rateb received another summons to a follow-up on that meeting at the police station. This time he reached out to the Association for Civil Rights in Israel (ACRI).

For several years ACRI had been gathering testimonies from civil society activists who had been summoned for similar 'warning conversations' with GSS agents. An ACRI employee who worked to defend the rights of residents of East Jerusalem was among them. An

activist involved in Jewish-Arab political activities in northern Israel had likewise been called in, questioned and cautioned, as had activists involved in protest activities against the Occupation, the construction of the Security Barrier, and the blockade on the Gaza Strip.

The testimonies that ACRI collected followed a pattern. Those summoned for these 'conversations' were all activists engaged in advocacy for policies that challenged public consensus. The conversations, which were not part of formal investigations of specific crimes, had the tenor of interrogations, with GSS agents questioning activists about both their personal lives and political activities. The activists were often asked to supply names and phone numbers of family or friends and in some instances were asked for details about their financial situation. In some cases, GSS agents explicitly told the activists that while they were not suspected of violating the law 'for now,' they should be careful not to do so in the future; other times the agents made vague assertions, without specific allegations, that the activists had been involved in disturbances of the peace. Occasionally, the warnings and threats were blunt: one of the 'suspects' was told to 'be aware that we will launch a case against you' but was given no explanation as to what alleged illegal conduct might precipitate such a case.

Most troublingly, in many of the 'warning conversations' it was made explicitly clear to those summoned that the GSS already knew a lot about them and had been monitoring their activity. One of the activists recounted how:

[The agent] began to raise all kinds of personal information about my life that even those close to me don't know…it was as if he was telling me 'we know who you are, we know what you do.'[1]

With reports of these 'warning conversations' mounting, ACRI contacted the GSS and the attorney general several times to demand that they immediately end the practice of 'warning conversations.' One of the few responses received in a letter from the Attorney General's Office, signed by a senior advisor to the attorney general, only intensified the concern.[2]

The letter explained that the activist in question was summoned to participate in a conversation because the GSS possessed information concerning his involvement in a violent demonstration in the country's north, even though GSS agents hadn't raised such an allegation during their conversation with him. As for the legal basis for summoning citizens to 'warning conversations,' the letter referred to the General Security Service Act (GSSA), which authorises the agency to thwart or prevent any illegal activity whose aim is to harm state security, the democratic regime or its institutions. This is despite the fact that, under Israeli law, activities that are considered public disruptions belong under the purview of the Israeli police, not the GSS.

And it was not just that the purported basis for the 'these exchanges' was tenuous; the letter also suggested, as the GSS agents had intimated during 'warning conversations,' that the conversations were linked to evidence gathered via other intelligence powers. According to the letter, when Israeli citizens are targeted for 'warning conversations,' it generally follows the collection of intelligence information. When such intelligence information is received, as explained in the Attorney General Office's letter, its credibility is examined and an attempt is made to supplement it as far as possible with additional intelligence 'gathering tools' — tools that sometimes may include the summation for 'inquiry,' i.e. 'warning conversations.'

When Rateb alerted ACRI that he had received a second summons to report to the police station for further questioning, ACRI sent an urgent letter to the attorney general and the Shin Bet demanding that they

> “The GSS official concluded this session by making it clear to Rateb that he already knew a great deal about his life and activities and that while he was currently ‘untainted,’ he should be wary of participating in activities that could harm the security of the state.”

rescind the summons. The next morning – remarkably swiftly – ACRI received a reply from the GSS’s legal department clarifying that Rateb Abu-Krinat was under no obligation to attend the meeting.

But additional ACRI requests that the GSS and the attorney general explain and delineate the limits of the GSS’s supposed authority to conduct these ‘warning conversations’ went unanswered. So, in July 2013 ACRI submitted a legal petition against the GSS to the Supreme court of Israel.

the context

Digital surveillance is pervasive in Israel with powers distributed among four main intelligence-gathering entities: Unit 8200, which is the Signal Intelligence (SIGINT) Unit of the Israeli Defence Forces; the GSS; the MOSSAD; and Israeli police.

As Israel’s internal security service, the GSS has sweeping access to all communications in Israel. Under the GSSA, the GSS is authorised ‘to receive and collect information’[3] for the purpose of carrying out its missions, including the ‘protection of State security and the order and institutions of the democratic regime against threats of terrorism, sabotage, subversion, espionage, and disclosure of State secrets.’[4] For the GSS, this includes the power to wiretap the phones and monitor the internet activities of Israeli citizens without judicial oversight. To use these tools, it is sufficient simply to receive approval from the prime minister.

To collect communications metadata, the GSS does not even need to seek approval from the prime minister. A permit is given by the head of the service.5 Secret appendices – which are attached to the franchises and licences the state issues to communications companies (according to the Communications Law[6]) and which include specifications on technical infrastructure (equipment and facilities located at the licensee’s premises) – grant Israeli intelligence agencies direct and full access to their databases, enabling the GSS to monitor all communications and collect all metadata directly, without any involvement or specific knowledge of the companies.

In 2007, as part of the Freedom of Information Act’s litigation, the Ministry of Communication refused to disclose the secret appendices attached to the franchises and licences. However, under the court’s enquiry, the minister confirmed that the GSS holds ‘the key’ to the databases – meaning the companies providing internet services do not even know how and when the GSS accesses their databases.

The Israeli public remains in the dark about the scope of surveillance that is conducted under this authority. The GSS is entirely exempt from the Freedom of

Palestinian and international activists react to stun grenades thrown by Israeli forces during a Day of Rage protest against the Prawer-Begin Plan in front of the Israeli settlement Bet El, Al Jalazun, West Bank, 30 November 2013.
Photo: Ryan Rodrick Beiler/Active Stills

Information Act, so the public has no means to find out how often and under what circumstances this power is used. While the prime minister is subject to Freedom of Information Requests (known as FOIA), the GSS exemption means that even something as general as the number of wiretapping permits the prime minister approves each year remains classified. When the prime minister was pressed directly on the question, he insisted that the information is not in his 'physical' possession, because he returns all requests and approvals of wiretaps to the GSS. When ACRI filed a FOIA petition seeking statistics from the Prime Minister's Office on the number of GSS surveillance permits it had approved, the District Court and then the Supreme Court rejected that petition, accepting the state's argument that the relevant data is entirely in the hands of the GSS. That position both distorts the scope of the GSS's legal privilege and calls into question how effectively and rigorously the prime minister supervises the GSS's wiretapping requests.

In 2012 Avi Dichter, the former head of the GSS between 2000 and 2005, acknowledged that he managed to pass the key section governing SIGINT data communication largely 'under the radar' thanks to the fact that people at the time did not realise the full significance of communications metadata and just how revealing that information can be. Dichter also insisted that the GSS 'paid' for those fantastic legal powers by agreeing to 'transparency' in its digital surveillance activities. But what this transparency amounted to was secret and limited reports to certain government ministers, a closed committee in the Knesset, and the attorney general – reports as hidden from the public as the programmes themselves, and reports, Dichter admitted, that were of little interest to these government overseers. In Dichter's words:

I can't recall a single instance as head of the GSS… when a legal or government official…called and told us that we hadn't met the deadlines for providing written or oral updates. In every instance, without a single exception, it was always us that pulled up our sleeves and contacted the attorney general or the Ministerial Committee to say 'friends, you forgot that we are required to report to you.'[7]

The purposes for which the GSS is empowered to mine communications metadata are very broadly and vaguely defined. Wiretapping is conditioned, at least by the wording of the law, on its being 'necessary for state security needs,' and in granting GSS wiretapping

Israeli police march as Bedouin youth throw stones during a protest against the Prawer-Begin Plan, on road 31 near Hura, Israel, on 30 November 2013.
Photo: Oren Ziv/Active Stills

requests, the prime minister is required to balance those needs against the right to privacy. By contrast, a permit to collect or use metadata is issued by the head of the GSS once he or she has been 'convinced that this was required by the Service to fulfil its functions under [the GSSA].'[8]

This is the same statutory standard the GSS relies on to justify its practice of summoning activists to 'warnings conversations.' But while metadata collection and the majority of the GSS's other surveillance activities operate entirely out of view, the 'warning conversations' are conducted in the public realm, offering a rare glimpse into the kinds of activities the GSS engages in under the heading of national security. In challenging the practice of 'warning conversations,' ACRI has sought to drag the GSS's interpretation of its functions and powers into the light.

The GSSA defines the GSS's role in an extremely broad way, stating that 'the service shall be responsible for the protection of State security and the institutions of the democratic regime against threats.'[9] These threats include not only terrorism or espionage but also 'subversion' and threats to 'other State interests vital for national State security, as prescribed by the Government.'[10] ACRI's petition challenged the GSS's wide interpretation of those statutory terms, especially in relation to 'subversive activities.'

In a 2007 response to an enquiry from ACRI, Yuval Diskin, the former head of the GSS between 2005 and 2011, asserted that 'the position of the GSS is that "subversion" can also include aiming to alter the fundamental values of the state by annulling its democratic or Jewish character.'[11] A 2012 GSS publication named 'Radical Right and Left' indicated that the service is not only gathering information on such alleged subversion but has acted on that information, noting that 'Shin Bet information, passed to the state enforcement agencies, has helped to curb acts of delegitimisation of Israel.'[12]

In its response to ACRI's petition challenging 'warning conversations,' the state asserted for the first time that, following a 2009 revision to the definition of 'subversion,' activities or protests against the 'Jewish character of the state' were no longer considered 'subversive activity' under the mandate of the GSS. The fact that such a decision had been made four years earlier, in secret,

> “[I]n many of the ‘warning conversations’ it was made explicitly clear to those summoned that the GSS already knew a lot about them and had been monitoring their activity.”

and was only revealed in response to ACRI’s petition, was troubling in itself. More troubling, though, was the state’s ongoing acknowledgement that the GSS was nevertheless continuing to monitor protests for subversion. According to the state:

As a rule, in a democracy, protests (that exceed the bounds of the law) are a police matter and not a matter for the GSS…However, the GSS must act to foil protest displays that are conducted for subversive and nationalistically motivated ideological reasons, and under circumstances in which the nature of the protest poses a risk to state security.[13]

In its response, the state failed to explain how it differentiates acceptable protests from demonstrations ‘that are conducted for subversive and nationalistically motivated ideological reasons’ and that pose ‘a risk to state security.’

Why are some demonstrations such as the ones Rateb engaged in on behalf of the Bedouin community and against the Prawer Plan treated as state security matters subject to GSS scrutiny, while other protests, such as those organised by Ultra-Orthodox Jews against army conscription, are not treated as such, even when there are fears of public disturbances? To what extent are issues that are of key importance to Israeli Arabs, for example, more likely to be classified and treated as ‘nationalist’ and ‘subversive’ threats to state security? Or treated as activities that serve to ‘delegitimise’ Israel, activities that the GSS asserts the authority to monitor and thwart.

In its response to ACRI’s challenge to the ‘warning conversations,’ the state asserted that thwarting ‘delegitimisation’ did not serve as the legal basis for summoning the plaintiffs named in ACRI’s petition. But as we mentioned before, the ‘warning conversations’ are only one of the state’s many intelligence ‘gathering tools’ (a term that covers a wide scope of surveillance activities). Furthermore, the Israeli government doesn’t differentiate between calls to delegitimise the occupation of the Occupied Territories and calls to delegitimise the very existence of Israel as a state, leaving a wide range of anti-occupation and ‘anti-Israeli’ protest activities vulnerable to the (much more pervasive) monitoring and surveillance of the GSS.

ACRI’s petition argues that ‘inviting’ political activists to ‘warning conversations’ exceeds the legal authority of the GSS, and it challenges the sweeping manner in which the GSS comprehends its mandate and the wide spectrum of political activities that it considers within its purview. The petition asserts that ‘warning conversations’ violate citizens’ fundamental constitutional rights – the rights, first and foremost, to freedom of expression and to protest, and also the rights to dignity, privacy, freedom, equality and due process – and that these ‘conversations’ have a chilling effect on legal protest activity. It further argues that protest activity in general properly belongs under the scrutiny of the police, which unlike the GSS is subject to public oversight and judicial review – however insufficient these powers of review may be in actual practice.

After a public hearing on ACRI’s petition – a hearing during which one of the judges noted that the criteria the GSS asserts for determining whether demonstrations and other protest actions constitute a security threat could be applied to almost every protest or political activity of Arab citizens of Israel – the judges announced they would continue the hearing in private with the GSS’s legal representatives alone. The court subsequently issued a confidential judgment in which, according to their explanation in open court, the judges asked for further clarifications. They also announced that when they receive those clarifications from the GSS, they will reach a final judgment and decide to what extent they can publish a public and unclassified ruling. Once the GSS submits its classified explanations, it could take up to six months for the final verdict to be handed down.

conclusion

Calling peaceful political activists for friendly conversations over a cup of tea with undercover security agents is hardly a hallmark of democratic societies – especially when those conversations have the tenor of interrogations and include probing questions about political and personal associations and activities, and when the agents are from a security service that wields enormous surveillance powers.

The case of Rateb Abu-Krinat and his fellow activists exposes how, in the hands of a security agency that operates with little public oversight or accountability, sweeping surveillance powers can be combined with intimidation tactics and can be turned on dissenters. As a result, surveillance can be used to harass activists and discourage even peaceful protests and legitimate, constitutionally protected political activities.

'Warning conversations' are only the visible tip of a massive intelligence-gathering apparatus that is being wielded with extremely limited oversight in ways that themselves may pose a threat to the fundamental rights of Israeli citizens.

The stakes in the current litigation are high. As ACRI argued before the Supreme Court:

The limits of the authority of the GSS to track political activity possess implications for the scope of its use of [intelligence] "gathering" tools – specifically its collection and analysis of communications data and execution of wiretapping. These activities are not placed under judicial or public scrutiny. In these circumstances, there is great importance in a clarifying ruling that delineates the borders of the law with regard to the political activities of the GSS. We can assume, that in many of the cases, in which activists are invited for "warning conversations", other unknown activities of [intelligence] "gathering" are performed. A ruling that sets out the interpretation of the GSS authority is necessary to prevent the excessive and harmful utilisation of these tools – a utilisation which by its nature will never be subjected to direct scrutiny.

notes

-

1. ACRI's petition (HCJ 5277/13 *ACRI v. GSS*), par. 23. Available at: http://www.acri.org.il/he/wp-content/uploads/2013/07/hit5277.pdf
2. Letter sent to ACRI by Mr. Raz Nizry, then senior advisor to the Attorney General's Office, dated 9 June 2010. The letter, in Hebrew, is available at http://www.acri.org.il/he/wp-content/uploads/2011/11/Nizri090610.pdf.
3. GSSA, Section 8(a)(1). Available at: http://www.knesset.gov.il/review/data/eng/law/kns15_GSS_eng.pdf
4. GSSA, Section 7(a)
5. GSSA, Section 11
6. Communications Law (Telecommunications and Broadcasting) 5742-1982, Section 13(b). Available at: http://www.moc.gov.il/sip_storage/FILES/9/3889.pdf
7. Avi Dichter speaking at the panel on 'The 10th anniversary of the SSG Act,' YouTube (Hebrew). Available at: http://youtu.be/BZ1sZqa0BR0?t=18m43s
8. GSSA, Section 11(c) [See Section 11(c) of GSSA, in footnote no. 6]
9. GSSA, Section 11(c) [See Section 11(c) of GSSA, in footnote no. 6]
10. GSSA, Sections 7–8
11. 'The Shin Bet - Guardian of Democracy?' Haaretz (12 February 2016). Available at: http://www.haaretz.com/print-edition/features/the-shin-bet-guardian-of-democracy-1.250879
12. General Security Service. '2012 Annual Summary: Data and trends in terrorism and prevention response,' GSS website, p. 13. Available at: https://www.shabak.gov.il/SiteCollectionImages/Hebrew/TerrorInfo/Years/2012-he.pdf
13. Section 22 in the state's response to ACRI's petition (HCJ 5277/13 *ACRI v. GSS*), 22 February 2014. Available at: http://www.acri.org.il/he/wp-content/uploads/2014/03/hit5277meshivim0214.pdf

Surveillance at a glance in Israel

Do citizens know more now than they did three years ago about the government's surveillance activities?
Yes

Did the Snowden disclosures lead to meaningful public debate in your country about the proper limits on government surveillance?
No

Since the Snowden disclosures, have any whistleblowers come forward to inform the public about government surveillance activities?
No

In the last three years, have the government's national-security surveillance authorities been narrowed, expanded, or neither?
Neither

In the last three years, have new structural checks (e.g. new transparency requirements) been imposed on intelligence agencies?
No

If the legislature/parliament is considering new legislation relating to government surveillance, would that legislation narrow the government's surveillance powers or expand them?
Expand them (not intelligence surveillance, but surveillance by police and other law enforcement agencies)

If the legislature/parliament is considering new legislation relating to government surveillance, would that legislation impose new structural checks?
Yes

Over the last three years, have the government's national-security surveillance authorities been the subject of domestic litigation, including in constitutional courts?
Yes

Over the last three years, have the courts rejected as incompatible with constitutional or human rights law any aspect of government surveillance?
No

Over the last three years, do you think the public has come to trust the intelligence agencies more, less, or neither?
Neither

Vigilant state: the ‘Surveillance Database’ and other tools

3
RUSSIA

Sergey Shimovolos, human rights defender from Nizhny Novgorod. Photo: Courtesy of Sergey Shimovolos.

RUSSIA

Vigilant state: the 'Surveillance Database' and other tools

the case

The 600-kilometre train trip from Nizhny Novgorod to Samara is a short one by Russian standards, and should have been routine for Sergey Shimovolos, who heads the Nizhny Novgorod Human Rights Union, a non-governmental association uniting ten human rights organisations and environmental organisations in the region. But as soon as Shimovolos boarded the train on 13 May 2007, his troubles began.

Three police officers descended on Shimovolos, demanding to see his identity documents and to know the purpose of his trip. Twice more during the 15 hour trip, he was questioned by police officers checking his identity documents, asking him about the purpose of his journey, and wanting to know if he had any acquaintances in Samara. Once he was even ordered to leave the train and follow the police officers to the police station but he refused to comply, and the police could not offer any legal grounds to detain him.

Shimovolos had an inkling of why this was happening. He was travelling to Samara to investigate the detention of several activists who had been involved in recent protests against the Kremlin, and he was doing so four days before Russian President Vladimir Putin was to host the 19th EU–Russia Summit on 17 and 18 May 2007 in the Volzhskiy Utyos sanatorium in Samara. Among the guests would be Chancellor Angela Merkel of Germany, which at that time held the presidency of the Council of the European Union, and José Manuel Barroso, president of the European Commission. On the agenda were negotiations on a new EU–Russia Partnership and Cooperation Agreement, energy cooperation, deployment of components of a US missile defence system in Poland and the Czech Republic, and Russia's accession to the World Trade Organization. Also on the agenda was the issue of Russia's human rights record, which in 2007 included international concerns about Russia's handling of a wave of 'March of Dissent' opposition protests in different regions of the country over the previous two years.

Activists were planning another 'March of Dissent' during the summit, and for the first time since 2005 the march had officially been approved by the local authorities. But that didn't stop police from carrying out a series of detentions that left many activists, human rights defenders and journalists unable to take part in the protests. In Samara, a number of activists and march organisers were detained on flimsy pretexts in the days leading up to the summit, and other leading activists who were planning on travelling to Samara were targeted throughout the country.

In Moscow, 27 people were detained at Sheremetyevo airport on the eve of the event, including the United Civil Front leaders Garry Kasparov, Alexander Ryklin and Alexander Osovtsov; National Bolshevik Party leader Eduard Limonov; Wall Street Journal reporter Alan Callison; Dutch TV reporter Allard Detiger; Daily Telegraph reporter Adrian Blumfeld; and Alexander Petrov, the representative of the Moscow office of Human Rights Watch. Checking passengers' names against a list, police officers seized the passports of several of these people and gave them back after the plane had departed, while officers of the Federal Security Service (known as the FSB) prevented others from boarding the plane.[1]

Authorities fanned out through the railway system as well. Sergey Udaltsov, the leader of the Vanguard of Red Youth, was detained at Kazanskiy rail station in Moscow as he was buying tickets for the Moscow–Samara train. Denis Bilunov, executive director of the United Civil Front, was detained on a train as it was approaching Samara, on the pretext of checking the authenticity of his pocket money. The detentions were raising alarms in Russia's human rights community. For Sergey

> According to various sources, the 'Surveillance Database' includes the names of 3,800 to 6,500 persons, some of them representatives of far-right and nationalist organisations, and some of them political and civil rights activists. Shimovolos was listed in the section entitled 'Human Rights Activists.'

Shimovolos, the harassment he endured on the train from Nizhny Novgorod was an example of the very thing he was travelling to Samara to investigate.

It did not end when he reached Samara. As he got off the train, Shimovolos was again stopped by several police officers. They checked his identity documents and this time, they ordered him to go with them to the police station so they could look up his name in what they called 'the database,' threatening to use force if he refused to comply with their order. Shimovolos was held at the police station for around 45 minutes before being released.

Shimovolos was angry. Troubled by what seemed to be a coordinated round-up of activists and journalists and by the insinuation that officials maintained a database that included peaceful dissenters and human rights activists, Shimovolos tried three times to initiate formal complaints against the police officers who had detained him; each time, prosecutors refused to open criminal proceedings against the officers. So in May 2007 and again in December 2008, Shimovolos filed civil actions for his arrest and his repeated detentions and for the fact that he was registered in the Russian government's surveillance database. Those efforts too were unsuccessful, and having exhausted all possible legal remedies in Russia, Shimovolos filed application before the European Court of Human Rights (ECtHR), arguing that his arrest and the collection of his personal data in a surveillance database violated Articles 5 and 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. Those proceedings and the investigations relating to them revealed not only that Shimovolos had indeed been the target of deliberate official harassment, but also that authorities maintained an extensive and intricate surveillance system aimed at controlling the movement of 'suspicious' persons in Russia.

Documents that came to light as a result of Shimovolos's complaints revealed that a month and a half before his journey, the Nizhny Novgorod Interior Department registered his name in a so-called 'Surveillance Database' ('Сторожевой контроль') maintained by the police. A few weeks later, at the beginning of May, regional police departments around the country were alerted that protest rallies were being planned by several opposition organisations to coincide with the EU–Russia Summit on 18 May, and police officers were instructed to detect and stop all members of such organisations travelling to Samara between 8 May and 20 May 2007; officers in airports and train stations were told to separate these travellers from others and dissuade them from continuing to Samara. Shimovolos was such a traveller: after he bought his train ticket from Nizhny Novgorod to Samara, local police departments along his route received telex messages indicating that he was travelling to Samara to take part in an opposition event and that he might be carrying extremist literature.[2] Because he was carrying no luggage, police could not invoke the ruse of searching for extremist literature; instead, he was repeatedly detained and questioned during his journey. But the information in the 'Surveillance Database' followed Shimovolos long after the Samara summit. More than a year later, in October 2008, Shimovolos was detained on a train while travelling to Moscow. The police checked his passport and then carried out an extensive search, first of his luggage, then of his compartment, and finally of the whole carriage, with officers even opening the carriage wall panels – an inspection that delayed the train by half an hour.

Although the orders creating and governing the functioning of Russia's domestic surveillance databases remain secret, Shimovolos's litigation before the ECtHR illuminated some crucial details about how those databases came into being, and how they operate. In those proceedings, the Russian government admitted that since around 2000 the internal affairs authorities of the Russian Federation had been using a 'Search-Highway' ('Розыск-магистраль') database that included persons on the Interpol wanted fugitives list; foreign nationals suspected of criminal offences committed in Russian territory; foreign nationals whose entry into the Russian Federation was prohibited or restricted; persons suspected of a variety of offences ranging from murder and terrorist acts to drug trafficking, antiquities smuggling and financial crimes; leaders and members of organised criminal groups; and leaders of ethnic communities. The order governing the creation and functioning of that database was never published. In 2005 the Russian government expanded the 'Search-Highway' database to include a database of potential extremists code-named the 'Surveillance Database' ('Сторожевой контроль'). In an affidavit submitted to the ECtHR, an officer of the Interior Department of the Russian Federation declared that the decision to register a person's name in the 'Surveillance Database' is made by the Ministry of the Interior or its regional departments on the basis of confidential information.

According to various sources, the 'Surveillance Database' includes the names of 3,800 to 6,500 persons, some of them representatives of far-right and nationalist organisations, and some of them political and civil rights activists. Shimovolos was listed in the section entitled 'Human Rights Activists.' Pressed to substantiate the legitimacy of including Shimovolos in the database, Russian authorities submitted that he had been one of the founders of the Russian-Chechen Friendship Society, and also published the newspaper Human Rights Defence (Правозащита).

On 21 June 2011, four years after the Samara summit, the ECtHR declared that the 'Surveillance Database,' functioning without minimum safeguards to prevent abuse, did not meet international due process and privacy standards and, more specifically, that the registration of Sergey Shimovolos's name in the database (which enabled the collection of information about his movements by train or air within Russia) violated Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, which guarantees the right to respect for a person's private and family life. The ECtHR likewise concluded that the unlawful detention of Shimovolos at the police station in Samara had violated his right to liberty and security.

Shortly after this ECtHR decision, in an interview with Gazeta.ru, Sergey Shimovolos reflected on the trail of clues he had followed in his pursuit of the truth about the Russian government's clandestine surveillance databases:

At my insistence the Samara police officers drew up a detention statement where they wrote that they had instructions for operational search, i.e. there had been a telephone message regarding me. That was a lead, and then (the) investigation started, which continued for two years. I addressed the prosecutor's office to initiate a criminal action against the FSB. In the investigation materials it was noted that 'a database' existed, in which I had been registered on suspicion of organising the Marches of Dissent. That means establishing a special regime of collecting information about a certain person, about his/her movements, his/her communications with the government authorities, the State Road Traffic Safety Inspection – with any institutions. A personal file is created. All that goes along with applying preventive measures towards the person suspected of extremism: s/he has to be captured, warned; explanations have to be demanded of him/her. Without a doubt all that is illegal.[3]

Interestingly, after the European Court's judgment was issued in Shimovolos's case, representatives of the

Anti-government demonstrators shout slogans during a protest in Samara, Russia, on 18 May 2007. Scores of anti-government protesters marched through the Russian city in a demonstration timed to coincide with a tense Russia-European Union summit.
Photo: Sergey Ponomarev/AP

Ministry of the Interior tried to deny that any such special 'Surveillance Database' existed. The Interfax Agency quoted a ministry representative as stating there was no provision for any database under that name in the regulations of the Ministry of the Interior. He did, however, acknowledge that police officers did use such a term in their operational practice and that 'it might sometimes be misinterpreted by citizens.'[4]

the context

The 'Surveillance Database' is just one of the components of an integrated surveillance system that enables Russian authorities to monitor the movement and communications of 'suspicious' persons, all in the name of an extremely broadly defined fight against extremism. Under a federal law entitled 'Counteraction of Extremist Activities,' which was enacted on 25 July 2002 and remains in force today, 'extremism' includes not only committing hate crimes and forcibly threatening the constitutional system, but also inciting enmity towards social groups, accusing officials of extremist crimes, and preventing the legitimate activities of government authorities.[5]

In September 2008, a special department was set up within the Ministry of the Interior to fight extremism, and counterextremism centres were established within each regional department of the ministry. These so-called 'E' Centres were modelled on former departments for fighting organised crime, and in many respects they adopted the same methods. By treating government opponents as lawbreakers and bringing sophisticated operational and investigative apparatus to bear against them, the 'E' Centres became a major tool for political spying in Russia.

Search and surveillance procedures are regulated under the 1995 Operational-Search Activities law, which governs a full range of operations including monitoring targets, tracking postal items and telecommunications, accessing and downloading digital information and communications, and the strategic infiltration of targeted groups. As a rule these operational activities can be conducted only within initiated criminal proceedings, and for activities potentially infringing on citizens' constitutional rights, a court order is required. But the legislation's lack of clear guarantees for the rights of citizens combined with the laxity and inefficiency of judicial review open the way for the operational-

Garry Kasparov speaks to the media at Moscow's Sheremetyevo airport on 18 May 2007. Police prevented Russian chess champion and opposition leader Kasparov from boarding a flight on that day to the city of Samara, where he planned to take part in a protest march coinciding with a Russia-EU summit, an aide said.
Photo: Misha Japaridze/AP

search system to be used as a tool for the surveillance of members of the opposition, political activists and rights advocates. Many of these weaknesses came to light when Roman Zakharov, the director of the Saint Petersburg regional centre for the Glasnost Defence Foundation, suspected that his mobile telephone calls were being intercepted and brought a case against the Russian government in the ECtHR. Although Zakharov was unable to prove that his telephone calls had been intercepted, the court found that the operational procedures governing the interception of telephone calls violated Article 8 of the European Convention on Human Rights. In its December 2015 opinion, the court identified a wide range of fundamental shortcomings in the Russian legislation that allow the security services and police to circumvent the warrant requirements and intercept any communications without obtaining prior judicial authorisation.

In the first place, the court found, the Russian legislation does not sufficiently narrow the list of persons whose telephone communications may be intercepted. Potential targets are not limited to persons suspected or accused of criminal offences, for example, but can also include any person who could have information about a criminal offence or any other information that could be relevant to a criminal case. Moreover, the court found, the Operational-Search Activities Act provides that telephone and other communications can be intercepted based on information about a wide and poorly defined range of events or activities that are said to endanger the national, military, economic or ecological security of Russia.

Second, the court learned, although security services are nominally obligated to obtain judicial authorisation prior to interception, the security services had no obligation to present the interception authorisation to the mobile network operator. This loophole essentially gave law enforcement authorities direct access to all mobile telephone communications and related communications data.

Third, under the legislation, even when a court grants a warrant for interception, it has no jurisdiction to supervise its implementation. The court is not informed of the results of the surveillance, and has no power to review whether the security services or police complied with the terms or requirements of the court order.

Finally, the court found that law enforcement was making prolific use of these surveillance powers, with very little resistance from the courts. According

> “In September 2008, a special department was set up within the Ministry of the Interior to fight extremism, and counterextremism centres were established within each regional department of the ministry (…) By treating government opponents as lawbreakers and bringing sophisticated operational and investigative apparatus to bear against them, the ‘E’ Centres became a major tool for political spying in Russia.”

to data released by the Judicial Department at the Supreme Court of the Russian Federation, in the period between 2007 and 2015, Russian courts of general jurisdiction considered 4,659,325 requests to monitor and intercept telephone or other communications, and approved 4,517,515, or 96.96%, of these requests.[6] Moreover, in each year during that period the number of such requests had increased, with the highest rate of increase relating to requests for operational-search activities outside or prior to the opening of formal criminal proceedings. With at least two people implicated in every one of those surveillance requests, that data suggests that in the past nine years a minimum of nine million people in the Russian Federation, or 6% of the population, might have had their calls or communications intercepted with a court authorisation. And considering that the European Court found in the Zakharov case a general lack of control on the access that law enforcement officials have to the surveillance apparatus, it is likely many more people had their calls and communications monitored with no court authorisation or oversight whatsoever.

For civil rights activists and human rights advocates in Russia, surveillance can include not just having their movements tracked and their mobile phone conversations monitored but also having their daily activities subjected to secret video and audio recordings.

On 14 August 2009 staff members at Agora Association discovered a hidden camera with a microphone in Agora’s offices that had been recording video and audio of conversations among the organisation’s leaders and visitors for an undetermined period. Agora’s requests to authorities to launch a criminal investigation of the illegal monitoring were refused.[7] Similarly, in August 2012 a hidden camera and a ‘bug’ were discovered in the office of the Anti-Corruption Fund of opposition politician Alexey Navalny.[8]

In February 2012 a video of the private life of politician Vladimir Ryzhkov, which had been recorded with a hidden camera, was uploaded onto the internet. In March 2016 a video of the private life of another politician, Mikhail Kasyanov, which was again filmed with a hidden camera, was shown on the national television channel NTV. Both videos contained scenes of intimate relationships and had clearly been made with the aim of exposing those persons in public.[9]

In all these cases there was no direct evidence that the videos were made by law enforcement. However, there are some indications that point in this direction. For example, the lawyers of Agora got an expert opinion that the camera and the microphone discovered in their offices were included in the list of special equipment for secret obtention of information, which can be used

> “[I]n the period between 2007 and 2015, Russian courts of general jurisdiction considered 4,659,325 requests to monitor and intercept telephone or other communications, and approved 4,517,515, or 96.96%, of these requests.”

only by state agencies. A month after the camera was found, a criminal case against Agora itself was opened on accusations of tax evasion. The case was later dismissed.

And on 5 October 2012 national television channel NTV showed the film ‘An anatomy of protest – 2,’ which contained hidden camera footage of a meeting of the Moscow-based opposition organisers Sergey Udaltsov, Leonid Razvozzhaev and Konstantin Lebedev and the Georgian politician Givi Targamadze. The filmmakers alleged that the footage showed the group discussing the organisation of civil riots and foreign financing for the opposition movement.[10] Udaltsov, Razvozzhaev and Lebedev were subsequently found guilty of organising riots and were sentenced to long prison terms.

Invasions of the privacy of opposition leaders and activists have also included the perlustration of email and other digital correspondence. In December 2011, immediately after the parliamentary elections that produced mass protests in Moscow and other cities of Russia, a pro-government media outlet published excerpts of the correspondence of the officers of the leading non-governmental organisation Golos, which independently monitored the election process. The media outlet announced it had obtained 60 megabytes of private electronic correspondence that revealed the financing of activities aimed at discrediting the elections in Russia.[11] Liliya Shibanova, executive director of Golos, publicly protested that the correspondence had been ‘taken from the mailbox’ of her deputy, Grigoriy Melkonyants, that he had often sent messages from his email account on her instructions, and that ‘hacking somebody else’s email account is a violation of law.’[12] Melkonyants himself reported that his email account was hacked on 5 December 2011 just before a press conference on the State Duma elections. As when Agora sought legal redress for the bugging of its offices, law enforcement authorities refused all calls by Golos for an investigation.

Despite the lack of direct evidence of government-ordered hacking, the consistent refusal to investigate the attacks against civic activists, journalists and human rights defenders arouses serious suspicions. In April 2013 human rights lawyer Marina Dubrovina, by submitting an order of client’s interest representation to the investigating officer at the FSB Department for Krasnodar region, was able to learn that her telephone calls were being intercepted and her email account was hacked. This followed the May 2012 hacking of the email, Skype and Facebook accounts of three other human rights lawyers: Voronezh-based Olga Gnezdilova, Saint Petersburg-based Dmitriy Dinze, and Svetlana Sidorkina from Moscow. Although crime incident reports were filed in all of these cases, none of the hackers or the organisers of the hacking attacks have been found or brought to justice.[13]

Anti-government demonstrators shout slogans during a protest in Samara, Russia, on 18 May 2007.
Photo: Sergey Ponomarev/AP

Meanwhile, information gathered through this shadowy email surveillance has been used in the prosecution of political and human rights activities. In the summer of 2015 the police detained four members of an action group that was demanding a referendum 'for a responsible government,' advocating amendments to the Constitution, and promoting an ethics law for high-ranking officials of the Russian Federation. Publicist Yuriy Muhin, Air Force reserve officer Kiril Barabash, system administrator Valeriy Parfenov and RBC journalist Alexander Sokolov were charged with involvement in the activities of an extremist organisation.[14] A key piece of prosecution evidence was the Gmail correspondence among the defendants, which was delivered to the investigation officers by an agent who had infiltrated the group and was included in the list of email recipients.

And as with clandestine video and audio recordings, the surveillance of private emails and other digital correspondence has been used specifically to discredit human and civil rights defenders. In March 2016, as part of an operation clearly intended to smear Igor Kalyapin, who heads the Committee for the Prevention of Torture and often works in Chechnya, the local TV channel showed his SMS communications. The text messages, dating back to November 2014, had clearly been obtained by law enforcement authorities in the course of their operational activities.[15]

Similarly, in March 2016 the national television broadcaster Channel Five (Pyatiy Kanal) showed two short films about the activities of the civil rights defence group Komanda-29, which specialises in defending people accused of high treason and dealing with matters related to divulging state secrets. Both films accused lawyers of Komanda-29 of working on behalf of other countries, offering as evidence their documents and email correspondence. According to Ivan Pavlov, director of Komanda-29, the information had been obtained as a result of email perlustration.[16]

conclusion

When in 2007 Sergey Shimovolos stepped off the train in Samara station and into police custody, he did not know that as early as 2005 Russian authorities had been developing an integrated monitoring system that would be used to target political activists and civil rights defenders and advocates. In the years since Shimovolos was told he was in 'the database,' this surveillance

system has only been expanded. Challenges brought by Shimovolos and many other activists and organisations over the last ten years have revealed a surveillance system that includes the monitoring of individuals' movements within the Russian Federation and at border crossings; interception of telephone communications; secret audio and video recordings; and the perlustration of email correspondence and hacking of internet service accounts. As these powers have grown, they have increasingly been used to monitor and discredit those whom the government brands 'the fifth column' and 'national traitors.'

In fact, the cases described above show how, in the absence of public and judicial control, a surveillance system formally established to counteract and investigate crime can become a tool for political persecution. And those who find themselves the target of this system have little recourse in Russia: not a single case involving the unwarranted interception of email, mail or telephone communications, the monitoring of social networks and internet activity, covert audio and video recording, or physical surveillance has led to legal proceedings or punishment of the culprits. In any society, such unfettered surveillance powers are likely to have a chilling effect on dissenting voices and civil society organisations; even more so when they are coupled, as has been the case in Russia recently, with efforts by authorities to criminalise a wide range of civic and political activities.

The fact that this is occurring in Russia, which never fully shed the structures of the Soviet surveillance state, poses particular challenges to confronting this new wave of uncontrolled and arbitrary surveillance over millions of Russian residents. In many countries, Edward Snowden's revelations sparked serious reflection and debate about the limits of state intrusion into private and family life. Not so in Russia. In fact, even though Snowden was granted provisional asylum in Russia in July 2013, in a poll conducted by the Public Opinion Foundation 41% of Russians confessed that they had never heard of Snowden or his revelations. And reports of specific cases of politically motivated surveillance in Russia are often met with a shrug, a legacy of the Soviet era that was characterised by the attitudes that 'we all are under surveillance' and 'I have nothing to hide.' Even recent information about how much of the personal information on property, health status, personal documents and communications, travel and financial transactions that is in state-controlled databases is also now available on the black market has done little to change these deeply rooted attitudes. But when a government collects more and more personal data and yet does not have the will to store it securely, it is no longer just the government's political opponents who should be worried about its prying eyes.

notes

-

1. All travellers from Moscow to Samara on the eve of the summit were under suspicion. Some people were detained. See NEWSru.com, 17 May 2007: http://www.newsru.com/russia/17may2007/samara_zaderj.html
2. A 2001 law enacted by the Russian Federation mandated that train tickets could be sold only on the presentation of a valid passport and with the registration of the traveller's personal data. In 2004 that requirement was extended to air travel, and in 2012 to interregional bus service. Thus, whenever anyone travelling in Russia buys a domestic ticket, his or her travel plans and personal information become available to authorities. For Shimovolos and other human rights activists, as well as for opposition figures and journalists, the requirements mean they often are forced to cancel and rebook tickets at the last minute in the hopes that they can reach their destination without detention or interruption.
3. 'Strasbourg admitted the existence of "black lists,"' by Alexandra Koshkina, Gazeta.ru (21 June 2011). Available at: http://bit.ly/22VFxPP
4. 'MI denied the Surveillance Database's existence,' by Anna Pushkarskaya, Kommersant (23 June 2011). Available at: http://www.kommersant.ru/doc/1664976
5. Federal Law No114-FZ. Available at: http://bit.ly/1TnrrRa
6. Available at: http://www.cdep.ru/index.php?id=79
7. 'The court found the order of search in Agora Association legal,' Open Information Agency (18 August 2009). Available at: http://openinform.ru/news/pursuit/19.08.2009/13402/
8. 'One more interception device and a hidden camera were found in Navalny's office,' Radio Svoboda (6 August 2012). Available at: http://bit.ly/1SrW7vN
9. 'The TV channel NTV showed hidden camera footage of opposition leaders,' RBC (1 April 2016). Available at: http://bit.ly/1M9pFlf
10. '"An anatomy of protest – 2": NTV suspects S. Udaltsov of high treason,' RBC (5 October 2012). Available at: http://www.rbc.ru/politics/05/10/2012/673004.shtml
11. 'Life News published the correspondence between "Golos" and US Department of State,' Lifenews.ru (8 December 2011). Available at: http://lifenews.ru/news/76604
12. '"Golos" will refer the matter to court,' Interfax (9 December 2011). Available at: http://www.interfax.ru/russia/220999
13. 'How the work of lawyers in Russia is obstructed. A report by rights defenders,' Novaya Gazeta (23 September 2013). Available at: http://bit.ly/23ahARu
14. 'The IGPR "ZOV" case' (of the referendum action group), Memorial human rights centre (29 October 2015). Available at: http://bit.ly/1M9per4
15. Report by Chechnya State Radio and TV Channel Grozni (16 March 2016). Available at: http://bit.ly/1oum6L7
16. Report by Channel Five (6 March 2016). Available at: http://bit.ly/1MNngwJ

Surveillance at a glance in Russia

Do citizens know more now than they did three years ago about the government's surveillance activities?
No

Did the Snowden disclosures lead to meaningful public debate in your country about the proper limits on government surveillance?
Russians do not appear to care about the Snowden disclosures at all. The discussion on the Snowden case focused primarily on the relationship between Russia and the United States and the decision to grant asylum.

Since the Snowden disclosures, have any whistleblowers come forward to inform the public about government surveillance activities?
No

In the last three years, have the government's national-security surveillance authorities been narrowed, expanded, or neither?
Expanded

In the last three years, have new structural checks (e.g. new transparency requirements) been imposed on intelligence agencies?
No, despite the European Court of Human Rights' judgment in the *Roman Zakharov v. Russia* case

If the legislature/parliament is considering new legislation relating to government surveillance, would that legislation narrow the government's surveillance powers or expand them?
Expand them. Since 2012 the Russian parliament has adopted dozens of laws that limit civil rights and freedoms.

If the legislature/parliament is considering new legislation relating to government surveillance, would that legislation impose new structural checks?
No. In the Russian parliament there is no political party that focuses on controlling the security services.

Over the last three years, have the government's national-security surveillance authorities been the subject of domestic litigation, including in constitutional courts?
No

Over the last three years, have the courts rejected as incompatible with constitutional or human rights law any aspect of government surveillance?
Yes. On 22 March 2016, one of Moscow's district courts dismissed the decision to fine a company called Yandex for having refused to provide the Federal Customs Service with its users' personal data, including electronic messages.

Over the last three years, do you think the public has come to trust the intelligence agencies more, less, or neither?
More. Between 2013 and 2015 the number of those who trust the state security service increased from 36% to 50%.

The Re (X) case and the invisible subjects of digital surveillance

4
CANADA

Canadian Federal Court Judge Richard Mosley.
Photo: Couvrette/Ottawa

CANADA

The Re (X) case and the invisible subjects of digital surveillance

the case

Near the end of 2013, Canadian federal court judge Richard Mosley issued a public judgment that rocked Canada's secretive national security community.

Four years before, in 2009, the Canadian Security Intelligence Service (CSIS) appeared in an *ex parte* secret hearing before Justice Mosley to seek permission to intercept and monitor the electronic communications of two Canadian citizens. CSIS already had a warrant to watch the two inside Canada; now the service was asking to be able to work with the Canadian Security Establishment (CSE), Canada's signals intelligence agency, to monitor them when they were outside the country. Normally the CSE is not legally allowed to intercept the communications of Canadians, but under what is called an 'assistance mandate,' it can use its equipment and expertise to surveil Canadians in the course of helping another agency with an authorised investigation. Courts had shown some wariness in approving such joint CSE-CSIS operations. A previous attempt to secure a warrant for an overseas operation had been rejected on the grounds that the CSIS Act, which defines the scope of CSIS's activities and powers, does not authorise security intelligence investigations overseas, particularly investigations that might, because of their intrusive nature, violate the laws of other countries.[1] But before Justice Mosley, CSIS argued that this application was different: in this case, the surveillance of the two targets would be carried out and controlled from inside Canada, meaning that information gathered by the surveillance would be subject to legal safeguards. Justice Mosley explicitly granted the warrant on this assurance, and for at least a year CSIS carried out electronic surveillance of these two individuals.

We still do not know who these 'suspects' were: not their names, or their gender, or any other details about their lives. We also do not know the nature of their actions, which were apparently deemed sufficiently suspicious to secure the domestic warrant in the first place. The secret nature of national security warrant cases means that the subjects are invisible. The process takes place in such secrecy that those who are surveilled will likely never know they have been targeted. And, unlike in surveillance related to criminal investigations, there is no requirement that anyone outside of these hidden proceedings ever be told that the spying occurred. Put simply, Canadians rarely know who is being subjected to electronic surveillance, or why.

To secure a warrant like the one it was seeking from Justice Mosley, CSIS has to convince the court that its planned surveillance operation is necessary and proportionate and that it will be carried out in compliance with the law, including the Canadian Charter of Rights and Freedoms. But because the proceedings are secret, and because there is little outside scrutiny or oversight, justices who hear these applications are dependent on the information the security services provide – and they are entirely unable to assess whether there is information being withheld by those same services. Justice Mosley granted the warrant application in 2009 to surveil the two suspects outside of Canada because he was persuaded that, by ensuring the surveillance was collected and controlled from within Canada, CSIS and CSE would be able to ensure that the private communications of Canadians they intercepted would be used only if they were essential for national security purposes. It was an important precedent for the CSIS: over the next four years the Federal Court issued 35 similar warrants based on Judge Mosley's decision.[2]

Then, in June 2013, Justice Mosley read something that he found alarming.

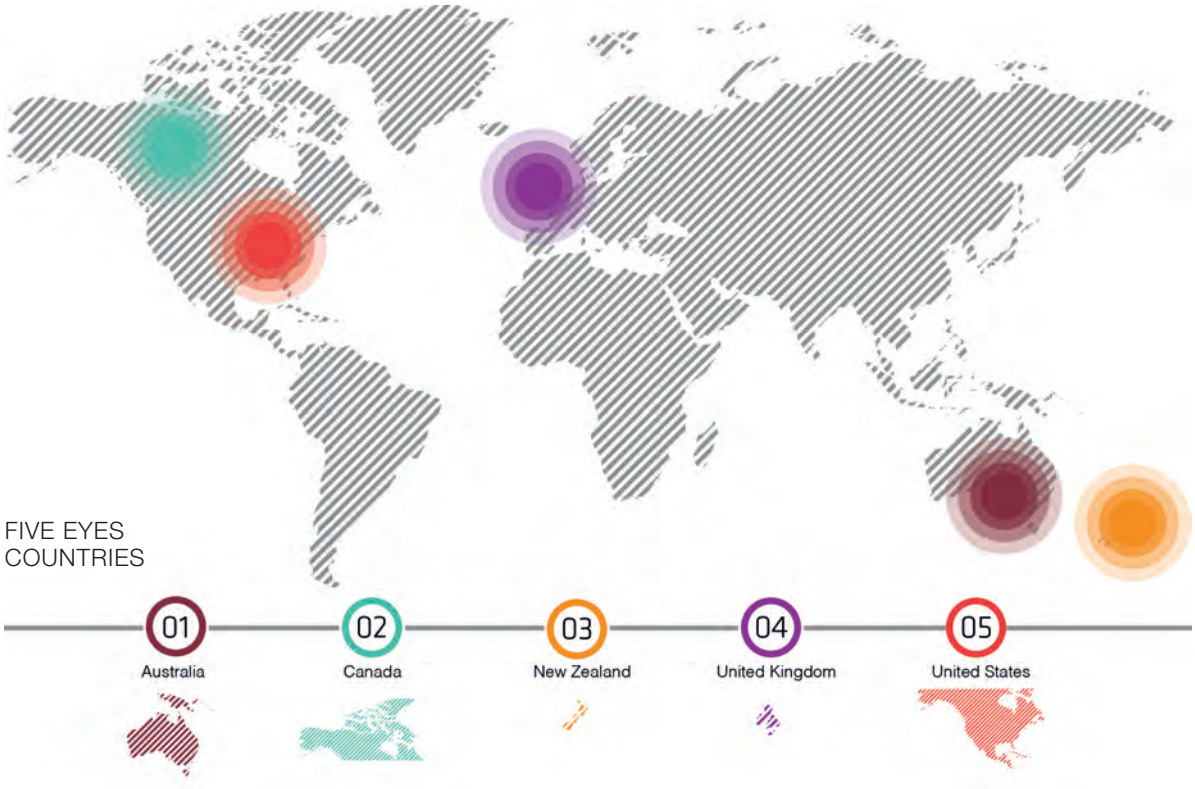
Every year the CSE is reviewed by the CSE commissioner, usually a retired judge who is appointed to examine the activities of the CSE to assess whether they comply with the law and to investigate any complaints against the agency. The CSE commissioner writes a report about

> “Justice Mosley issued a blunt, public judgment in the case that had become known as Re (X), declaring emphatically that the Canadian Security Intelligence Service had committed ‘a breach of the duty of candour owed by the service and their legal advisors to the court.’”

this review. The public version of the commissioner’s report is extremely circumspect and carefully worded to reveal very little about the actual workings of the CSE, and it seldom attracts attention beyond a small circle of scholars and policy watchers. But for Justice Mosley, something jumped out: in a discussion of the particular type of warrant that he had approved, the commissioner recommended that CSE tell its CSIS partner to ‘provide the Federal Court of Canada with certain additional evidence about the nature and extent of the assistance CSE may provide to CSIS.’[3]

The recommendation raised a red flag for Justice Mosley: it suggested that there was something the court – and by extension, he himself – needed to know about how the warrants he had initially granted were being used. So he took the rare step of calling lawyers for CSIS and CSE to reappear before him and to explain what exactly was going on. He specifically wanted to know if there was information or evidence that had been withheld from him during the warrant application, and whether it would have made a difference to his decision to issue the warrant and allow the surveillance.

Since such proceedings are also secret, we don’t know all of the details of that encounter, or of the subsequent hearings that Justice Mosley requested based on what he learned that day. However, a redacted, publicly released version of a document summarising those proceedings revealed that the CSE wasn’t the only agency collecting information on the two individuals under surveillance; it had asked its counterparts in other agencies, its Five Eyes allies, to help carry out the digital electronic surveillance. This clearly violated the letter and spirit of the CSE’s original assurances. The warrant was granted under the specific understanding that CSIS and CSE would control the information about these Canadian targets, and that the information they gathered about these Canadians would stay in Canada. That assurance was crucial. When information is collected and held in Canada, it is protected



by Canadian laws and used only for Canadian interests. When it is collected by others, there are no such protections. There are agreements – again, completely secret – between allies that are said to regulate this kind of information collection and sharing, but there is no guarantee that these agreements will be upheld if another country decides it is of national interest to use the information it collects in these joint operations for its own purposes.

The document also revealed that the failure of CSIS and CSE to mention their intention to ask for help from allies was not inadvertent. Rather, the CSE employee who appeared before the judge explicitly admitted that his initial submission was carefully 'crafted' with legal counsel to leave out mention of second parties who might be asked to help with the surveillance.

Near the end of 2013, Justice Mosley issued a blunt, public judgment in the case that had become known as Re (X), declaring emphatically that the Canadian Security Intelligence Service had committed 'a breach of the duty of candour owed by the service and their legal advisors to the court.' Decrying the service's deception, Justice Mosley wrote, 'The Court must be concerned that the authority granted it by Parliament to authorise intrusive investigative activities by the Service may be perceived in the public arena as approving the surveillance and interception of the communications of Canadian persons by foreign agencies.'[4]

The government appealed Justice Mosley's decision, but the Federal Court of Appeal upheld his judgment in July 2014. CSIS prepared to take its case to the Supreme Court of Canada, saying that 'CSIS must be able to carry out its crucial role in gathering intelligence on threats to the security of Canada confident that they are acting within the law, and the public is also entitled to know what constraints are imposed on CSIS in this regard.' The Canadian Civil Liberties Association (CCLA) prepared to move for leave to intervene in this appeal in the public interest. But in 2015 the Canadian Parliament passed two bills, C-51 and C-44, explicitly granting the CSIS greater powers to conduct surveillance outside Canada. With many of the crucial legal questions rendered moot by the new laws, the government dropped its Supreme Court appeal of Re (X), which stands, in the end, as a rare government defeat and an even rarer opportunity for public scrutiny of national security surveillance practices in Canada.

the context

Through the efforts of Edward Snowden and other whistleblowers, we have a great deal more information than we once had about the capacities of Canada's intelligence agencies and the ways the Canadian national security apparatus works with the United States, the United Kingdom, Australia and New Zealand – its international partners in the 'Five Eyes' alliance. We

Maher Arar bows his head at a news conference discussing the government's apology and compensation package, in Ottawa, on 26 January 2007. Arar was wrongfully deported to, detained, and tortured in Syria.
Photo: Tom Hanson/AP

know, for example, from a top-secret memo released by Snowden that CSE offers 'unique geographic access to areas unavailable to the US' and has 'opened covert sites at the request of the NSA.' The NSA, in turn, shares technology for 'state-of-the-art collection, processing and analytic efforts and [Information Assurance] capabilities.'[5] By one estimate, participation in the Five Eyes gives Canada access to 'a [CAN] $15 billion global partnership,' greatly expanding Canada's surveillance capabilities.[6]

The more we know about the technical capabilities of the Canadian intelligence services and their Five Eyes partners, the more likely it seems that information sharing across borders may be used to circumvent Canadian law. While CSIS cannot target and access Canadians' communications within Canada without a warrant,[7] and CSE is prohibited from directing its activities at Canadians with few exceptions,[8] these agencies' allies have no such prohibitions in their laws against surveilling Canadians. To the contrary, foreign communications are the typical target of intelligence surveillance, and there have been suspicions, and occasionally evidence, that allies collect information on one another's citizens intentionally and then find ways to share it – as when, as The Guardian newspaper has reported, British intelligence has voluntarily shared information collected via the 'Tempora' programme with the NSA.[9]

The Canadian government insists that agreements among the spying partners prohibit these kinds of arrangements, but there is insufficient transparency for anyone to trust these assurances, and it seems unlikely that Canada could remain entirely disengaged from activities practised among its closest allies. In fact, then CSE Commissioner Robert Décary explicitly stated in a recently declassified report that he cannot determine whether or not the Five Eyes partners keep their promises to protect information about Canadians. What he found was that beyond 'certain general statements and assurances' between CSE and its partners, he was 'unable to assess the extent' to which the Five Eyes partners 'follow the agreements with CSE and protect private communications and information about Canadians in what CSE shares with the partners.'[10]

Canadians have ample reason to fear intelligence sharing among the Five Eyes partners. In September 2002 Maher Arar, a dual Syrian-Canadian citizen, was intercepted at JFK airport in New York on his way home to Canada from a family vacation. He was initially detained in the United States under suspicion that he belonged to Al Qaeda, and he was subsequently rendered by the United States to Syria, where he was tortured. A Commission of Inquiry in Canada determined that he was an innocent victim and that inaccurate intelligence reports and communications that Canadian intelligence services shared with the United States without proper checks or caveats led to the mistake. Moreover, by

A vehicle passes a sign outside the Canadian Security Intelligence Service (CSIS) headquarters in Ottawa on 5 November 2014.
Photo: Reuters/Latinstock

turning the information over to the United States, Canadian intelligence had lost control both of the information and of the ability to influence the actions of its partner. Canada eventually apologised to Maher Arar and made a substantial financial settlement for its complicity in his rendition and torture, but no apology and no amount of money can repair the damage done to his life.

The most gripping surveillance stories are about individuals – real, specific people with families, friends, jobs – who have personal experience with being surveilled and who can talk about the effects that surveillance has had on their lives, about the travel or job opportunities lost, about relatives implicated or threatened, and about the sense of violation and fear engendered by being watched. They are stories that show the profound human cost of laws and practices that subvert individual rights in the name of national security. They are also usually stories that come to light because the individuals figured out that they were being watched, often because the information gained by the watchers was used in a way that caused these people harm – by landing on a no-fly list, or being turned back from a border crossing, or in extreme cases like that of Maher Arar, experiencing rendition and torture.

But the Re (X) case reminds us that there are many people out there who never know that they are being watched, never know that their privacy is being so profoundly invaded, and, in the end, may never be detained or charged with a terrorist offence. There are quite likely many, many cases in which surveillance is mistaken or unjustified – or, as in the Re (X) case, it is carried out under warrants secured based on manipulated facts – that garner no attention and engender no protest because those who are surveilled remain invisible.

Edward Snowden has described Canada's mechanisms for regulating and controlling surveillance by its intelligence agencies as 'one of the weakest oversight frameworks of any Western intelligence agency in the world.'[11] Had it not been for one justice who stood up for the integrity of the secret warrant process, Canadians would still not know that two of their fellow citizens had been swept up in the web of transnational digital surveillance. Justice Mosley knew to review his decision to issue the warrant only because he studied the CSE commissioner's annual report, in which the CSE commissioner hinted that there was something about the way CSE was assisting CSIS that the Federal Court needed to know. By then, four years had elapsed since he issued the original warrant, and that warrant, secured based on misleading information, had served as precedent for securing many other similar warrants.

> “Re (X) reminds us that the secrecy that intelligence agencies require to do their jobs must be complemented with appropriate accountability mechanisms to protect people from abuses and mistakes.”

conclusion

Justice Mosley stood up for the law and the Canadian people who are protected by it. His courage and initiative helped make visible, and safeguard, some of the invisible subjects of security surveillance.

Unfortunately, knowledge has not equalled reform in Canada. Rather than responding to the Re (X) case and the issues it raises by reviewing and restricting the legal authority for Canadian security agencies and agents to act outside of Canada, the Canadian government has passed two bills, C-44 and C-51, which broaden intelligence agency mandates.

C-51, the more sweeping of these measures, was introduced in January 2015 and received royal assent in June, a remarkably swift progression for an omnibus bill that makes such a wide range of changes to Canada’s national security law. In particular, in terms of surveillance, C-51 allows an exponential increase in information sharing across government agencies and institutions and potentially with foreign powers as well, without strengthening accountability measures. It also gives CSIS new powers to take covert action, even action that goes against international laws, again, with no additional oversight. That the bill passed so rapidly is disconcerting given the intensity of the reservations and criticisms raised not just by civil society but by privacy, legal and civil rights experts, prominent civil servants, academics, former Supreme Court justices and former Canadian prime ministers – and given the fact that public support swung from a majority in favour when the bill was introduced, to a majority opposed as more information about the specific features of the new law became known. CCLA was active in the debates around C-51, arguing that it is fundamentally flawed and, in specific sections, unconstitutional, and that there is no evidence that the broad changes it makes to a range of intelligence powers – including expanded possibilities for surveillance – are even needed.[12] CCLA is now concentrating on preventing this legislation from being used to deprive people of their rights, as protected in our Charter of Rights and Freedoms, and has filed an application with the Ontario Superior Court to have certain provisions of the 2015 Anti-terrorism Act declared unconstitutional.

There should certainly be no expansion of digital surveillance powers and intelligence sharing in Canada without new and more effective structures for oversight. Re (X) reminds us that the secrecy that intelligence agencies require to do their jobs must be complemented with appropriate accountability mechanisms to protect people from abuses and mistakes. Cautiously worded annual reports from agency review bodies, occasionally supplemented by

highly redacted documents obtained by journalists in response to Freedom of Information requests, are simply not enough. Re (X) also highlights the need for courts and other oversight authorities to have sufficient access to information about intelligence operations in general and about specific surveillance requests, in order to test the veracity of statements and claims by security services in surveillance applications. To the extent possible, that information needs to be made publicly available as well to challenge official rhetoric, which often attempts to convince us that the more information is collected and shared, the safer we will be, and to counter it with the warning that it is dangerous for us to share too much with the wrong people. We must ensure that promises that our intelligence agencies act proportionately and legally are backed by strong, appropriate laws governing information collection and sharing. Finally, and ultimately, we must make sure that all of the laws that govern our national security agencies and activities reflect rather than reject our human rights guarantees of due process, privacy and the dignity of every individual.

notes

-

1. For a detailed description of the legal intricacies of the judgments, see Craig Forcese, 'Triple Vision Accountability and the Outsourcing of CSIS Intercepts' (6 December 2013). Available at: http://craigforcese.squarespace.com/national-security-law-blog/2013/12/6/triple-vision-accountability-and-the-outsourcing-of-csis-int.html
2. Security Intelligence Review Committee. 'SIRC Annual Report 2012-2013: Bridging the Gap', p. 18. Available at: http://www.sirc-csars.gc.ca/anrran/2012-2013/index-eng.html
3. Robert Décary. Communications Security Establishment Commissioner: Annual Report 2012-2013. Available at: https://www.ocsec-bccst.gc.ca/s21/s46/s18/eng/2012-2013-annual-report. Note that the Canadian Security Establishment (CSE) was at that time called the Canadian Security Establishment Canada (CSEC).
4. 2013 FC 1275, at para 97.
5. National Security Agency/Central Security Service information paper, 'NSA Intelligence Relationship with Canada's 'Communications Security Establishment Canada (CSEC)' (2013'). Available from the Snowden Archive at: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH1ee3.dir/doc.pdf
6. Canada, Parliament, Senate, Standing Senate Committee on National Security and Defence [SSCNSD] (2012). Transcript of Proceedings. 41st Parl., 1st sess. Meeting No. 15. Available at: http://www.parl.gc.ca/Content/SEN/Committee/411/secd/10ev-49784-e.htm?Language=E&Parl=41&Ses=1&comm_id=76
7. Canadian Security Intelligence Service Act (R.S.C., 1985, c. C-23), Section 21. Available at: http://laws.justice.gc.ca/eng/acts/C-23/
8. National Defence Act (R.S.C., 1985, c. N-5), Section 273.64 (2)(a). Available at: http://laws.justice.gc.ca/eng/acts/n-5/fulltext.html
9. 'GCHQ taps fibre-optic cables for secret access to world's communications,' The Guardian (21 June 2013). Available at: http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa
10. 'CSEC commissioner calls for safeguards on Five Eyes data sharing,' The Canadian Press (14 July 2014). Available at: http://www.cbc.ca/news/politics/csec-commissioner-calls-for-safeguards-on-five-eyes-data-sharing-1.2706911
11. Edward Snowden. CBC News video interview (4 March 2015). Available at: http://www.cbc.ca/news/canada/edward-snowden-says-canadian-spying-has-weakest-oversight-in-western-world-1.2981051
12. In support of CCLA around the debates on C-51, eight members of INCLO signed a joint letter that was presented to the Senate Committee on 23 April, to show international support for CCLA's position and to emphasise the importance of international human rights law and privacy rights in global counterterror initiatives.

Surveillance at a glance in Canada

Do citizens know more now than they did three years ago about the government's surveillance activities?

Yes

Did the Snowden disclosures lead to meaningful public debate in your country about the proper limits on government surveillance?

No (academics, civil society and individuals discussed it but government passed legislation expanding surveillance powers)

Since the Snowden disclosures, have any whistleblowers come forward to inform the public about government surveillance activities?

No

In the last three years, have the government's national-security surveillance authorities been narrowed, expanded, or neither?

Expanded

In the last three years, have new structural checks (e.g. new transparency requirements) been imposed on intelligence agencies?

No

If the legislature/parliament is considering new legislation relating to government surveillance, would that legislation narrow the government's surveillance powers or expand them?

The most recent legislation under the previous Canadian government (Bill C-51, the Anti-terrorism Act, 2015) expanded surveillance powers; as of October 2015 we have a new government whose platform suggests they may narrow these powers, but it's not yet entirely clear what they will do as they also supported the original legislation.

If the legislature/parliament is considering new legislation relating to government surveillance, would that legislation impose new structural checks?

Indications are that they will, yes

Over the last three years, have the government's national-security surveillance authorities been the subject of domestic litigation, including in constitutional courts?

Yes

Over the last three years, have the courts rejected as incompatible with constitutional or human rights law any aspect of government surveillance?

No. However, CCLA has an active constitutional challenge filed with the Ontario Superior Court of Justice.

Over the last three years, do you think the public has come to trust the intelligence agencies more, less, or neither?

Less

The AMIA case, the judiciary and the intelligence services

5
ARGENTINA

An image of the ruins left after the bombing of the AMIA in Buenos Aires, on 18 July 1994.
Photo: Julio Menajovsky

ARGENTINA

The AMIA case, the judiciary and the intelligence services

the case

On the morning of 17 July 2015, from a small stage set up in a plaza in downtown Buenos Aires, a man and a woman read out 85 names. After each name, the crowd gathered at the site called out 'present.' In the background, the daily routine around the Argentine Palace of Justice went on as usual, horns honking, office workers rushing in and out of buildings.

Twenty-one years before, at 8.43 am on 18 July 1994 – a day that had begun much like this one – a terrorist bomb blew up the community centre of the Argentine-Israeli Mutual Association (known as AMIA in Spanish). The six-story building crumbled into a mountain of rubble. Eighty-five people lost their lives and 300 were injured: workers, people running errands, passers-by, young and old. Why? By whose hand? How? The official judicial investigation into the most serious terrorist attack in Argentine history has spanned over two decades, and we still don't have the answers.

Even after the return to democracy in Argentina, the State Intelligence Secretariat (SIDE, its acronym in Spanish) and its successor, the Intelligence Secretariat, existed in the shadows, operating covertly; no-one explained what it did, and what exactly it did or did not know. State and para-state agents used false identities. Their agencies collected data on Argentine citizens, in some cases relevant, in others mere gossip, with no oversight whatsoever. They spent their secret budgets with zero accountability, an entire structure devoted to serve political purposes. The agencies tapped the phones of business people, journalists, government officials and opposition members, producing information that politicians used to discredit adversaries, often with the participation of influential journalists and mass media. And when information trafficking wasn't enough, SIDE agents had access to reserve funds for bribes and influence peddling, to bend decisions to their will.

The intelligence agencies also managed to hold sway over the judicial system, particularly during the 1990s. The courts were so dependent on information from the intelligence services that the relationship between the judiciary and the intelligence community became inverted: more than a supporter or collaborator in criminal investigations, the Intelligence Secretariat essentially owned the most significant judicial processes, which included cases involving political or business corruption and felonies involving complex organisations. As in the political sphere, the ties between the intelligence services and the judicial branch were further consolidated through bribes sourced from SIDE reserve funds.

This web of relations linking the political system, the judicial branch, the prosecutor's office and the intelligence system was firmly in place at the time Argentina suffered its two most devastating terrorist attacks: a bombing on 17 March 1992 in which a truck exploded at the Israeli Embassy in Buenos Aires, killing at least 22 people and injuring more than 350, and, two years later, the even deadlier AMIA bombing.

The first judicial investigation of the AMIA attack was handled by federal investigating magistrate Juan José Galeano. In its crucial early months, his work was plagued by irregularities, not least of which was the involvement of the SIDE in the investigation. And by mid-1996, two years after the attack, his investigation had still not yielded any significant findings – nor had a parallel investigation into the Israeli Embassy bombing. The public was growing impatient: starting just after the AMIA bombing, a group called Memoria Activa began gathering every Monday in front of the Palace of Justice to read out the names of the 85 people who died in that attack, and their demand for truth and justice was garnering ever stronger support from the Argentine people. Both Judge Galeano and the government needed a scapegoat.

A few days after the bombing of AMIA, more than 150,000 people assembled in the rain in the Dos Congresos square to condemn the terrorist attack in Buenos Aires, on 21 July 1994.
Photo: Eduardo Longoni

So the judge and the SIDE conspired to construct an explanation based on statements by Carlos Telleldín, a car salesman who had been arrested for being the last registered owner of a van found amid the rubble of the AMIA. Telleldín, in jail since 1994, was accused of having turned the vehicle over to the terrorists, but up until mid-1996, he had not revealed the identity of those people. Information provided by foreign intelligence services to the judicial investigators following the attack suggested that the attack had been orchestrated by the Islamic Republic of Iran. But in July 1996, just a few days before the second anniversary of the attack, Telleldín stated before Judge Galeano that he had given the van to a group of policemen from Buenos Aires province. He told the court that these police officers often extorted him and that he had turned over the vehicle to them in exchange for protection for his illegal enterprise of selling stolen cars. Galeano ordered the arrest of 15 police agents, including Juan José Ribelli, the chief of the Investigation Brigade of the Buenos Aires provincial municipality of Lanús. On the second anniversary of the bombing, with this 'local connection' behind bars, state officials assured Argentine society that the terrorist cell responsible for the bombing had been dismantled. Because the police force in Buenos Aires province was notorious for its violence and ties to illegal networks, the story was believable.

But less than a year later, in April 1997, the Argentine media aired a video recording of a meeting between Judge Galeano and Telleldín. In that video, the two appeared to discuss the purchase of the copyrights to a book that Telleldín was supposedly writing. After the video's release, both denied an allegation that the conversation in fact referred to a payment for Telleldín's last testimony. In late 2001, with Telleldín's statement as the sole evidence, the trial began against the police accused of involvement in the attack of AMIA.

In 2003, nine years after the bombing and during the first days of the Néstor Kirchner administration, a sector of the Intelligence Secretariat disclosed information corroborating that several agents had indeed been part of a bribery operation linked to the AMIA bombing investigation, and that the same day that Telleldín had first accused the police in 1996, intelligence employees had met his wife at a bank. At this time, the government made a key political decision: it issued a decree relieving intelligence agents of their duty to keep their activities a secret, thus freeing them to testify in the ongoing trial that secret money from the intelligence agency had been used to pay Telleldín in exchange for his accusation that the police officers from the province of Buenos Aires had served as the 'local connection' of the attack. The intelligence agents testified that

A man blows the shofar, the ancient Jewish musical horn, during a commemorative act by Memoria Activa in Buenos Aires on 17 July 2015.
Photo: Santiago Cichero

> “The official judicial investigation into the most serious terrorist attack in Argentine history has spanned over two decades, and we still don’t have the answers.”

in July 1996, with the knowledge of then President Carlos Menem and at the request of Judge Galeano, Hugo Anzorreguy, Secretary of Intelligence at the time, ordered his subordinates to deliver USD 400,000 to Telleldín’s wife in payment for her husband’s statement.

The money came from reserve funds that the SIDE administered without any oversight or accountability, and the secret nature of the budget allowed the money to be used to fabricate a story that derailed the investigation of facts for years. But now the consequences of a notoriously common practice – using reserve funds to buy or manufacture information – stood exposed for all to see. The pact between the government, the State Intelligence Secretariat, foreign intelligence agencies, Judge Galeano and Telleldín had produced a false lead in the investigation of the attack, diverting it from legitimate leads and throwing the legitimacy and legality of the entire bombing investigation into question.

Paying a bribe that had been decided at the highest political level was not the only illegality committed during Judge Galeano’s judicial investigation of the AMIA attack. When it came to the facts, the SIDE and a sector of the federal police owned the investigation; intelligence agents carried out searches and witness interrogations, and the judge and the prosecutors endorsed their actions. The SIDE also ventured into wiretapping: for a year it listened in on phones at the Cuban and Iranian embassies in Buenos Aires without a judicial warrant, as well as phone lines belonging to other people under investigation. Though SIDE agents have since admitted they carried out this illegal eavesdropping, the cassette recordings of the conversations never surfaced.

In October 2004, the court in charge of the trial against Telleldín, Ribelli and the other police officers ruled that the accusations against the ‘local connection’ were founded on judicial irregularities, paid statements and the illegal use of state resources. The judges determined that the investigation had not been aimed at discovering the truth, but rather at legitimising a deceit constructed by senior officials of the different branches of state; it was ‘a fabrication at the service of unscrupulous politicians,’ the judges said. All of the accused were acquitted and the court ordered a new investigation, with all of the investigative work done to that point declared null and void. The following year, the prosecutors who had been involved in the investigation resigned and Judge Galeano was removed from the bench for his illegal acts; these former officials are presently standing trial. Ten years had passed since the bombing, and the only response to the demands for justice had been the exposure of a powerful cover-up manoeuvre.

After Judge Galeano was removed from office, President Néstor Kirchner appointed Alberto Nisman to preside as special federal prosecutor over a new investigation. But Nisman was not new to the case: he had been on the initial investigative team that had collaborated with the Intelligence Secretariat, and he too would base much of his investigation on information that Secretariat provided, most of which could not be used as evidence in court. In one such instance, in 2005 Nisman announced that he had identified the suicide driver of the van – a statement that was never backed up or proved in judicial proceedings.

In 2006, two years after taking over the investigation and 12 years after the AMIA bombing, prosecutor Nisman issued an 800-page indictment accusing eight top Iranian ex-officials, including former President Ali Akbar Rafsanjani and former Minister of Intelligence

Ali Fallahian, of orchestrating the attack. A year later INTERPOL issued 'red alert' notices for five of the eight officials indicted, instructing member states to arrest them so they could be sent to Argentina to testify in court.[1] The Iranian government refused to turn its citizens over to the Argentine justice system, creating an impasse in the case that lasted for several years.

Then, in March 2012, the governments of Argentina and Iran signed a Memorandum of Understanding to create a commission that would allow Argentine judges to travel to Tehran to conduct interviews, and possibly even interview the named defendants, but that did not ensure that the defendants would appear before an Argentine court. In the ten years that transpired from the time Nisman took over as special prosecutor in 2004 until late 2014, the investigation had been at a near standstill. However, on 14 January 2015, he filed a complaint alleging that the Memorandum of Understanding was a manoeuvre by Argentine President Cristina Fernández de Kirchner and other officials to cover up the bombing and protect the Iranians. The allegation rested on wiretaps of the phones of people who had no central role in the national political system; the recorded conversations allegedly implied a deal to benefit the Iranians. Nisman was scheduled to appear before the Argentine Congress on Monday 19 January to lay out the details of his complaint to lawmakers from the ruling party and from the opposition. Over the weekend, according to subsequent news reports, Nisman tried unsuccessfully to contact the person who, as the operational chief of intelligence services until December 2014, had control over the AMIA investigation over the years and who had facilitated the wiretapping on which the accusation against the Fernández de Kirchner government was based. Late in the evening on Sunday 18 January, Nisman was found dead in his home with a bullet in his head.

The court investigation of Nisman's death remains open and, for the moment, the theory that the death was a suicide prevails. Meanwhile, Nisman's complaint against the Argentine president has not prospered: two judicial authorities determined that there was insufficient proof to open a judicial case, given the fact that no conclusions could be drawn from the recorded conversations. Nisman's death and the context in which it occurred had significant impact on public opinion, and after years of an often solitary struggle by the victims, the AMIA case has at last become a key issue on the political agenda.

In August 2015 the trial to determine the individual criminal responsibilities of political and judicial officials in the cover-up of the AMIA attack began in Buenos Aires. The victims and broad sectors of the Argentine public are hoping that the trial will finally expose the truth of what happened.

the context

The irregular judicial investigation can be explained by the weakness of Argentina's criminal investigation system, the obscure and illegal historic functioning of the intelligence services, and the fact that over the years politicians continued to rely on this matrix of spurious relations between the intelligence agency and the federal judicial system.

In upholding a fabricated story, the Argentine state was not compelled to follow up on other leads. For example, the court never looked deeper into the hypothesis that a group of Syrian citizens with alleged connections to then President Carlos Menem was involved in the attack. It didn't even investigate whether the intelligence services had suspicions/indications prior to the AMIA bombing that a terrorist attack could take place in Argentina. Also, the hypothesis that the local intelligence services had information on another possible attack was not investigated either. In 2004, ten years after the bombing, it was revealed that international pressure had also played a role in the cover-up. Diplomatic wires from the Argentine Embassy in Israel, issued just hours after the explosion, showed that an official from Yitzhak Rabin's government had travelled immediately to Argentina to coordinate a 'matching version' of the bombing, laying the blame on Iran for the attack.[2]

From a broader point of view, there is also the question of the motivation for the cover-up. In the two decades since the attack, geopolitical calculations, Argentina's relations with other countries – Syria and Iran among them – and the internal politics of every groundbreaking moment over the course of the investigation have conspired to hide the truth.

The AMIA case has highlighted the dangerous subterranean connections between Argentina's intelligence services and its political and judicial spheres, and underscored just how important reining in and reforming Argentina's intelligence and surveillance operations is for the rule of law and for the health of Argentine democracy.

In 1999 Memoria Activa, represented by the Centro de Estudios Legales y Sociales (CELS) and the Center for Justice and International Law (CEJIL), denounced Argentina before the Inter-American Commission on Human Rights (IACHR) in connection with the AMIA bombing for violating the right to life and bodily integrity. Citing the irregularities committed by the judicial branch, the federal police and the intelligence services, it also lodged a complaint against the country for violating its duty to conduct an effective investigation. In March 2005 the Argentine state acknowledged its responsibility: 'There was a breach of compliance with the duty of prevention in not having adopted the appropriate and effective measures to try to prevent the attack, considering that just two years

> “[I]t is also necessary that the political system, the judicial branch and other powers, including the mass media, acknowledge and confront the toxic and often irreparable impact that unaccountable and arbitrary use of the intelligence services has had on democracy and the protection of human rights.”

earlier there had been a terrorist act against the Israeli Embassy in Argentina.' In that same document, it also acknowledged that 'there had been a cover-up of the facts and severe and deliberate breach of the duty to properly investigate the crime, which caused a clear denial of justice.' The Argentine state committed itself to reforming its intelligence organs.[3]

However, for over ten years, the Argentine government did not adopt measures to fulfil its commitment to the IACHR to make the inner workings of the intelligence services transparent. Instead, political and judicial officials continued to tolerate the covert power of intelligence agents in order to benefit from the spoils of that power. Irregular relations among judges, attorneys, lobbyists and notable intelligence agents affected the functioning of the federal judicial system, enabling alliances between political entities (both government and opposition), business, unions and church sectors, among others. The potential for extortion and destabilisation remained huge.

After Nisman's death – and amid suspicions that this underground network was seeking to destabilise the government in response to a recent shake-up of the intelligence agency – President Fernández de Kirchner decided to undertake a reform of the intelligence system. In late January 2015 she sent a bill to Congress to dissolve the Intelligence Secretariat and create the Federal Intelligence Agency (AFI) in its stead. The bill contained valuable elements, such as requiring that the appointments of AFI's director and deputy director be approved by the Senate and placing the office in charge of wiretapping under the authority of the national Attorney General's Office. However, the initial proposal did not include the kinds of substantial changes needed to address the critical issues that contributed to the failure of the AMIA bombing investigation, such as ending the absolute secrecy of the system, rethinking the criteria for classifying and declassifying information, establishing oversight of reserve funds, and imposing limits on the participation of new AFI agents in criminal investigations.

Strong criticism and concrete suggestions from CELS[4] and other organisations resulted in important modifications to the bill that was finally passed by Congress. In order to eliminate the blurred lines and improper relations between judicial officials and spies, the law prohibited the new intelligence agency from participating in criminal investigations in the place of police and security forces. To address the problem of excessive secrecy, a default acceptance of secrecy as a rule of intelligence work was replaced with a requirement that secrecy only be maintained when the physical integrity of an analyst or fundamental social values such as democratic life are at stake (although vague phrasing in the language establishing that the state's interest can justify limiting this principle could still result in arbitrary denials of access to information).

A man with the shofar, the ancient Jewish musical horn, during a commemorative act by Memoria Activa in Buenos Aires, on 17 July 2015.
Photo: Santiago Cichero

Moreover, the new law created a mechanism to declassify documents and provide citizens with access to information. In the case of the intelligence budget, it established that all expenses are public and therefore subject to the oversight contemplated in laws on financial administration. In the event that the publication of budgets could affect an ongoing intelligence operation, the law provides that these budgets may be kept secret but must be recorded in official documents signed by the AFI director and accessible to the Bicameral Commission in charge of supervising intelligence organisations.

This legislative reform was an important political attempt to improve the democratic legitimacy of the intelligence agencies. However, for the reform to be effective and the oversight mechanisms to work, the changes need to be accompanied by government will to enable and enforce change.[5] In December 2015 a new government assumed the presidency of Argentina. This administration faces the challenge of firmly establishing this new, accountable approach to intelligence. The refocusing of the intelligence system's objectives, its professionalisation, and the fulfilment of actions aimed at implementing the reforms that improve the system's transparency must be priorities for the new government.

At the same time, as Argentina has learned in its efforts to address human rights abuses in the past, it is also necessary that the political system, the judicial branch and other powers, including the mass media, acknowledge and confront the toxic and often irreparable impact that unaccountable and arbitrary use of the intelligence services has had on democracy and the protection of human rights.

So far, we have seen setbacks under the new administration. The appointed director of AFI is a businessman close to the president who has no known experience with intelligence matters. Many of the agency's new high-ranking officials have close ties to the people responsible for the irregularities and abuses mentioned previously. The first concrete measure that President Mauricio Macri took without consulting Congress, was to move the wiretapping unit from the Attorney General's Office (with which Macri is tussling politically) to the realm of the Supreme Court. This has fed fears that former SIDE agents could be brought back in to do wiretapping due to a lack of trained court personnel. In the month of May 2016, President Macri issued an executive order that overruled norms that were put into effect during 2015 that specified which types of expenses could be classified and which ones

could not, and established a record-keeping procedure for secret expenses to facilitate future oversight and review. This executive order disregards the commitment signed between the Argentine state and the families of the AMIA victims and reverts to the former administrative system for reserve funds that was used by the SIDE to buy off witnesses. In response to a note sent by CELS and Memoria Activa to the Chief of Cabinet of Ministers, AFI director Gustavo Arribas responded evasively and refused to reveal the system currently used to report the use of reserve funds. The Argentine state, responding to a question posed by the UN Human Rights Committee acknowledged that the lack of a record-keeping and oversight system for intelligence expenses could be considered 'a setback regarding transparency.'[6]

conclusion

Without a base of democratic principles or oversight, the intelligence services' capacity to do damage was tremendous; in fact, the most serious terrorist attack in the history of Argentina remains to this day unexplained and unpunished.

The opaque functioning of the intelligence services during decades affected many layers of the political system: the security forces, the judicial system and various government spheres. Often justified as necessary to maintain and consolidate governance, these clandestine relationships only served to undermine, not reinforce, democracy. The AMIA case is a concrete example of the grave consequences of these illegitimate pacts. It is essential that the executive, legislative and judicial branches and civil society organisations act together to build strong democratic systems to govern security and intelligence structures and to keep them from becoming autonomous in their goals and operations. It is fundamental that these institutions work together to ensure accountability for the activities of the intelligence agencies and to avoid any setbacks in the reforms already enacted.

On a Friday morning last in July 2015, after the traditional reading of the 85 names of the people killed 21 years before in the explosion, Memoria Activa member Diana Malamud, whose husband died in the AMIA bombing, took the microphone on the makeshift stage before the Palace of Justice:

For 21 years we have been searching and continue to search for the truth. Who was behind the attack that murdered our families? Who executed it, who supported it, who hid it, who covered it up? As for the cover-up question, we know the answer.

Driven largely by the fallout from the death of prosecutor Nisman, at last some concrete steps are being taken to hold accountable those who conspired to create a false narrative of responsibility after the bombing. After years of delays and resistance on the part of the judiciary, on 6 August 2015, a court in Buenos Aires heard opening arguments in the trial of those who stand accused of orchestrating that cover-up, including former President Menem, Judge Galeano; and senior intelligence officials. A year into the of trial, some truths have started to come to light. Testimonies from federal police officers and court employees have confirmed that the so-called 'Syrian lead' that led to people linked to Menem was not investigated. Telleldín himself recognised that the money he received from the SIDE was to incriminate the Ribelli group. The accusers in the first, botched trial now stand accused themselves.

The victims and society as a whole deserve answers.

notes

-

1. Those sought by INTERPOL are: former Iranian Intelligence Minister Ali Fallahian; former commander of the QUDS Force, the elite arm of the Iranian Revolutionary Guard, Ahmad Vahidi; former commander of the Revolutionary Guard, Mohsen Rezai; former Cultural Attaché of the Iranian Embassy in Argentina, Moshen Rabbani; and former third secretary of the Iranian Embassy in Argentina, Ahmad Reza Asghari. Former Hezbollah Chief of Foreign Affairs Imad Fayez Mughniyah was included in the original list, but on 12 February 2008 his vehicle exploded while he was driving through the streets of Damascus, Syria. Sources from the intelligence community claimed in a report published by Newsweek in March 2015 that the killing of Fayez Mughniyah was co-organised and executed by intelligence agents from the Mossad and the CIA.
2. The documents were brought to light by journalist Horacio Verbitsky, the president of CELS' board of directors, in 'La InfAMIA,' Página12 (18 July 2004). Available at: http://www.pagina12.com.ar/diario/elpais/1-38318-2004-07-18.html. The so-called 'Iranian lead,' and subsequent abandonment of the Syrian one, were convenient for the Argentine government as well as the Israelis. In the case of Argentina, this was because it veered the investigation away from a group of Syrian residents in the country with economic ties to the family of President Menem. At the same time, it was useful for the Rabin government 'given that the opposition parties and some news media were using the event to hit Rabin's peace policy hard,' as evidenced in the diplomatic wires.
3. Decree 812/05. Available at: https://www2.jus.gov.ar/amia/pdf/decreto_812.pdf
4. Analysis document presented by CELS when it was announced that a bill to reform the intelligence system was being sent to Congress (1 February 2015). Available at: http://www.cels.org.ar/comunicacion/index.php?info=detalleDoc&ids=4&lang=es&ss=46&idc=1894
5. CELS' analysis of the modifications introduced by the Senate to the bill to reform the intelligence system (12 February 2015). Available at: http://www.cels.org.ar/comunicacion/index.php?info=detalleDoc&ids=4&lang=es&ss=46&idc=1899
6. Informe Caso Amia, Comisión Interamericana de Derechos Humanos, Available at: http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fAIS%2fARG%2f24441&Lang=en

Surveillance at a glance in Argentina

Do citizens know more now than they did three years ago about the government's surveillance activities?
No. The vast majority of the public remains unaware of the activities of the intelligence agencies.

Did the Snowden disclosures lead to meaningful public debate in your country about the proper limits on government surveillance?
Yes. However, the debate is only confined to small groups especially worried about the implications of Snowden's revelations.

Since the Snowden disclosures, have any whistleblowers come forward to inform the public about government surveillance activities?
No

In the last three years, have the government's national-security surveillance authorities been narrowed, expanded, or neither?
Narrowed, but only to a limited extent. The national intelligence agency no longer controls the office in charge of executing legal wiretappings.

In the last three years, have new structural checks (e.g. new transparency requirements) been imposed on intelligence agencies?
Yes. In early 2015 Congress passed a bill dissolving the old Intelligence Secretariat and creating a new agency. The legislation incorporated new standards on transparency and public access to information and limited the powers of the intelligence system.

If the legislature/parliament is considering new legislation relating to government surveillance, would that legislation narrow the government's surveillance powers or expand them?
N/A

If the legislature/parliament is considering new legislation relating to government surveillance, would that legislation impose new structural checks?
N/A

Over the last three years, have the government's national-security surveillance authorities been the subject of domestic litigation, including in constitutional courts?
Yes. The courts are investigating several criminal complaints against agents and former agents for illegal espionage, smuggling of communications equipment and obstruction of justice, among other offences. In March 2015 two high-ranking naval officers were sentenced to prison with parole for ordering illegal political intelligence.

Over the last three years, have the courts rejected as incompatible with constitutional or human rights law any aspect of government surveillance?
No. (However, in 2009 the Argentine Supreme Court ruled in 'Halabi' that a law mandating communications companies to keep metadata from telephone and internet traffic affected the right to privacy and declared it unconstitutional)

Over the last three years, do you think the public has come to trust the intelligence agencies more, less, or neither?
Neither. The public has never trusted the intelligence agencies in Argentina.

From the halls of Parliament to the cubicles of cybercafés: the Indian government is watching

6
INDIA

A cybercafé in Bangalore, Karnataka, India.
Photo: Alamy/Latinstock

INDIA

From the halls of Parliament to the cubicles of cybercafés: the Indian government is watching

the case

In 2008 the Indian Parliament was at the height of a nine-month battle over a nuclear energy deal with the United States. The stakes were high: under the terms of the deal, India would open 14 of its civilian atomic reactors to international inspections, and in return, India would be permitted to expand its civilian nuclear programme without signing the Nuclear Non Proliferation Treaty.

The country was divided and the political climate was tense. The government of Prime Minister Manmohan Singh was pressing for the deal, insisting it would enhance India's status as a global superpower, while critics and opposition parties were questioning the US government's intentions in brokering the deal, and warning of the damage it might do to long-standing relations with other important allies, especially Iran. The deal's critics, moreover, were accusing Singh of corruption and dirty tricks in his efforts to convince lawmakers to support the deal. Shouting 'be ashamed' and 'thief,' Singh's opponents marched into Parliament carrying duffel bags full of cash to symbolise what they insisted had been a scheme to buy votes, and managed to force a confidence vote on the Singh government. Singh survived that vote, and in July 2008 the Indian Parliament approved the nuclear deal by an extremely slim margin.[1]

One year later, in an entirely unrelated incident, journalist Saikat Datta noticed an unmarked car following him as he was driving home from work in Delhi. He tried to ignore his concerns, but the same car followed him the next day. So Datta jotted down the vehicle's number plate and called the police, who informed him that the numbers were fake. Law enforcement intercepted the car and apprehended the driver and two passengers, only to discover that the men were officials with India's Intelligence Bureau.[2]

For the journalist, it could not have been a complete surprise to learn that he was being watched by Indian intelligence. After all, Datta focused primarily on national security reporting and had been looking closely at the intelligence services.

Undeterred, Datta continued to follow leads from confidential sources and in the spring of 2010 he published a series of articles in Outlook magazine exposing the Indian government's use of new surveillance technology to intercept and record Indians' mobile phone conversations.

Datta's sources revealed numerous cases in which the government's National Technical Research Organisation (NTRO) had tapped the private conversations of political leaders, bureaucrats and foreign dignitaries. In 2007 the NTRO intercepted and recorded a conversation between Congress general secretary Digvijay Singh and a Punjabi politician concerning the politician's potential participation in an upcoming election. In another case, NTRO eavesdroppers recorded a phone call between Bihar chief minister Nitish Kumar and his colleagues concerning state funding.[3] And, Datta reported, in the contentious months before the 2008 nuclear deal was approved, the NTRO had intercepted and recorded the mobile phone conversations of a number of politicians opposed to the agreement, among them Prakash Karat, the general secretary of the Indian Communist Party and one of the most high-profile leaders opposing the deal.[4]

In his series of exposés, Datta revealed that the NTRO was using a new form of surveillance technology to intercept these conversations, as well as the private phone conversations of many other Indian citizens and residents. According to both anonymous government sources and leaked documents, the phone tapping was made possible by passive cellular interception devices that the Indian government began importing from Eastern Europe in 2005. In early 2006 the NTRO had

actually tested the technology on the agency's overseer, then National Security Advisor M K Narayanan. Narayanan was asked to place a call to his secretary, which intelligence officials intercepted, recorded and transcribed. Narayanan, who reports only to the prime minister, had been impressed with the new technology and decided to invest in it.

This form of cellular interception is known as 'off-the-air' GSM and CDMA monitoring (or Stingrays), and it is designed to target the two most commonly used mobile networks in India.[5] The technology functions by intercepting calls and messages as they travel between phones and mobile phone towers, allowing interceptors to listen in and record communications without help from telecom providers.[6] As one senior intelligence official told Datta, 'It can be deployed anywhere. We don't need to show any authorisation since we're not tapping a phone number at the exchange but intercepting signals between the phone and the cell phone tower and recording them on a hard disk. If too many questions are asked, we can remove the disk and erase the conversation. No one gets to know.'[7]

Datta's reporting showed how the NTRO had employed this technology to monitor the Singh government's political opponents, but it also revealed ways in which the government was using it against huge swaths of India's population. In addition to targeting individual phone numbers, the technology has also enabled the NTRO to conduct bulk surveillance, including filtering through an entire region's communications. In some cases, the Indian government has used the technology to target certain geographic regions based on their ethnic or religious demographics. Datta reported that the NTRO frequently targets predominantly Muslim neighbourhoods in cities including Delhi, Lucknow and Hyderabad, 'randomly tuning into conversations of citizens in a bid to track down terrorists.'[8]

the context

India's off-the-air cellular interception system is just one of the many tools in the government's increasingly empowered and unaccountable mass surveillance regime.

That regime is known as the Centralized Monitoring System (CMS). The Indian government announced in 2009 that it was developing an electronic intelligence collection system that would enable agencies to monitor all phone and internet communications in the country.[9] CMS, which was designed to replace the more decentralised and privatised system of the past, was expected to be fully operational by March 2016.[10] As Reuters reported, CMS allows the government to 'listen to and tape phone conversations, read e-mails and text messages, monitor posts on Facebook, Twitter, or LinkedIn and track searches on Google.'[11] In effect, CMS gives the government direct access to the communications of India's 1 billion mobile and landline subscribers and 108 million internet subscribers, allowing it to bypass telecom and internet providers.[12] This massive data collection system was conceived, designed and now operates entirely without parliamentary approval or oversight.

CMS is breathtaking in its scope and lack of oversight, and is almost entirely unrestrained by relevant Indian laws.

Historically, two major laws have limited the government's ability to intercept communications: the Indian Telegraph Act of 1885 and the Information Technology Act of 2000, as amended in 2008. Both laws allow time-limited and targeted surveillance and require individualised authorisation of each interception request by either the home secretary or the secretary of the department of information technology.[13]

> CMS gives the government direct access to the communications of India's 1 billion mobile and landline subscribers and 108 million internet subscribers (...) This massive data collection system was conceived, designed and now operates entirely without parliamentary approval or oversight.

The colonial-era Telegraph Act restricts the interception of communications to cases where it is conducted in response to a public emergency or to protect public safety. In these circumstances, the government was permitted to intercept and collect data in the interest of 'the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence.'[14]

Throughout the 1990s, the trend was towards narrowing the surveillance powers that the government claimed under the Telegraph Act. In 1996, the People's Union for Civil Liberties, an Indian civil liberties organisation, brought a lawsuit challenging Indian surveillance laws on the grounds that they violated the right to privacy of Indian citizens. While India's Constitution does not set out any specific right to privacy, the judiciary has interpreted other constitutional rights, including the right to life and liberty, to protect individual privacy. The People's Union for Civil Liberties argued that the kinds of communications monitoring that were permissible under the Telegraph Act and other Indian laws infringed on these basic rights. The Indian Supreme Court agreed to expand the right to privacy to include communications, issuing a set of guidelines for lawful wiretapping that included a requirement that all surveillance be authorised by a federal or state home secretary. The guidelines were intended to provide temporary safeguards against intrusive surveillance until Parliament could craft and enact new privacy legislation that articulated legal protections for private communications. This never happened.

Instead, throughout the 2000s, the pendulum swung away from privacy protections and towards even more expansive surveillance powers. The Information Technology (IT) Act, amended after the November 2008 terrorist attacks in Mumbai, substantially weakened even the 130-year-old Telegraph Act. The newer IT law does not require a public emergency or threat to public safety to trigger the interception of communications, and it specifically broadens the categories of justifications that the government can use to 'intercept, monitor or decrypt' information to include 'the investigation of any offence.'[15] The IT Act essentially gives the central government the unrestricted ability to determine who it will target, to access all of their private information and communications, and to prosecute them.[16]

The IT Act raised alarms among civil liberties and privacy organisations in India. Even an expert group established by the government's Planning Commission to create a framework for a new privacy law was troubled, concluding in a 2012 report that the combination of the long-standing Telegraph Act and the newly minted IT Act has 'created an unclear regulatory regime that is non transparent, prone to misuse, and that does not provide remedy for aggrieved individuals.'[17]

Activists from the Communist Party of India raise arms while shouting slogans during a rally against the India-US nuclear deal in New Delhi, India, on 18 September 2007. Photo: Gurinder Osan/AP

Moreover, although both the Telegraph and IT Acts technically require that the interception of citizens' communications be time-limited and targeted, other rules and regulations directly contradict or undercut these restrictions.[18] For example, to operate in India, telecommunications companies must secure licences from the Department of Telecommunications; those licences require telecom providers to allow the government direct access to all communications metadata and content, regardless of whether the government has a warrant. Furthermore, the licences issued by the Department of Telecommunications restrict bulk encryption of users' information to 40 bits, an extremely weak level of encryption. Because GSM networks generally employ 64-bit fixed bulk encryption, Indian providers often eliminate encryption altogether, leaving users' communications entirely unprotected from both government and private interception.[19]

Telecommunications companies are not the only private businesses forced to aid the government in its surveillance. Regulations established in 2011 require cybercafés to collect detailed records of every patron's identity, address and phone number, as well as their browser history and the amount of time each user spends on the internet. This information, which the businesses are required to keep for one year, must be submitted to the government every month.[20] Because the majority of Indians have access to the internet exclusively through cybercafés, this on-site usage monitoring gives the government an open window on the private expressive activities of a huge percentage of the country's citizens.[21]

These licences and arrangements with private businesses give the government the ability not only to intercept and record phone conversations and messages, but in effect to access all internet communications and activity, from emails to Google searches to social media content.[22] That it is using these powers is clear: in recent years the government has arrested numerous people for criticising it on social media, and it has increasingly pressured websites, including Google and Facebook, to censor the speech and activity of its users.[23]

Giving domestic surveillance entities such extensive and direct access to private communications and internet activities would be a concern even if there were effective checks in place on the intelligence agencies and on their use of surveillance powers. But in India, the lack of transparency of the intelligence agencies, coupled with a nearly complete absence of meaningful judicial or independent oversight, leave Indian citizens and residents especially vulnerable.

Activists of the Communist Party of India shout anti-government slogans during a demonstration against the India-US nuclear deal, in New Delhi, India, on 27 November 2007. Photo: Manish Swarup/AP

Like the Telegraph Act, domestic intelligence in India has colonial roots. In 1887 Great Britain established India's Intelligence Bureau, which was designed to investigate various types of criminal activity.[24] The agency, created by executive authority, is now one of at least ten central government agencies authorised to intercept citizens' communications.[25] The other intelligence agencies, similarly established by executive diktat, followed the model set by their colonial forebear and ignored constitutional requirements for parliamentary approval.[26]

In reality, there is no functioning legal mechanism through which the public can hold the government accountable for violations of their privacy rights (which are not explicitly recognised in Indian law) or of the laws that officially govern surveillance practices. Under the Centralized Monitoring System, not only do government agencies conduct surveillance without judicial authorisation, but there is no statutory redress mechanism for individuals to challenge the illegal interception of their communications. The most an aggrieved party can do is bring a claim before a court, but bringing such a case is made difficult by the extreme secrecy surrounding the government's intelligence activities, and the fact that neither the government nor its intermediaries, including the telecom companies, has any legal obligation to provide notice to targets of surveillance.[27]

This lack of transparency is exacerbated by the 2005 Right to Information Act, which, though it technically gives Indians a legal right to request government information, exempted all intelligence and security agencies from adherence to the law.[28] This makes it nearly impossible for Indian citizens to bring proof of their government's unlawful surveillance before a judge. Moreover, several Supreme Court rulings since the court's 1996 decision establishing a limited constitutional right to privacy have eroded individual privacy rights. The right to privacy is now severely limited by broad exemptions, including for 'an important countervailing interest which is superior,' a 'compelling state interest,' or a law that is 'just, fair and reasonable.'[29]

In the absence of effective judicial checks, oversight of Indian surveillance agencies and powers is left largely in the hands of the executive branch. Under the 1996 guidelines, the home secretary has responsibility for personally reviewing every individual federal request by a government agency to intercept communications. To ensure that there are no lapses, three other bureaucrats – the cabinet secretary, the law secretary and the telecommunications secretary – make up a 'monitoring committee' that meets periodically to review the orders passed by the home secretary. The number of requests

> “[I]n recent years the government has arrested numerous people for criticising it on social media, and it has increasingly pressured websites (…) to censor the speech and activity of its users.”

the home secretary and monitoring committee are reviewing is staggering: 7,000 to 9,000 phone taps were being authorised at the federal level each month, as of 2013.[30] This means that the home secretary is signing off on about 100,000 requests every year. As critics have noted, if the secretary took only three minutes to consider each request, it would take 15 hours per day (including weekends and holidays) to evaluate 9,000 requests per month.[31] The numbers alone suggest that this process is little more than a mechanical rubber stamp.

conclusion

In his far-reaching 2010 Outlook magazine exposé, Saikat Datta revealed that the Indian government has moved aggressively in recent years to acquire and deploy powerful new digital surveillance technologies like ‘off-the-air’ GSM and CDMA cellular monitoring, and that these technologies are now woven into what is arguably one of the most intrusive and unaccountable mass surveillance regimes in the world. Moreover, as Datta reported, the Indian government is directing those surveillance powers not just at external threats, but internally as well, at some of the country’s most prominent politicians; at activists, dissidents and disfavoured minorities; and, as he himself learned by looking into the rear-view mirror the year before his reporting was published, at journalists who try to illuminate the inner workings of India’s unaccountable intelligence agencies.

In some ways, those intelligence agencies operate like their colonial-era forebears, with no independent oversight and limited recognition of the privacy rights of Indian citizens. Increasingly, though, the tools that they wield are the tools of mass surveillance; GSM and CDMA monitoring are just one aspect of a new, more centralised and universal monitoring system that includes everything from phone tapping to social media tracking and has dramatically expanded the scope and quantity of information the government can collect. From the halls of Parliament to the most far-flung, modest internet café, the Indian government is watching.

notes

-

1. ‘India’s Government Wins Parliament Confidence Vote,’ The Washington Post (23 July 2008). Available at: http://www.washingtonpost.com/wp-dyn/content/article/2008/07/22/AR2008072200161.html
2. ‘Outlook Journalist Nabs Tailing IB Men,’ Outlook (11 April 2009). Available at: http://www.outlookindia.com/newswire/story/outlook-journalist-nabs-tailing-ib-men/657969
3. ‘We, The Eavesdropped,’ Outlook (3 May 2010). Available at: http://www.outlookindia.com/magazine/story/we-the-eavesdropped/265191
4. Available at: http://www.outlookindia.com/magazine/story/we-the-eavesdropped/265191
5. ‘Phone tap technology widely available; both GSM & CDMA phones easy to tap,’ The Economic Times (16 December 2010). Available at: http://articles.economictimes.indiatimes.com/2010-12-16/news/27610363_1_interception-phone-sim-card
6. See: https://www.privacyinternational.org/node/76
7. Available at: http://www.outlookindia.com/magazine/story/we-the-eavesdropped/265191
8. ‘A Fox On A Fishing Expedition,’ Outlook (3 May 2010). Available at: http://www.outlookindia.com/magazine/story/a-fox-on-a-fishing-expedition/265192
9. Human Rights Watch. ‘India: New Monitoring System Threatens Rights’ (7 June 2013): https://www.hrw.org/news/2013/06/07/india-new-monitoring-system-threatens-rights; and ‘India’s Snooping and Snowden,’ The Wall Street Journal (5 June 2014): http://blogs.wsj.com/indiarealtime/2014/06/05/indias-snooping-and-snowden/
10. ‘India’s surveillance project may be as lethal as PRISM,’ The Hindu (21 June 2013). Available at: http://www.thehindu.com/news/national/indias-surveillance-project-may-be-aslethal-as-prism/article4834619.ece
11. ‘India sets up elaborate system to tap phone calls, e-mail,’ Reuters (20 June 2013). Available at: http://www.reuters.com/article/us-india-surveillance-idUSBRE95J05G20130620
12. Addison Litton. ‘The State of Surveillance in India: The Central Monitoring System’s Chilling Effect on Self-Expression,’ Washington University Global Studies Law Review, Volume 14, Issue 4 (2015). Available at: http://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1556&context=law_globalstudies; see also ‘State of Surveillance: India’: https://privacyinternational.org/node/738#Communications Landscape
13. ‘How Surveillance Works in India,’ The New York Times (10 July 2013). Available at: http://india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india/?_r=0
14. Available at: http://www.dot.gov.in/sites/default/files/the_indian_telegraph_act_1985_pdf.pdf
15. Available at: https://www.hrw.org/news/2013/06/07/india-new-monitoring-system-threatens-rights
16. Available at: http://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1556&context=law_globalstudies
17. Available at: https://www.hrw.org/news/2013/06/07/india-new-monitoring-system-threatens-rights
18. Available at: http://india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india/?_r=0
19. Available at: http://india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india/?_r=0
20. The Centre for Internet and Society. ‘Internet Privacy in India.’ Available at: http://cis-india.org/telecom/knowledge-repository-on-internet-access/internet-privacy-in-india
21. Available at: http://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1556&context=law_globalstudies
22. Available at: http://india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india/?_r=0
23. See, for example, ‘A Mumbai Student Vents on Facebook, and the Police Come Knocking,’ The New York Times (20 November 2012): http://www.nytimes.com/2012/11/21/world/asia/india-police-arrest-student-over-facebook-post.html; ‘PUCL leader Jaya Vindhayala sent to judicial custody for objectionable Facebook post on Tamil Nadu Governor K. Rosaiah,’ India Today (13 May 2013): http://indiatoday.intoday.in/story/pucl-leader-jaya-vindhayala-remanded-judicial-custody-objectionable-posts-tn-governor-india-today/1/270867.html; and ‘India professor held for cartoon “ridiculing Mamata,”’ BBC News (13 April 2012): http://www.bbc.com/news/world-asia-india-17699304
24. ‘Created by telegram, IB finds itself standing on thin legal ground,’ Hindustan Times (14 November 2013). Available at: http://www.hindustantimes.com/india/created-by-telegram-ib-finds-itself-standing-on-thin-legal-ground/story-UFrue3ywW4P96DhvQFtadM.html; see also ‘Ex-officer questions Intelligence Bureau’s legal status,’ The Times of India (26 March 2012): http://timesofindia.indiatimes.com/city/chennai/Ex-officer-questions-Intelligence-Bureaus-legal-status/articleshow/12407777.cms
25. ‘“DNA” Exclusive: Raw Invades Your Privacy,’ DNA (17 December 2011). Available at: http://www.dnaindia.com/india/report-dna-exclusive-raw-invades-your-privacy-1626874
26. Available at: http://www.hindustantimes.com/india/created-by-telegram-ib-finds-itself-standing-on-thin-legal-ground/story-UFrue3ywW4P96DhvQFtadM.html
27. Available at: http://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1556&context=law_globalstudies
28. See Right to Information government website: http://www.righttoinformation.gov.in/rtiact.asp
29. Available at: https://privacyinternational.org/node/738
30. ‘Can India Trust Its Government on Privacy?’ The New York Times (11 July 2013). Available at: http://india.blogs.nytimes.com/2013/07/11/can-india-trust-its-government-on-privacy/?_r=0
31. Available at: http://india.blogs.nytimes.com/2013/07/11/can-india-trust-its-government-on-privacy/?_r=0

Surveillance at a glance in India

Do citizens know more now than they did three years ago about the government's surveillance activities?

No

Did the Snowden disclosures lead to meaningful public debate in your country about the proper limits on government surveillance?

No

Since the Snowden disclosures, have any whistleblowers come forward to inform the public about government surveillance activities?

No

In the last three years, have the government's national-security surveillance authorities been narrowed, expanded, or neither?

Expanded

In the last three years, have new structural checks (e.g. new transparency requirements) been imposed on intelligence agencies?

No

If the legislature/parliament is considering new legislation relating to government surveillance, would that legislation narrow the government's surveillance powers or expand them?

Expand

If the legislature/parliament is considering new legislation relating to government surveillance, would that legislation impose new structural checks?

No

Over the last three years, have the government's national-security surveillance authorities been the subject of domestic litigation, including in constitutional courts?

Yes

Over the last three years, have the courts rejected as incompatible with constitutional or human rights law any aspect of government surveillance?

No

Over the last three years, do you think the public has come to trust the intelligence agencies more, less, or neither?

More

The cameras
are on…
and they know
who they’re seeing

7
HUNGARY

Security cameras against the background of a billboard with a human eye.
Photo: Mark Lennihan/AP

HUNGARY

The cameras are on… and they know who they're seeing

the case

During the campaign for the 2014 national elections, the mayor of Budapest's 8th District dropped a bombshell: his local government was installing 180 new CCTV cameras with facial recognition capability, a system he pledged would provide full surveillance coverage of his part of the city.[1]

It wasn't just the plan that raised alarms but the powerful figure who was behind it. Máté Kocsis was not just the two-term mayor of a poor but gentrifying district in central Budapest; he was also a member of Parliament and one of the leading politicians in Hungary's governing Fidesz party, occupying the posts of party vice president in Budapest and director of communications of Fidesz nationally. He was a local government and law enforcement commissioner in the Budapest municipality, and in Parliament he served on the Committee on National Security and headed the Committee on Homeland Security and Law Enforcement. He also served on an ad hoc committee on crimes committed by police officers ('uniform crime') and on an investigative committee probing the implications of the NSA surveillance scandal for Hungary and Hungarian sovereignty. He was also president of the Hungarian Handball Association and vice president of the Ferencvárosi Torna sports club – patronage positions for a ruling party known to peddle influence through sports donations and lucrative stadium construction projects.

To sell his plan, Kocsis launched a 'social consultation' campaign, a propaganda strategy Fidesz often uses to gather 'findings' that serve to justify controversial measures. Budapest's 8th District is home to a large Roma population, and for decades during and after Soviet rule it suffered from high poverty, crime and neglect. Touting the benefits of the cameras not only for crime investigation but also for crime prevention, the local government sent letters to residents of the district asking for proposals on where to locate the new cameras. 'Research' blended with campaigning, and Kocsis rode his plan to victory: in April 2014 he was re-elected to a third term, and he moved quickly to install the all-seeing network of digital cameras.

Since then, Kocsis has managed to carry out his plan while eluding almost all meaningful public scrutiny. The plan had an announced budget of HUF 300 million (about USD 1 million), with the federal Ministry of the Interior providing two-thirds of the funds and one-third coming from the local government, which would officially purchase the cameras. Hungarian law required a mandatory public procurement process for all projects with budgets over HUF 250 million, but Kocsis had that ceiling raised to HUF 300 million to circumvent this obligation, and although it is funded with public money, the details of the project remain shrouded in secrecy. Every Freedom of Information request regarding the tender for the cameras has been denied by the local government, which claims the information is confidential for national security reasons. The local government has stated that the facial recognition software installed on the cameras is 'world famous,' but the exact name and brand is also confidential.

As the facial recognition cameras were being installed in secret locations throughout the district, work was proceeding on a new headquarters to run the district's surveillance system. The cameras were officially the property of the local government, but the data the cameras generated was to be processed by the Special Service for National Security, one of Hungary's national security agencies. The main, vaguely defined role of the Hungarian Special Service is to support secret intelligence gathering conducted by other government agencies. Beyond a 2013 hacker revelation that the Hungarian government had acquired and deployed controversial FinFisher surveillance software, little is known about what this secret intelligence gathering

> “[W]hat was touted as a crime-prevention tool in one particular area of Budapest is in fact a blueprint for a much larger system.”

involves or what methods and procedures the Special Service uses in its work.

What is clear is that the Special Service is very much the agency behind the 8th District's facial recognition cameras, and that what was touted as a crime-prevention tool in one particular area of Budapest is in fact a blueprint for a much larger system. The Special Service has been charged with testing the new technology, and if it declares the experiment a success, facial recognition cameras would be installed next in all Budapest metro stations.

the context

Hungarian citizens are all too familiar with surveillance. Intercepting phone calls, bugging homes and gathering information through intelligence agents were widespread practices in the communist regime – a regime the Fidesz party, a party of young liberals promoting parliamentary democracy and the rule of law, was established in 1988 to oppose. In the decade following the transition to democracy and a market economy, those values took root and an effective multi-party democratic system emerged with diverse local governments, an independent judiciary and a sharp focus on European integration.

But following disappointing election results in 1994, Fidesz veered from liberal to reactionary and surged, first in municipal and then in national elections. Left behind were its founding democratic commitments; in power, Fidesz has in recent years eroded or dismantled many of Hungary's democratic advances, weakening local governments, reshaping the voting system and undermining the independence of judicial institutions, including the Constitutional Court, and of key oversight bodies such as the ombudsman system, the data protection authority, and agencies with authority over economic and financial institutions and public service media.

Police officers watching a the test operation of the newly established surveillance system, at the new monitoring room of the 8th Disctrict police station, in Budapest, Hungary in 2014.
Photo: Orsi Ajpek/Index

It has also turned a hostile eye on civil society in Hungary. In a 2014 speech, Prime Minister Viktor Orbán declared that non-governmental organisations are 'political activists paid by specific foreign interest groups' who 'wish to use this system of instruments to apply influence on Hungarian political life.' He also said that he would set up a parliamentary committee to reveal 'who the real characters are behind [the] masks' of NGOs in Hungary. The Government Control Office has begun targeted audits of organisations considered critical of the government – including the Hungarian Civil Liberties Union (HCLU) – without proper legal justification, and in September 2014 the offices of two organisations that were helping to distribute funding from a Norwegian NGO were unlawfully raided by police.

This clear hostility to the activities of civil society organisations is occurring against a backdrop of a re-emerging, and ever more opaque, culture of surveillance.

There are two categories of surveillance powers in Hungary today: secret surveillance for the purposes of criminal investigations, and secret surveillance for national security purposes. Separate agencies carry out these two categories of surveillance, and legally speaking, there are differences in the external authorisation and warrant requirements and the oversight and control mechanisms governing their operations. But little is actually known about the nature and extent of these surveillance powers, their regulatory framework, and whether their actual activities comply with laws and regulations.

For criminal investigations, the police, customs and public prosecution authorities are authorised to conduct secret surveillance operations within the more restrictive limits of Hungarian law. But these entities receive support from the Special Service for National Security, which provides the technical tools and expertise for intelligence information gathering and covert data acquisition.

The Counter-Terrorism Centre of the Hungarian police is also empowered to employ secret surveillance, for both criminal and non-criminal investigatory purposes. When it is gathering intelligence related to a criminal investigation, the Counter-Terrorism Centre is required to seek judicial authorisation, but investigations to prevent terrorist acts or in the interests of national security bypass judicial control and are authorised directly by the minister of justice. The Counter-Terrorism

New monitoring room of the surveillance cameras of the 8th Disctrict police station, in Budapest, Hungary in 2014.
Photo: Orsi Ajpek/Index

> [A]ppointing the Special Service for National Security to operate CCTVs in the country is a clear violation of the principle of separation between police and national security services.

Centre's powers are extensive and include secret house searches, surveillance recording, the opening of letters and parcels, and inspecting and recording the contents of electronic or computerised communications, all without the knowledge of the surveillance targets.

In 2012, two lawyers who believed they were being monitored by the Counter-Terrorism Centre brought their concerns to the European Court of Human Rights (ECtHR), challenging the regulation that empowers the centre to spy on anyone without a court order by citing national security concerns. The lawyers challenged such surveillance, which required only the signature of the minister of justice, on the grounds that it was politically motivated and an unjustified and disproportionate violation of their right to privacy. The ECtHR's judgment stated that the relevant Hungarian legislation did not provide sufficiently precise, effective and comprehensive safeguards on the ordering, execution and potential redress of such measures. The court found that the scope of the measure could include virtually anyone, particularly given new technology which enables the government to easily intercept massive amounts of data outside of the original range of operation. Further, on the basis that the ordering takes place entirely within the realm of the executive, without an assessment of strict

necessity, and in the absence of any effective remedial or judicial measures, the court concluded that the law violated the right to respect for private and family life.[2]

If the boundaries and operations of the police and security agencies are unclear for most Hungarians, the surveillance landscape is clouded further by indications that private companies have cooperated with the government and quasi-governmental entities in illegal domestic surveillance activities. A 2008 investigation by the National Security Office found that a private company called UD Zrt, whose owners included members of the Hungarian national security apparatus, had spied on politicians by mapping their lifestyles, habits, financial activities and phone-call histories.

In short, Hungary's nebulous network of surveillance agencies and powers creates an atmosphere of unease, especially for NGOs and opposition political activists in Hungary. More than 25 years after the end of communist rule, there is once again widespread concern that both the criminal investigation and national security surveillance apparatuses are being deployed for political ends, in ways all too reminiscent of the communist era.

conclusion

Under Hungarian law, only the police and the 'authority for public security' are authorised to set up surveillance cameras; appointing the Special Service for National Security to operate CCTVs in the country is a clear violation of the principle of separation between police and national security services. But the question of control goes far beyond who is setting up and who is monitoring the cameras. Facial recognition cameras depend on a database of facial images to search and match. As with all other aspects of the CCTV project, there has been no official information on how this database is being assembled, and whose images it includes.

In a June 2014 meeting of a parliamentary committee, Kocsis stated that the goal was not to construct a database that contained the images of all Hungarians; the goal is to find criminals, he insisted, and so the database will be drawn from official criminal records. But even limiting the database to criminal records raises serious legal and due process issues: for starters, the Hungarian criminal record system is notoriously error-ridden and outdated. Moreover, it contains the records not only of those who have been convicted of crimes but of those who are facing criminal procedures or have restrictions on travelling abroad. Even for those who have been convicted of crimes, nothing in the Hungarian Criminal Code or in their sentences allows for permanent, warrantless surveillance.

Relying on a database drawn from official records is particularly problematic in areas like the 8th District, with its significant Roma population. Hungarian police have a history of discriminatory law enforcement in Roma communities, where citizens have been disproportionately fined for minor offences such as not having a bell on a bicycle or pushing a baby buggy in the road. The HCLU has challenged such practices in court and recently won a ruling affirming that this disproportionate sanctioning of Roma people for minor offences is discriminatory. However, the criminal records that this discriminatory policing produces are likely to remain in the official files that feed into the CCTV database, all but ensuring that Roma residents will be disproportionately subjected to facial recognition surveillance.

In fact, there are indications that the government intends to build a far more comprehensive database of images. Under draft legislation currently pending, a searchable registry of pictures of every Hungarian citizen would be operational starting in 2016. The Special Service for National Security would have broad authority to request data from that registry, giving it the power to make secret, remote and wholesale identifications of all Hungarian citizens.

Under Hungarian law, the location and capability of CCTV cannot be secret, and thanks to a court judgment in a Freedom of Information Act lawsuit brought by the HCLU a decade ago that required the Budapest City Police Department to reveal where it had installed an earlier generation of surveillance cameras, we know where the new generation of facial recognition cameras have been installed as well. The website of the 8th District police force boasts a map flooded with red dots marking the location of the surveillance cameras. But nobody knows for sure what is happening with the images that the cameras in Budapest's 8th District are seeing, or who, exactly, those cameras are recognising. We do know, according to Kocsis, that the cameras are on, in 'test mode,' and that their installation and operation has not been slowed by the absence of a legal framework to regulate their use, or the complete lack of transparency in how the system is being tested and evaluated.

'Regulation can wait,' Kocsis declared recently, 'until the cameras are actually in use.'

notes

-

1. 'Budapest's 8th district to get experimental face-recognition surveillance system,' The Budapest Beacon (July 2014). Available at: http://budapestbeacon.com/public-policy/budapests-8th-district-to-get-experimental-face-recognition-surveillance-system/10266
2. Case of *Szabó and Vissy v. Hungary*, application no. 37138/14, judgment of 12 January 2016, 89.

Surveillance at a glance in Hungary

Do citizens know more now than they did three years ago about the government's surveillance activities?
No

Did the Snowden disclosures lead to meaningful public debate in your country about the proper limits on government surveillance?
No

Since the Snowden disclosures, have any whistleblowers come forward to inform the public about government surveillance activities?
No

In the last three years, have the government's national-security surveillance authorities been narrowed, expanded, or neither?
Expanded

In the last three years, have new structural checks (e.g. new transparency requirements) been imposed on intelligence agencies?
No

If the legislature/parliament is considering new legislation relating to government surveillance, would that legislation narrow the government's surveillance powers or expand them
Expand

If the legislature/parliament is considering new legislation relating to government surveillance, would that legislation impose new structural checks?
No

Over the last three years, have the government's national-security surveillance authorities been the subject of domestic litigation, including in constitutional courts?
Yes

Over the last three years, have the courts rejected as incompatible with constitutional or human rights law any aspect of government surveillance?
No

Over the last three years, do you think the public has come to trust the intelligence agencies more, less, or neither?
Neither

Smoke and mirrors: Irish surveillance law and the illusion of accountability

8
IRELAND

Garda Ombudsman Commission, 8 February 2013.
Photo: The Irish Times

IRELAND

Smoke and mirrors: Irish surveillance law and the illusion of accountability

the case

On 10 February 2014 an article appeared in the Irish edition of a well-known British Sunday newspaper beneath the simple headline: 'GSOC under high-tech surveillance.' The article described a series of events which, had it not been describing real life, could well have served as the plotline for an intriguing political thriller.

The setting for the story was a modest three-story office building, not far from Dublin's bustling city centre shopping district, that houses the office of the Garda Síochána Ombudsman Commission (GSOC). GSOC is an independent state-funded oversight body that receives and reviews complaints about the Garda Síochána, the Irish national police, and it functions as one of only a handful of truly independent policing oversight bodies in the world. As GSOC describes it, the commission's primary responsibility is dealing with 'complaints made by members of the public concerning the conduct of members of the Garda Síochána.' Under Irish law, the commission retains extensive powers to investigate and prosecute allegations of misconduct against serving officers, right up to – with the consent of the minister for justice and equality – the Garda commissioner, or chief of police.

GSOC is a three-member body that was established in December 2005 to replace the old Garda Síochána Complaints Board, an internal police complaints mechanism. The commission has more powers than its predecessor. GSOC has the power to investigate complaints made against police officers by members of the public and to launch investigations on its own volition where it appears that a police officer has committed an offence or acted in a way that justifies disciplinary action. Since its establishment, GSOC has been involved in a number of high-profile investigations into allegations of serious misconduct and criminal behaviour by serving members of the Garda Síochána.

The working relationship between GSOC and the police has, at times, become fractious.

In his article, Sunday Times journalist John Mooney described how towards the end of the summer of 2013, GSOC hired a private British security firm, expert in countersurveillance, to sweep its offices for traces of surveillance activity being carried out against the commission. In his statement before a cross-party parliamentary oversight committee, which convened a number of hearings into the matter, the then chairman of GSOC, Simon O'Brien, indicated that concern over the possible leaking or acquisition of sensitive information from its offices had initially prompted the sweep. As a result of the findings of the security company, GSOC, unbeknown to the minister for justice and equality, launched its own public interest investigation on suspicion that it was under surveillance by members of the Garda Síochána.

The nature of modern covert surveillance techniques – at least according to Verrimus, the UK-based security and countersurveillance firm hired to undertake the investigation – is that they are, by design, very difficult to detect with any degree of certainty. Following its investigations, Verrimus was unable to uncover any concrete evidence pointing definitively to surveillance activity. However, during tests conducted at the offices of GSOC on a number of occasions, the firm identified three separate technical anomalies that, in its professional assessment, pointed towards likely attempts to access the communications systems, including personal mobile devices, of persons in or near the offices of GSOC.

The first anomaly highlighted by Verrimus related to an unused Wi-Fi device in GSOC that had reportedly connected with an external Wi-Fi network source without authorisation. This external network was later shown to have emanated from a coffee shop in the

same building complex as GSOC. In his evidence before the parliamentary committee, the Minister for justice and equality was at pains to downplay the significance of this anomaly, in part because the device had never apparently been utilised by GSOC. But in its own statement on the matter, Verrimus maintained that this anomaly remained a credible cause for concern, as any attempt by an internal Wi-Fi network to connect externally would be highly irregular and unlikely to be a mere mistake.

The second anomaly related to a poly-conferencing telephone system located in the office of the chairman of GSOC, Simon O'Brien. An unexplained occurrence detected following late-night testing of the phone system suggested the system may have been compromised. The anomaly was recorded during a late-night test of the system by investigators. The test comprised sending an alerting signal down the phone line to check for possible security threats. The procedure is aimed at 'flushing out' a potential eavesdropper. In its report, Verrimus noted that moments after the signal sent a prolonged burst of music, the same phone received an incoming call. In its assessment, the security firm concluded that 'the likelihood of a "wrong number" at that time to that exact unknown number at the time of an alerting test is so small it is gauged at virtually zero.' In other words, the receipt of a phone call moments after an unusual and unexpected audio signal was sent through the phone line suggested deliberate behaviour by someone listening to the phone line, perhaps checking the integrity of the connection without suspecting a countersurveillance operation was underway.

The third threat identified by Verrimus was related to potential interception of telecommunications remotely. Verrimus reported that, following tests, it had detected a faked or spoofed GSM/3G network 'base station' configured for a UK mobile company operating in the vicinity of the offices. The base station was capable of connecting to any phone subscribing to that operator or even, as was later confirmed, other operators, depending on specifications. Any phone connecting to the spoofed base station would have been susceptible to having its information, including phone call data, compromised. In its report, Verrimus concluded that the technology used to simulate such a network was most likely an IMSI Catcher or 'Stingray,' a device used to acquire hardware codes from mobile phones and SIM cards used in connecting to a particular network. The tests conducted to detect the spoofed base station coincided with visual sightings by on-site Verrimus personnel of an unmarked vehicle with blacked out windows parked in the vicinity of the GSOC offices, which the firm concluded suggested the potential for mobile surveillance capability. Verrimus noted that because IMSI Catchers are generally available only to government-level entities, the detected device pointed to intentional, sophisticated surveillance. However, no evidence was uncovered that any GSOC phones had been compromised as a result of the anomaly.

In a series of reports on its investigations, Verrimus did not conclude that a surveillance attack had definitely taken place against the offices of GSOC. Based on the available evidence, the company concluded a number of facts. Firstly, the phenomenon of the Wi-Fi device in the boardroom 'acting in an insecure manner was evidenced.' Secondly, 'a fake or spoofed 3G base station was detected locally.' Finally, in relation to the conferencing system in the chairman's office that received a call back at the moment the line was tested, the firm concluded that the test 'may have triggered a response from an Attacker/Listening Post/ Monitoring station.' Verrimus went on to state that, in such a case, it was 'likely that the "listener" found the intermittent audio input on the line at 01.40 hours an odd occurrence and without thought or consideration to the possibility of a [countersurveillance] operation

Members of An Garda Síochána (Irish Police Service), 2013.
Photo: Brenda Fitzsimons/The Irish Times

decided to test the call line to ensure it was working… assuming there would be nobody there at that time.' These conclusions left little doubt that Verrimus believed that the detected anomalies represented a distinct threat and that GSOC may have been subjected to surveillance or attempted surveillance. Moreover, in the view of the firm, at least one of the anomalies was so technologically adept that it would have been difficult for any entity other than a police or state intelligence service to deploy it.

That the Verrimus report would cast suspicion on the state sparked outrage inside the government, and internal resistance significantly slowed an official investigation. Then Minister for Justice and Equality Alan Shatter TD made a defiant appearance before the parliamentary committee, decrying the notion that either he (as had been suggested) or the police should come under any suspicion at all. 'My only interest is that we get at the truth,' the minister told the committee, while at the same time claiming that the suggestion that he may have authorised such surveillance was in the realm of 'total fantasy.' But under questioning from committee members, the minister revealed that he had not even asked the Garda commissioner whether or not the police had carried out surveillance activity against GSOC. Nor had he asked the Directorate of Military Intelligence (known as G2), another body with legal surveillance authority, whether it had been engaged in monitoring the police oversight body. In the minister's view, there was 'no evidence' that called for an internal investigation into the police or military intelligence services – a position that would be echoed repeatedly by high-ranking Irish officials even as concerns grew over what became known as the 'GSOC bugging scandal.'

Rather than supporting a substantive investigation, the government's response to the political storm focused on the messengers: officials challenged the credibility of Verrimus's assessment of the threats presented by the anomalies, questioned the behaviour of GSOC in launching its own public interest investigation into possible police involvement in surveillance of GSOC, and criticised the chairman of GSOC for failing to inform the minister for justice and equality of this investigation. GSOC ultimately admitted that while its suspicion of police involvement was based on good cause, it found no evidence of Garda misconduct and that while, under Irish law, GSOC is not required to inform the

“
It is impossible on the basis of the technical opinions and available information, categorically to rule out all possibility of covert surveillance.
”

minister of its investigations, it nevertheless regretted its decision not to keep the minister apprised of its bugging enquiry. Almost completely lost in the domestic political wrangling was the very serious possibility that GSOC might have been subjected to powerful, intrusive and illegal surveillance.

But outside of the government, concern over the GSOC bugging scandal grew by the day, and on 18 February 2014, eight days after journalist John Mooney's article first appeared in The Sunday Times, the government bowed to pressure from opposition parties, the media, independent legal experts including the Irish Council for Civil Liberties (ICCL) and the general public, and established a judicial enquiry. That enquiry was led by a retired High Court judge, the Honourable Mr. Justice John Cooke. Sixteen weeks later, on 10 June 2014, the judge published a 64-page partially redacted report.

The terms of reference for the judicial enquiry were set by the government. At the heart of the enquiry Judge Cooke was asked to determine the sequence of events that led to GSOC launching its own public interest investigation, to examine any reports and documentation relevant to that investigation, and to review and assess any evidence of a security breach or attempted security breach at GSOC. In his findings the judge did not conclusively rule out surveillance. Instead, a number of innocent explanations were proffered for the anomalies encountered. Noting the limitations arising from the 'ad hoc and non-statutory basis of [the] Enquiry' the judge noted that he had been granted no authority 'to adjudicate on disputes of fact' and that the conclusions reached in the report were reliant upon the voluntary co-operation of the parties concerned and of those whom the judge considered appropriate to approach. Having confined his review to the documentation that related to the actual apprehended threats of surveillance to GSOC, the judge concluded that:

It is impossible on the basis of the technical opinions and available information, categorically to rule out all possibility of covert surveillance.

However, he went on to say that:

[I]n the three threats identified by Verrimus, it is clear that the evidence does not support the proposition that actual surveillance of the kind asserted in the Sunday Times article took place and much less that it was carried out by members of the Garda Síochána.

The report goes on to offer a series of alternative and potentially innocent explanations for the anomalies discovered by Verrimus, which, the judge concludes, must be considered as plausible. The judge notes that the data connection relating to the Wi-Fi system in the boardroom could not have been used to activate a microphone capable of eavesdropping on conversations since the device in question was not microphone enabled. Thus, no actual surveillance could have taken place. Similarly, the spoofed 3G base station that Verrimus reportedly detected could equally be explained by the activity of local mobile phone companies testing 4G networks in the area, although no definitive evidence to support this supposition is presented in the report. Finally, though concluding that the call-back phenomenon on the conferencing system remains unexplained, the judge stated that there is no evidence that the 'ring-back reaction was necessarily attributable to an offence or misbehaviour on the part of a member of the Garda Síochána.' This explanation is as curious as it is diverting, since an answer to the question of whether someone was listening or capable of listening is quite distinct from the question 'who was listening?'

Justice Cooke's report was immediately criticised, both for its methodology and its findings. In reaction to the report's findings, ICCL Executive Director Mark Kelly noted that given the constraints imposed by the government's terms of reference for his investigation, Justice Cooke found precisely what it seems to have been preordained that he would find: that it is impossible to rule out categorically all possibility of covert surveillance. Kelly said that it was striking that the judge appeared to have made absolutely no independent investigative attempt to establish objectively whether or not surveillance of GSOC by the Garda Síochána had been sought or authorised. He also noted that not a single member of the Garda Síochána or the Defence Forces was interviewed, and there appeared to have been no examination of the

records kept on the use of surveillance equipment by police or military intelligence services. Nor were the 'oversight' activities of the 'designated judges' under the relevant legislation subjected to any form of review.

Instead of interviewing members of the Garda Special (Crime and Security) Branch, the Defence Forces' intelligence branch (G2), or officers of the Revenue Commissioners, Justice Cooke focused on the question of whether or not the GSOC's suspicions that it had been the target of surveillance were well-founded, sidestepping completely the core question of whether or not any agency of the state sought or obtained permission to engage in surveillance of the independent police complaints authority. Leaving unanswered the question of whether GSOC had been bugged, Justice Cooke likewise avoided the crucial questions that would follow a determination that such spying had occurred: Who did the bugging? Was the spying authorised? And why?

Responding publicly to the publication of the judge's report, Mr. Kelly opined that a report that merely revisits a range of more or less plausible explanations for communications anomalies, without even attempting to compare them with information readily available to the police and military intelligence services, can only be qualified as an exercise in 'smoke and mirrors.'

the context

Until 2009 surveillance in Ireland was largely governed by the provisions of the Interception of Postal Packets and Telecommunications Messages Act 1983, as amended. The legislation provided police and the Defence Forces with limited powers to listen to telephone calls, open and read mail and, if equipped with the capacity to do so, read email. The state could only invoke the provisions in exceptional circumstances and only when authorised upon application to the highest level – the minister for justice and equality. However, more recent legislation has expanded these powers to an unprecedented degree.

The Criminal Justice (Surveillance) Act 2009 codified a range of statutory powers relating to surveillance activity by state agents. Its introduction coincided with a strengthening of Ireland's non-jury Special Criminal Courts system, established originally to try members of subversive organisations but used increasingly, in the face of considerable criticism from international treaty monitoring bodies, to try persons suspected of organised crime. The 2009 Act authorised not only the police and Defence Forces but also, in certain circumstances, Revenue Commissioners to conduct surveillance. The act even expanded the legal definition of surveillance, so that surveillance is now defined as:

[*M]onitoring, observing, listening to or making a recording of a particular person or group of persons or their movements, activities and communications, or monitoring or making a recording of places or things, by or with the assistance of surveillance devices.*[1]

Under the new powers, authorities could seek authorisation for covert surveillance of up to three months on a secret application to a judge of the District Court (Ireland's lowest judicial tier) by a police officer, a member of the Defence Forces or an officer of the Revenue Commissioners of appropriate rank. In circumstances deemed urgent, where judicial authorisation is unobtainable, the Act provides for authorisation without judicial oversight for a period of up to 72 hours for an investigating agency, subject to certain conditions, for requests submitted by an officer of sufficient rank.

The 2009 Act gave police and government agencies unprecedented access to people's private lives, and an important new incentive to push the limits of legality. In a significant departure from the previous legislation, the Act stated that once authorisation is granted, agents can enter any place, either commercial or residential, without the knowledge or consent of the owner or person in charge of the premises – by force if necessary – for the purposes of conducting a range of surveillance activities, including installing or removing a surveillance device on an internal telecommunications system. Any evidence obtained through surveillance could be admitted as evidence in criminal proceedings, even when a police officer failed to comply with the requirements for authorisation, so long as the court found that the failure had been inadvertent, the officer had acted in good faith, and it was in the interests of justice to allow the evidence.[2]

Finally, the 2009 Act further eroded already weak oversight mechanisms meant to keep surveillance powers in check. Previously, the government was authorised to monitor postal and telephone communications as necessary in the 'national interest,' and postal and telecommunications companies could be required to provide authorities with access to the data retained through their services and make it available to the government upon request. Companies could also be compelled to intercept a customer's communications by assisting with the installation of surveillance capabilities on their networks and by providing direct access to their equipment to facilitate surveillance. In cases considered by the investigating authorities as urgent or in the interest of 'state security,' requests for co-operation could be made orally by a person of sufficient authority. What exactly constituted 'state security' was never defined in legislation.

Pre-2009 legislation completely exempted interception and tracking devices from the judicial authorisation requirement. While the minister for justice and equality was required to seek authorisation to intercept

> [A] report that merely revisits a range of more or less plausible explanations for communications anomalies, without even attempting to compare them with information readily available to the police and military intelligence services, can only be qualified as an exercise in 'smoke and mirrors.'

communications relating to criminal investigations or 'state security,' tracking devices – defined as equipment used for the purpose of providing information regarding the location of a person, vehicle or thing – required no such authorisation, on the theory that tracking devices do not record conversations and are therefore less intrusive than monitoring devices and that they are often deployed in urgent situations where warrant requirements might cause undue delay.

Legislation since 2009 has essentially transposed this loose framework to newer digital technology. For example, the Communications (Retention of Data) Act 201[3] permits a member of the police at or above the rank of chief superintendent, without securing a court order, to request telecommunications and internet service providers to disclose data retained by the service provider, where the data is required for the prevention, detection, investigation or prosecution of a serious offence; to safeguard the security of the state; or to save a human life. In cases of urgency, these requests can be communicated orally.

Both the previous and updated legislation authorise a High Court judge to review surveillance operations to determine whether they comply with the law. But the reporting requirements are so weak that it is virtually impossible to ascertain what powers are being used, how often, and whether the surveillance operations satisfy even the minimal legal requirements.[4] That the police, Defence Forces and Revenue Commissioners are using their surveillance powers is clear: last year the global telecoms company Vodafone disclosed that between 1 April 2013 and 31 March 2014 it had received 7,973 requests to turn over communications data.[5]

The concentration of surveillance powers in the hands of Ireland's domestic police, Defence Forces and Revenue Commissioners – all having the power to initiate their own operations and information requests, and with little independent oversight – is troubling enough. But in recent months, it has become clear that Irish citizens and residents are vulnerable to government-approved foreign surveillance as well.

On 25 November 2014, the German newspaper Süddeutsche Zeitung released documents obtained by the whistleblower Edward Snowden that revealed that the British intelligence agency GCHQ may have been monitoring Irish telephone and internet communications by tapping a series of underwater cables stretching from Ireland to the United States and Wales.[6]

The next day the new minister for justice and equality, Frances Fitzgerald TD, signed into law a statutory instrument[7] allowing foreign law enforcement agencies to tap Irish phone calls and intercept emails. That provision brought into effect the third part of the Criminal Justice (Mutual Assistance) Act 2008, which regulates

how Ireland collaborates with other governments in criminal investigations, both in relation to surveillance by Ireland and requests by foreign agencies to Ireland to authorise their own surveillance activities in the country. One particularly troubling aspect of this new law is a clause stating that companies that object or refuse to comply with an intercept order could be brought before a private 'in camera' court session for adjudication.

The spectre of abuse under Ireland's intelligence sharing agreements is far from theoretical. In 1999 in a startling revelation by a UK television news company, it was revealed publicly that British intelligence agencies had, for seven years from 1990 through 1997, intercepted all telephone, fax, email and data communications between the United Kingdom and Ireland, including legally privileged and confidential information – and that it had stored all this information, en masse, at an Electronic Test Facility operated by the British Ministry of Defence.

In 2005, following these revelations and subsequent legal challenges, the ICCL joined with Liberty and British-Irish Rights Watch to file suit in the European Court of Human Rights (ECtHR), claiming that this massive data 'fishing expedition' had breached the privacy of their inter-organisational telephone communications in violation of Article 8 of the European Convention on Human Rights (ECHR), and that the mass interception of all communications between the United Kingdom and Ireland between 1990 and 1997 was disproportionate and lacked transparency. The Strasbourg Court concurred, ruling that the UK government must 'set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material,' and that the surveillance it had carried out during that period did not protect the applicants' rights under the ECHR's Article 8 right to privacy 'in accordance with the law.'

conclusion

The possible bugging of GSOC exposed some very significant fault lines in Ireland's surveillance landscape and particularly on both the ability and willingness of public authorities to provide effective oversight. In the end, GSOC may or may not have been the subject of surveillance by agents of the state. However, as evidenced by the judge's narrowly focused report, little effort was made to determine whether such surveillance had actually taken place. It is perfectly possible that covert surveillance had been carried out and even authorised at the highest level. Nothing that has been stated either officially or in the subsequent findings of the enquiry has prevented this possibility.

What is evident is that a very significant opportunity was missed for the judge to ask the right questions of the right people. What is known about the state's surveillance activity? What is being done to ensure standards are checked and maintained? What kind of surveillance jurisdiction exists in Ireland and where does responsibility for failings lie? In other words, who, if anyone, is effectively watching the watchers?

Both the 'bugging' scandal and the existing legislative framework governing surveillance point inextricably to the need for significant reform in this area. Effective independent review and audit at regular intervals by an independent regulatory authority is urgently required. Without such reform, Ireland will remain a 'black site' among its EU and international peers in terms of the paucity of internal control mechanisms for oversight and accountability that are necessary to ensure legitimate use of surveillance by agents of the state. What's more, given the revelations of previous misuse of data by agencies both foreign and domestic, and as technology develops (creating new and innovative opportunities for increased monitoring and surveillance), a significant casualty will, likely, be public trust.

notes

-

1. Criminal Justice (Surveillance) Act 2009, Section 1
2. Yvonne Daly. 2010 'Legislative Developments – Criminal Justice (Surveillance) Act 2009,' Annual Review of Irish Law 2009 p. 341
3. Communications (Retention of Data) Act 2011, Section 6. Available at: http://www.irishstatutebook.ie/2011/en/act/pub/0003/print.html
4. 'More robust oversight of surveillance laws is "crucial", experts warn,' Irish Examiner (15 June 2015). Available at: http://www.irishexaminer.com/ireland/more-robust-oversight-of-surveillance-laws-is-crucial-experts-warn-336910.html
5. Vodafone. 'Country-by-country disclosure of law enforcement assistance demands' (2014). Available at: http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement/country_by_country.html
6. 'UK Spy Base GCHQ tapped Irish internet Cables,' The Irish Times (6 December 2014). Available at: http://www.irishtimes.com/news/crime-and-law/government-accused-of-cowardice-over-tapping-of-cables-1.2022045
7. Statutory Instrument 541. Available at: www.irishstatutebook.ie/eli/2007/si/541/made/en/pdf

Surveillance at a glance in Ireland

Do citizens know more now than they did three years ago about the government's surveillance activities?
Yes

Did the Snowden disclosures lead to meaningful public debate in your country about the proper limits on government surveillance?
No

Since the Snowden disclosures, have any whistleblowers come forward to inform the public about government surveillance activities?
Yes

In the last three years, have the government's national-security surveillance authorities been narrowed, expanded, or neither?
Neither

In the last three years, have new structural checks (e.g. new transparency requirements) been imposed on intelligence agencies?
No

If the legislature/parliament is considering new legislation relating to government surveillance, would that legislation narrow the government's surveillance powers or expand them?
Narrow

If the legislature/parliament is considering new legislation relating to government surveillance, would that legislation impose new structural checks?
Yes

Over the last three years, have the government's national-security surveillance authorities been the subject of domestic litigation, including in constitutional courts?
Yes (*Maximillian Schrems v. Data Protection Commissioner*)

Over the last three years, have the courts rejected as incompatible with constitutional or human rights law any aspect of government surveillance?
No

Over the last three years, do you think the public has come to trust the intelligence agencies more, less, or neither?
Neither

The case of Makaburi: the role of surveillance in extrajudicial killings

9
KENYA

Muslim cleric Abubakar Shariff Ahmed, also known as Makaburi, argues with senior police officers outside the Masjid Musa mosque in Mombasa, Kenya, on 5 February 2014.
Photo: AP

KENYA

The case of Makaburi: the role of surveillance in extrajudicial killings

A government is expected to protect national security as a predominant priority. In Kenya, terrorism has emerged as one of the greatest threats to national security, since hundreds of Kenyan citizens and residents have been killed and many more injured by terrorists in recent years. While it is well within the Kenyan government's interests to robustly confront this threat, it must do so in a manner that lives up to the country's constitutional principles – principles that recognise the respect of the individual's fundamental rights and freedoms as essential to the national interest. Unfortunately, Kenya seems to be on a path that paradoxically sacrifices fundamental rights and freedoms in the name of national security. In confronting the terror threat, Kenya has enacted laws that have expanded state power at the expense of individual liberties, including laws that have eliminated any meaningful limits on the government's surveillance authority. This is particularly worrying given Kenya's history of abuse of surveillance powers by security officers, who have often employed surveillance in the service of gross human rights violations such as torture and extrajudicial killings. The case that follows is among several that have sharpened concerns that surveillance powers are once again being used not in support of law enforcement investigations and prosecutions, but in support of targeted killing.

the case

Abubakar Shariff Ahmed, who was widely known by his nickname "Makaburi" (which means "graves" in Swahili), was a Muslim cleric based in the coastal city of Mombasa who preached at the controversial Masjid Musa mosque, where his youthful and ardent followers viewed him as a sheikh who spoke boldly against the oppression they faced as young Muslims in Kenya.

Makaburi had assumed leadership of the mosque after two other controversial clerics who were considered his close associates had been killed in murky circumstances: Aboud Rogo in 2012 and Ibrahim Ismail the following year. As with Rogo and Ismail, Makaburi's sermons were filled with references to what he deemed to be unjust wars that the West was waging against Muslims around the world. These clerics also called on their followers to rise up and defend themselves and their faith – fiery exhortations that their critics contended distorted the true tenets of the Muslim faith and were clearly bent towards extremism and radicalisation. To the Kenyan government, these sermons were more than theological: it considered the Masjid Musa mosque a centre for the radicalisation and recruitment of Muslim youth for the Al Shabaab terrorist group in the ongoing war in Somalia.

In 2010 and 2011, Al Shabaab, which is based in Somalia but operates a network of cells within Kenya, carried out a series of kidnappings of foreign nationals in Kenya's coastal resorts and in northern areas of the country. In response, Kenyan Defence Forces (KDF) troops moved into Somalia in "Operation Linda Nchi" in October 2011. The KDF and the African Union peacekeeping mission in Somalia (AMISOM) swiftly dislodged Al Shabaab from the southern Somalian port city of Kismayo, but Kenya's military successes in Somalia were met by accelerating terrorist attacks at home. From the start of Operation Linda Nchi to September 2014, according to statistics released by Kenya's Anti-Terrorism Police Unit (ATPU), 264 people were killed and 923 injured in 133 terrorist attacks in Kenya.

As the terror attacks in Kenya increased, Makaburi attracted more and more attention from the Kenyan government and international intelligence agencies. In 2012 the United States Department of the Treasury designated him a supporter of Al Shabaab, declaring:

Abubaker Shariff Ahmed has preached at mosques in Mombasa that young men should travel to Somalia, commit extremist acts, fight for al-Qa'ida, and kill U.S. citizens. Abubaker Shariff Ahmed was arrested in late

December 2010 by Kenyan authorities on suspicion of involvement in the bombing of a Nairobi bus terminal. Abubaker Shariff Ahmed is also a leader of a Kenya-based youth organization in Mombasa with ties to al-Shabaab. As of 2010, Abubaker Shariff Ahmed acted as recruiter and facilitator for al-Shabaab in the Majengo area of Mombasa.

Over the next two years, Makaburi was arrested three more times, accused the first time of having committed a robbery with violence, the second time of being a member of Al Shabaab, and the third time of inciting Mombasa youth to violence. But the Kenyan government never obtained sufficient evidence to convict Makaburi of any of these charges, and Makaburi was outspoken in claiming he was being judicially harassed. 'How am I a terrorist? Who have I terrorised?' he asked during an Al Jazeera news interview in 2013. 'I'm in court now for 3 years and nothing has been proved against me. I'm the one who's being terrorised; my life is the one that's in danger.' He went so far as to sue the Kenyan government for the unlawful seizure of his property after a house raid in 2011, successfully recovering damages of Kenya Shillings 670,000 (approximately USD 6,700). The court awarded the damages a week before he was gunned down after attending a court hearing on 1 April 2014 in connection with a criminal case filed against him.

Roughly six months before Makaburi's murder, on 21 September 2013, a terrorist attack at the Westgate Mall in Nairobi left at least 50 dead and 170 wounded. After that attack, Makaburi was quoted as saying that the killings were justified. 'It's not terrorism because in Islamic Sharia we have revenge,' he told a reporter. 'The Kenyan army is doing the same thing to people in Somalia…the Quran says eye for an eye.' At the same time, he acknowledged that the Kenyan authorities were becoming increasingly frustrated by their inability to prosecute him, and he began to say it was only a matter of time before they would execute him. He spoke more and more of martyrdom, claiming that any sheikh who taught the Islamic religion as a whole, including jihad, is killed in Kenya. During a television interview in October 2013, Makaburi was more specific about the source of the threat, claiming that "Recce," an elite squad of the General Services Unit (GSU) of the Kenyan national police, had been given the green light to assassinate him, as it had done with his colleagues before. Despite declaring he was ready to die, Makaburi began to take security precautions, spending nights in different places and living away from his wife and children.

On 1 April 2014, Abubakar Shariff Ahmed, alias Makaburi, was shot dead by unknown gunmen outside the Shanzu Law Courts in Mombasa, collapsing in a hail of bullets along the same stretch of road where Aboud Rogo and Ibrahim Ismail had been similarly murdered. His very public death brought into sharper focus what was by then already a prevailing suspicion: that the Kenyan police had embarked on extrajudicial killings as part of its counterterrorism efforts. And it raised a troubling new question: to what extent were these killings being fuelled by information gathered from proliferating systems of domestic and international surveillance?

the context

As the Kenya Human Rights Commission (KHRC) and other civil society organisations in Kenya have documented, Kenya has a history of extrajudicial executions, one in which the GSU of the police, in particular, has carried out such killings with impunity. In the mid- to late-2000s, the GSU was linked to the killings and disappearances of hundreds of members of a banned sect and criminal gang known as the Mungiki;[1] the rise in violent deaths of Muslim

An armed Kenyan policeman patrols past the Masjid Musa mosque, where Muslim cleric Sheik Ibrahim Ismael was killed, following riots after Friday prayers in the area in Mombasa, Kenya, on 4 October 2013.
Photo: AP

clerics identified as radical also pointed to a similar government elimination programme.

As the extrajudicial executions of members of the Mungiki occurred against a backdrop of the Mungiki campaigns of violence and extortion against other communities, the killings of clerics has occurred against the backdrop of Al Shabaab's intensifying terrorist activities in Kenya.[2] These attacks are having a devastating effect on the social and economic well-being of the northern Kenya region in particular, which is already seeing a mass exodus of non-Muslim teachers and other civil servants who have been targeted in terrorist attacks.

Kenyan government officials have sought to confront this rising terrorism forcefully and decisively, stating that they would not relent on their war against terror. Immediately after launching Operation Linda Nchi, then President Mwai Kibaki declared, 'The security of our country is paramount. We will defend our territorial integrity through all measures necessary to ensure peace and stability.'[3] This was originally understood to define the KDF's mission and operations in Somalia, but as attacks increased in Kenya, it also clearly applied to the domestic counterterrorism strategy. By as early as October 2011, the government was contemplating a security operation in Nairobi to purge the city of Al Shabaab militants and sympathisers. '[Al Shabaab] is like a big animal with its tail in Somalia,' the assistant minister of internal security said at the time. 'We are still fighting the tail and the head is sitting here [in Nairobi].'[4]

On the ground, security operations in Kenya largely featured police-led sweeps targeting illegal migrants and undocumented persons who are perceived to be the source of the internal threats. These operations have sparked allegations of undue profiling of members of the Somali and Muslim communities, and have reportedly involved human rights violations such as prolonged detentions, extortion and looting of property, physical assaults and violence and, in some extreme instances, extrajudicial executions.

One of the more notable security sweeps, Operation Usalama Watch, took place in April 2014 following a series of grenade attacks in Nairobi and Mombasa. So extensive were the raids that the Kasarani National Stadium was converted into a mass detention centre for urban refugees and persons suspected of being

in the country illegally. Human rights organisations immediately characterised the operation as discriminatory and unconstitutional. The sweep seemed to target only Somali refugees, ethnic Somali Kenyans, Ethiopians, South Sudanese and other Kenyan Muslim populations. Some of those detained levelled allegations of extortion against the police, and reported that they had been held in deplorable conditions and without access to their families or legal representatives. Refugees in urban areas were forcibly relocated to refugee camps, and some were summarily deported to Somalia from Kenya, likely violating the principle of non-refoulement of the 1951 Refugee Convention and the 1969 Organisation of African Unity Convention Governing the Specific Aspects of Refugee Problems in Africa. And it was not only the civil liberties community that protested. The government faced scathing public criticism for a sweeping, indiscriminate approach to security operations that seldom unearthed significant terror activities or threats. The mass arrests were branded public relations exercises and a demonstration of the government's inability to deal with the terror threat. The government found itself under pressure from the public to develop a security strategy based on intelligence rather than brawn or brute force.

In response, that strategy has come to rely more and more on surveillance in general and digital surveillance in particular. The Kenyan government has invested heavily in surveillance technology and significantly expanded the authority of state security agencies, the National Police Service (NPS) and the National Intelligence Service (NIS) in particular, to carry out digital surveillance. In 2012 two major pieces of legislation – The Prevention of Terrorism Act No. 30 and The National Intelligence Service Act No. 28 – curtailed privacy rights and expanded the ability of police to secure *ex parte* and emergency authority to monitor communications. Another wave of amendments and laws enacted in 2014 continued the trend, criminalising publications and other expression 'that is likely to be understood as directly or indirectly encouraging or inducing another person to commit an act of terrorism,'[5] and authorising National Security Organs to intercept communications for the purpose of detecting, deterring and disrupting terrorism without obtaining a warrant from the court, but instead by following procedures to be prescribed by the cabinet secretary in charge of internal security.

> "[W]ere these killings being fuelled by information gathered from proliferating systems of domestic and international surveillance?"

The 2014 amendments were passed under acrimonious circumstances that included violent scuffles between legislators in the National Assembly. The Kenya National Commission on Human Rights (KNCHR) joined the Coalition for Reform and Democracy (CORD, the leading opposition party) and other civil society organisations in challenging the Security Laws (Amendment) Act in court, and on 23 February 2014 the High Court declared several provisions of the Act restricting publications and expression to be unconstitutional, but preserved the new authority to intercept communications without a court order.

These new surveillance powers came even as Kenya was still struggling to reform state security and intelligence structures that had often been used to target political opponents and suppress dissent. A 2013 report by Kenya's Truth, Justice and Reconciliation Commission (TJRC) detailed how the notorious Special Branch of the national police oversaw an intelligence system that included the detention and torture of political dissidents during the struggle for multiparty democracy in the 1980s. Armed with far greater digital surveillance powers, the Anti-Terrorism Police Unit (ATPU) of the national police is fast gaining a similar reputation, fuelled by revelations of the suspected surveillance and execution of several Muslim clerics in Kenya's coastal region. Furthermore, Kenya's National Intelligence Service in July 2015 was revealed to have sought hacking software from an Italian surveillance malware vendor known as Hacking Team, and to have requested that the company shut down a website belonging to a popular blogger and critic of the current government.[6]

Our organisation, KHRC, has engaged in various advocacy efforts that have sought to illuminate the

“The link between fighting terror, extrajudicial executions and digital surveillance is proving to be an area of increasing concern that will require further investigation or scrutiny.”

opportunities and risks posed by the internet with regard to civil liberties. In addition to challenging the previously mentioned surveillance powers granted to the state in the war against terror, KHRC has mapped the Internet Legislative and Policy Environment in Kenya.[7] KHRC has also highlighted and spoken against the harassment of bloggers and human rights defenders on the basis of what they publish online. The link between fighting terror, extrajudicial executions and digital surveillance is proving to be an area of increasing concern that will require further investigation or scrutiny.

On 7 December 2014, Al Jazeera broadcast[8] a report on the assassination of Makaburi in which several unidentified officers stated on camera that they had been part of a death squad that was charged with killing the controversial cleric after attempts to prosecute him in court failed. ‘Makaburi in Mombasa is a very dangerous person to our country,’ an officer identified as ‘The Commando’ from the General Services Unit’s elite Recce squad declared in that news report. ‘What do you do with such a person? Do you spare such a person because you are observing human rights?’[9]

Al Jazeera reported[10] that its investigation had uncovered collaboration among the Anti-Terrorism Police Unit (ATPU), the National Intelligence Service (NIS), the Radiation Unit of the regular police service and the GSU’s Recce squad to oversee the assassination of persons considered to be terror threats. Its investigation revealed that persons such as Makaburi were placed under surveillance by the NIS, which was tasked with developing profiles of persons of interest, including where they went and whom they met or visited. The information would then be used to decide whether the person of interest would be eliminated. ‘We move tactically to understand what is taking place on the ground,’ an NIS officer identified only as ‘The Spy’ told Al Jazeera. ‘We collect this information, then we provide it to the right source for an action to be taken.’ According to the Al Jazeera report, the NIS delivers its surveillance information to the Kenyan National Security Council (NSC), the highest security organ in the country, which includes the president, deputy president, the cabinet secretary for the interior, the cabinet secretary for defence, the attorney general, the director of the NIS, the inspector general of police and the chief of the Kenya Defence Forces. The NSC decides whether to issue an execution order, which is then passed to a Recce unit death squad. The Recce officer identified as ‘The Commando’ told Al Jazeera that the assassinations specifically target influential figures like the radical clerics. ‘When we receive information that “so and so” is organising a certain group who are likely to terrorise people, the first person to get rid of is the leader,’ he said.

This, Al Jazeera reported, is exactly the sequence that was followed in the Makaburi assassination. A series

Mulsim men are detained by police officers at the Masjid Mussa mosque in Mombasa, Kenya, on 2 February 2014. Gunfire erupted in and around the mosque following a raid by armed police who had received a tip-off that Muslim youths were being radicalised and trained for military attacks.
Photo: Joseph Okanga/Reuters

of intelligence cables obtained by Al Jazeera said to be from Kenya's Criminal Investigation Department (CID) confirmed that Makaburi had been the subject of intense surveillance over the course of 2013. Though redacted in several areas, the cables indicate that Makaburi became the subject of concern for the security organs that believed he was actively planning and financing a series of terror attacks in the country, and that by April 2013, he had declared himself the 'Amir' of all Al Shabaab operatives in the country. It is this intelligence that is said to have swayed the NSC to sanction the assassination of Makaburi in April 2014. In the chilling accounts of the unnamed officers from the ATPU, Recce and Radiation units featured in the Al Jazeera investigation, the officers acknowledged that the execution of Makaburi was planned in Nairobi by high-ranking police officers and government officials. They also admitted they were responsible for the killing of other Muslim clerics.

Buried amid the many bombshell revelations of Al Jazeera's investigation were allegations that the surveillance behind the extrajudicial killings had been facilitated and supported by foreign governments that were partners in the 'global war on terror.' In addition to receiving financial support and equipment, security agents alleged that the British government had provided training on how to do surveillance 'in an advanced way' to get information. These sources further claimed that the Recce unit receives training from Israel, that the training includes instruction on how to eliminate persons of interest, and that the death squad often relied on intelligence from foreign partners to identify targets. 'Once they give us the information, tomorrow he is no longer there,' one of the officers told Al Jazeera. When the Al Jazeera report aired, both the British and Israeli governments went on record to deny the claims that they were complicit in the extrajudicial killings of Muslim clerics. The British government went on to state that it has raised concerns over the extrajudicial killings to the Kenyan government.

conclusion

At the height of the public debate surrounding the enactment of the Security Laws (Amendment) Act of 2014, the government spokesperson claimed that Kenya had joined 'the long list of democracies that have been updating their security laws to better ensure the safety of citizens from terrorist and criminal organisations that operate with increasing sophistication and brutality.' But the executions of Makaburi and other Muslim clerics have raised the

spectre of an increasingly sophisticated and brutal lawlessness on the part of the Kenyan government that specifically targets Kenyan citizens, one in which digital surveillance information gathered domestically or gathered and shared by foreign governments is forming the basis for kill orders issued in secret, without any constitutional or legal due process.

There is no doubt that Kenya is grappling with legitimate and serious security concerns. More than 300 persons have been killed in terrorist attacks in Kenya since 2011. But the state's response to such terror must abide by the Kenyan Constitution and uphold human rights obligations, even when confronting those who hold extreme and repugnant views. Persons suspected of being terrorists or working with terrorists must be afforded due process and be tried in a court of law. Failing to do so creates a culture of impunity that will ultimately undermine the safeguards that ensure people are presumed innocent until proven otherwise in court.

It is clear from the execution of Makaburi and other clerics that Kenya's counterterrorism security operations have not always conformed to the standards of the Kenyan Constitution. Nor, it appears, have the extrajudicial killings targeting only clerics. KHRC and other human rights organisations are increasingly receiving allegations of disappearances of young men from the coastal region and northern Kenya who were reportedly arrested by the ATPU.

At the same time, there are growing indications that the government's counterterrorism surveillance is now targeteng not just suspected terrorists, but also journalists and bloggers who discuss terrorism and other controversial subjects. Using the provisions of a law that criminalise 'the improper use of a telecommunication system,' the police have commenced an overzealous surveillance of social media, and there has been a marked increase in cases of individuals who are either being arrested or brought in for questioning on the basis of what they share online on blogs and social media pages. In January 2016 journalist Yassin Juma was arrested for posts he published on his social media accounts reporting updates on a recent attack on the Kenya Defence Forces (KDF) by Al Shabaab in Somalia. Even more worrying is the case of Judith Akolo, another journalist who in January 2016 was summoned for questioning by the Directorate of Criminal Investigations for retweeting a post from a blogger known for providing updates on security issues in Kenya; this same blogger was similarly brought in for questioning. And in an especially troubling development, what began as online surveillance targeting potential terrorist threats has expanded to include the monitoring and criminalisation of expressive activity that has nothing to do with terrorism, with bloggers now being arrested for causing annoyance by posting stories on various political leaders.[11]

Kenya's troubled human rights history has taught us that our country's security forces require more, not fewer, safeguards to protect the safety and rights of Kenyan citizens. But new laws have given Kenya's security forces, long prone to abusing their authority in security operations, even greater discretion regarding how they conduct surveillance. This surveillance without oversight has not led to lawful prosecutions; instead, it has led to a culture of fear, harassment, self-censorship and apparently to extrajudicial killings by a state-sanctioned death squad.

notes

-

1. Kenya National Commission on Human Rights (KNCHR). 'The Cry of Blood' Report on Extra-Judicial Killings and Disappearances (2008). The report highlights that by November 2007 KNCHR had been made aware of 500 cases of extrajudicial executions where the police may have been complicit. Available at http://www.africancrisis.org/Docs/crimes-against-humanity-extra-judicial-killings-by-kenya-police-exposed.pdf
2. 2015 has seen the frequency and devastation of the attacks escalate even further, with the most notable attack being the one that targeted Garissa University College, wherea reported 147 civilians were killed, including university students and staff. Other attacks attributed to Al Shabaab have taken place in the counties of Wajir, Mandera and Lamu seeking to stoke religious and ethnic divisions in these areas.
3. 'Kenya to target al Shabaab sympathisers in Nairobi,' BBC (2011). Available at: http://www.bbc.com/news/world-africa-15384331
4. Available at: http://www.bbc.com/news/world-africa-15384331
5. Security Laws (Amendment) Act 2014, Section 64. Available at: http://kenyalaw.org/kl/fileadmin/pdfdownloads/AmendmentActs/2014/SecurityLaws_Amendment_Act_2014.pdf
6. See Wikileaks: https://www.wikileaks.org/hackingteam/emails/?q=kensi.org
7. KHRC. 'The Internet Legislative and Policy Environment in Kenya' (2014). Available at: http://www.khrc.or.ke/mobile-publications/civil-political-rights/34-the-internet-legislative-and-policy-environment-in-kenya/file.html
8. 'Inside Kenya's Death Squads,' Al Jazeera (2014). Available at: http://interactive.aljazeera.com/aje/KenyaDeathSquads/
9. Available at: http://interactive.aljazeera.com/aje/KenyaDeathSquads/
10. Available at: http://interactive.aljazeera.com/aje/KenyaDeathSquads/
11. See Bloggers Association of Kenya (BAKE): http://www.blog.bake.co.ke/2016/01/24/bake-condemns-the-arrest-and-intimidation-of-kenyans-online/

Surveillance at a glance in Kenya

Do citizens know more now than they did three years ago about the government's surveillance activities?
Yes

Did the Snowden disclosures lead to meaningful public debate in your country about the proper limits on government surveillance?
No

Since the Snowden disclosures, have any whistleblowers come forward to inform the public about government surveillance activities?
Yes

In the last three years, have the government's national-security surveillance authorities been narrowed, expanded, or neither?
Expanded

In the last three years, have new structural checks (e.g. new transparency requirements) been imposed on intelligence agencies?
No

If the legislature/parliament is considering new legislation relating to government surveillance, would that legislation narrow the government's surveillance powers or expand them?
Expand them

If the legislature/parliament is considering new legislation relating to government surveillance, would that legislation impose new structural checks?
No

Over the last three years, have the government's national-security surveillance authorities been the subject of domestic litigation, including in constitutional courts?
Yes

Over the last three years, have the courts rejected as incompatible with constitutional or human rights law any aspect of government surveillance?
Yes

Over the last three years, do you think the public has come to trust the intelligence agencies more, less, or neither?
Less

Spying for others: troubling cases of transnational surveillance

10
SOUTH AFRICA

Kumi Naidoo, then head of Greenpeace, talks in front of a two-story-high, mechanically operated polar bear called Aurora installed by activists from Greenpeace during the COP21, United Nations Climate Change Conference in Le Bourget, north of Paris, France, on 9 December 2015.
Photo: Francois Mori/AP

SOUTH AFRICA

Spying for others: troubling cases of transnational surveillance

the kumi naidoo case

Kumi Naidoo, a South African national, has deep roots as an activist. Growing up in apartheid-era South Africa, Naidoo began organising his community in his early teens, working with neighbourhood youth and mobilising mass demonstrations against the apartheid regime. In 1980, when he was only 15 years old, he was arrested, expelled from secondary school and threatened with a 15-year jail sentence. Naidoo went underground in South Africa for some time and eventually sought exile in England, where he pursued postgraduate studies at the University of Oxford. Naidoo returned to South Africa a month after Nelson Mandela was elected president, and he worked as a researcher, journalist, university lecturer and youth counsellor, and for ten years directed CIVICUS, an international NGO focused on civic participation.

In 2009 Naidoo joined Greenpeace as its international executive director. Persuaded to take on the position by his daughter Naomi, Naidoo saw his role as the executive director of Greenpeace as an alliance builder and an agent of change. Importantly, he saw the intricate connections between environmental justice, women's rights and human rights, and he approached his work with the aim of bolstering all three.

In early 2015 the Al Jazeera news network obtained leaked intelligence cables revealing that South Korea had identified Naidoo as a possible security threat during the G20 summit that took place in Seoul, South Korea, in November 2010. According to the cables, South Korea had asked South Africa for 'specific security assessments' of Naidoo, linking him with two other South Africans who had been swept up in an anti-terrorist raid in Pakistan (but who were later released and returned to South Africa). South Africa never informed Naidoo of South Korea's request – a phone call from an Al Jazeera reporter was the first he heard of it – and he still has no idea whether the state complied with the request, or whether anything was done with any information that may have been provided in response.

Naidoo understandably found the leaked cable distressing. As he stated to a reporter when he learned about the possible surveillance:

My main reaction when I was contacted by Al Jazeera was not one of surprise or frustration or anger, it was one of sadness, hurt and deep disappointment.[1]

Naidoo had visited South Korea several times, and he believes its intelligence service made the request because of his outspoken opposition to nuclear power. No stranger to surveillance in his youth, Naidoo was concerned that the South African government may be revisiting old habits of the post-apartheid era. For now, though, what Naidoo seeks most of all are answers; as he commented in the same report:

I want to believe that I will get the confirmation from my government saying that it's not been the case and they did not share information on me with any external, whether it's South Korean or other agencies.

In July 2015, the Legal Resources Centre (LRC) issued an access to information request on behalf of Naidoo to the State Security Agency for records relating to the requested surveillance operation. The LRC specifically asked for:

— the request for information received from South Korea mentioned in the cable leaks regarding Naidoo, Greenpeace and its members;
— South Africa's response to the South Korean request for information regarding Naidoo, Greenpeace and its members;

— any agreement, memorandum of understanding or other document providing for, facilitating, encouraging or otherwise contemplating the sharing of intelligence between South Africa and South Korea;
— any request for information received from any country regarding Naidoo, Greenpeace and its members, and any response provided by South Africa in reply; and
— any request for an interception order requested or granted under the relevant South African legislation.

The State Security Agency has not issued any response to that request. That inaction is deemed a refusal of the request under South African law. The LRC then lodged an internal appeal but again no response was forthcoming. Under the access to information laws, the next step, then, would make it necessary to institute court proceedings in terms of the Promotion of Access to Information Act 2 of 2000 in order to gain access to the requested information.

Meanwhile, the South African government's public response to the leaked information suggesting it may have been surveilling a citizen, who is a world-renowned, peaceful activist, has been especially troubling. Rather than opening a dialogue about the possible surveillance activities, the government condemned the leaks and indicated that a full investigation – into the leaks, not the possible surveillance of Naidoo – had been launched. In a statement dated 25 February 2015, the minister of state security stated that:

While it is an international practice for countries to share intelligence on cross cutting issues pertaining to economic opportunities and security matters amongst others, the leaking of the purported documents detailing operational details of the State Security Agency is condemned in the strongest possible terms.

In terms of the legal and policy framework governing South African management of classified information, it is illegal to disclose such information outside of the classification protocols in place. Such conduct has the dangerous effect of undermining operational effectiveness of the work to secure this country and borders on undermining diplomatic relations with our partners in the international community. Any leakages of classified information undermine the national security of any state.

A full investigation has been launched into the purported leakage, its veracity and verification will be handled in terms of the protocols governing the management of classified information.[2]

Members of the leading parliamentary opposition party, the Democratic Alliance, warned that these revelations could be used as an excuse to press ahead with a pending Protection of State Information Bill that contained provisions that civil society organisations were already cautioning could have a chilling effect on whistleblowers and journalists. The Right2Know campaign, a civil society group, echoed the warning:

We fully expect that locally South Africa's state security structures will paint these leaks as a hostile act, and use this event to seek greater control over the flow of information, these leaks may even be used as a pretext to sign the Protection of State Information Bill into law… It is telling that this important act of journalism would easily fall under the secrecy bill's broad and expansive definition of 'espionage', which carries penalties of up to 25 years in jail, and has no public interest defence.[3]
Naidoo, too, expressed disappointment at the government's response to the cable leaks:

What I don't see in the cables that are available is in fact a denial from the South African government to the

> In early 2015 the Al Jazeera news network obtained leaked intelligence cables revealing (...) South Korea had asked South Africa for 'specific security assessments' of Naidoo.

South Koreans, saying: 'This is a citizen of ours who was part of the liberation struggle who had been supporting democracy and human rights since the age of 15 and we do not believe there's any reason for you to [make this request]'.[4]

the context

For many years, political activists in South Africa have raised concerns that state intelligence structures may be monitoring their work even in the post-apartheid era, and that intelligence agencies may be abusing their powers. While some have dubbed this trend 'the rise of the securocrats' for the way in which South Africa's security cluster is being seen as becoming increasingly secretive, powerful and involved in political affairs, in the country[5] others question whether South Africa's intelligence services ever truly reformed in the democratic era.

One of the most significant surveillance sagas in South Africa has been in relation to the so-called spy tapes. The tapes contain recordings made by intelligence officials of conversations between the former head of the crime investigation unit (referred to at the time as 'the Scorpions') and the former head of the National Prosecuting Authority relating to corruption charges brought against President Jacob Zuma in 2007 for his alleged involvement in an arms deal scandal.[6] This had major political ramifications for all involved, and was perhaps one of the most glaring demonstrations in the post-apartheid era of the reach of the intelligence services. Indeed, what this made clear was that no one was beyond surveillance, no matter what position the person may hold. As part of a court case challenging the decision to drop the criminal charges against President Zuma, it became possible for the tapes themselves to be made available to the public, thereby giving the public an idea of the kind of information that the security services were interested in.[7]

The impact of surveillance on the media and civil society is a particular concern. For example, in October 2011, the then Inspector General of Intelligence (IGI) confirmed that the telephone calls of a leading Sunday Times journalist had been monitored by the investigative unit of the South African Police Services.[8] The IGI insisted that the surveillance was 'part of a lawful investigative method' that 'was approved by the designated justice in respect of [the journalist] pertaining to the allegations of crime, and not for the reason that he is a journalist.' The journalist was subsequently arrested at the Sunday Times offices with his notebooks, computer and mobile phone having been seized. He was charged with fraud, forgery and uttering (an offence associated with the use of a forged document), but these charges were never prosecuted. The actions of the police service have been widely criticised as being nothing more than scare tactics to intimidate the journalist from revealing information that may have been detrimental to people in power. There have also been subsequent concerns raised that surveillance activities have been undertaken to spy on members of the media engaging in legitimate journalistic activities, and that this has been made possible by the low levels of oversight of the agencies involved.

Such incidents have raised serious concerns about the effectiveness of post-apartheid legislation that authorises surveillance and is meant to ensure that surveillance is carried out in a lawful manner with proper oversight. Because the intelligence services under apartheid South Africa were used routinely to harass political critics of the regime, since the transition to democracy in 1994, the new government has taken steps to revise the intelligence services' mandates. But a broad emphasis on national security has translated into a persistently broad mandate for the intelligence services.

In 2002, South Africa passed the Regulation of Interception of Communications and Provision of Communications Related Information Act, 2002 (RICA) to regulate surveillance of communications. Subject to certain exceptions, RICA requires the permission of a judge for the interception of communications upon 'reasonable grounds to believe' that a serious criminal offence has been, is being, or probably will be committed. RICA sets out the conditions for the granting of interception directives.

To guarantee the capacity of relevant state agencies to conduct interceptions, RICA requires

Protesters shout slogans during a rally denouncing the G20 Seoul Summit in Seoul, South Korea, on 10 November 2010.
Photo: Lee Jin-man/AP

that telecommunication service providers deliver telecommunication services that can be intercepted. RICA also requires all South Africans to register their subscriber identity module (SIM) cards with their mobile phone providers. While the constitutionality of RICA has yet to be tested, experts have proffered the view that certain provisions may not pass muster if challenged. Notably, there is no provision to require that those subjected to communication surveillance be notified that their communications have been intercepted, even after the completion of the relevant investigation. This means that the authorities are given a power that is almost entirely hidden from the public eye. For instance, even if the surveillance of Kumi Naidoo had been authorised under RICA, Naidoo would not have known about the surveillance unless information had been leaked to him. And even now that he knows about the possible targeting, there is no automatic recourse under RICA for him to better understand what surveillance activities were undertaken and why. These weaknesses violate the 'necessary and proportionate' principles that individuals should be notified of decisions authorising communications surveillance with enough time and information to enable them to appeal the decision, and should have access to the materials presented in support of the application for authorisation.[9]

However, surveillance under RICA is only part of the overall surveillance landscape in South Africa. For instance, the National Communications Centre (NCC), which houses the state's mass surveillance capabilities, has maintained the view that its activities are not regulated by RICA. If this is correct, this means that its operations are conducted outside of the law. The NCC has the power to collect and analyse 'foreign signals,' which include communications that emanate from outside the borders of South Africa but that pass through or end in South Africa, and communications metadata, all with little or no oversight or restriction. With regard to metadata, little is known about how metadata is collected and stored, or why it is necessary to store it for a period of 3-5 years. Furthermore, a warrant to access stored metadata need not be sought from the RICA judge; rather, it can be sought from any sitting magistrate or high court judge, for which no statistical reporting data is provided.

The enactment of the Protection of Personal Information Act, 2013 (POPI) holds the promise of a possible safeguard of the right to privacy. However, as of July 2016, the Information Regulator has yet to be appointed, and various key provisions of POPI, including the conditions for the lawful processing of personal information, are not yet operational.[10] Furthermore, also as of July 2016, the key position of the IGI, this being the functionary tasked under the South African Constitution to carry out civilian oversight of the intelligence services, has stood vacant since March 2015.

Right2Know activists protesting outside the hearings of the National Electricity Regulator of South Africa in Midrand on 4 February 2016.
Photo: Shayne Robinson

Overall, the South African public lacks meaningful information about the extent of surveillance in the country. The Joint Standing Committee on Intelligence (JSCI), this being the parliamentary committee tasked with overseeing the work of intelligence services in South Africa, is mandated to release public reports on the application of RICA. However, the report is typically scant in detail. The JSCI's most recent report does not provide any information on why any of the RICA interceptions were carried out, or on their outcome and effectiveness in preventing or investigating crimes. Meanwhile, there appears to be no centralised oversight or requirement of public disclosures of statistics on metadata collection and use, and telecommunications companies are barred from publishing information (including aggregated statistics) on both the interception of communications and metadata.[11] The JSCI also continues to operate a closed committee, despite repeated requests to open it to the public. The result is that South Africans remain largely in the dark about the workings – and targets – of the country's intelligence services.

conclusion

It is clear that at least some organisations and individuals are being monitored by state security structures in South Africa; yet it is unclear how this is being done, the reasons for the monitoring, or what use is being made of the information that has been collected. In some instances, there are serious concerns that the security structures may be over-zealous and overstepping their mandate. Furthermore, there are also serious concerns that the South African government shares information indiscriminately with foreign governments, without appropriate checks in place for the subjects of such information to be notified or challenge the information or the sharing.

What we do know is that the security services are looking to increase their capabilities. The most recent report of the JSCI warned that criminals are using more sophisticated electronic communications technology, and that the security agency urgently needs modern technology to intercept these electronic communications.[12] The report also indicated that, out of 202 surveillance requests submitted by the police, all 202 were granted. From the July 2015 leak of

> While some have dubbed this trend 'the rise of the securocrats' for the way in which South Africa's security cluster is being seen as becoming increasingly secretive, powerful and involved in political affairs, in the country others question whether South Africa's intelligence services ever truly reformed in the democratic era.

information from the Hacking Team, it was revealed that the South African government had expressed interest in the purchase of surveillance and hacking technology.[13] However, the chain of communication ends abruptly, leaving it unclear whether any equipment was ultimately purchased. Little is known about what surveillance capabilities the government presently has and uses. But the leaks have revealed at least some measure of political will on the part of the South African government to be equipped with this technology.

While the security services have an important role to play in appropriate circumstances, South Africa's history has shown how surveillance powers can easily be used to infringe basic rights. To these all-too recent memories add the fact that, with new technology, people simply may never know that they have been under surveillance. For South Africans, this combination of history and technology heightens the risk of intimidation – and the likelihood that surveillance, and the prospect of surveillance, will have a chilling effect on the work of activists, the media and politicians, and stifle the important role that they play in an open and accountable democracy.

an international twist

In South Africa, as in many emerging democracies in the world today, civil liberties organisations like the LRC are devoting more time to challenging expanding surveillance powers and safeguarding privacy rights at home. But the revelations by Edward Snowden of a vast architecture of international digital surveillance led by the United States and its partners in the so-called Five Eyes brought another preoccupation as well: the possibility that civil liberties and non-governmental organisations anywhere on Earth are being watched not just by their own governments but by spy agencies operating continents away. And so in July 2014 ten human rights organisations[14] (six of whom are INCLO members) joined together to try to establish whether their organisations had been under the surveillance of the British Government Communications Headquarters (GCHQ) through its mass surveillance programmes.

The organisations filed a complaint with the Investigatory Powers Tribunal (IPT) challenging the legality of GCHQ's mass surveillance programmes. The IPT is a special court established to hear complaints of unlawful surveillance, to determine whether those programmes are contrary to human rights protections contained in the United Kingdom's Human Rights Act and the European Convention on Human Rights (ECHR). It is the only court in the United Kingdom that can hear cases against the security services.

> “[T]he revelations by Edward Snowden of a vast architecture of international digital surveillance led by the United States and its partners in the so-called Five Eyes brought another preoccupation as well: the possibility that civil liberties and non-governmental organisations anywhere on Earth are being watched not just by their own governments but by spy agencies operating continents away.”

The case, aimed at uncovering the truth about transnational mass surveillance programmes and determining whether those programmes were capturing the communications of these organisations and clients, posed enormous and unique challenges – not least of all because, under UK law, the state is not required to inform you that you have been subjected to spying, even if you have done nothing to warrant surveillance and the surveillance activities reveal that you are beyond reproach. Had it not been for Snowden's leaks revealing that the UK and US governments were conducting mass interception programmes and sharing information with each other and other international partners, the organisations would never have known the extent of surveillance and could not have made it over the first, and often fatal, hurdle for seeking to challenge state surveillance programmes.

This, however, was not the only hurdle. Throughout the course of the litigation, the UK government maintained its policy of 'neither confirm nor deny'; it would not admit to its mass surveillance programmes, nor would it say that they did not exist. This was despite the fact that the US government had already acknowledged that Snowden's revelations about its parallel PRISM programme and upstream collection, were true. The IPT's response to this was to examine the law based on a compromise: the hearing would proceed on the basis of an assumed hypothetical factual premise, that mass surveillance as revealed by Snowden takes place.

Further, and perhaps most difficult, was that the ten organisations were only allowed to participate in some of the IPT hearings. The IPT held at least one closed hearing, attended only by the court members, the government and its representatives. The human rights organisations were not represented at this hearing, or provided with a summary of the material presented to the IPT during that session (despite repeated requests to the IPT for all the information provided in secret to be disclosed, each of which was refused). Beyond the obvious issues of the unfairness of excluding one side from the legal process, this approach led to profound practical difficulties and confusion.

For example, following the closed hearing the IPT told the UK government that some of the material it had presented to the tribunal in secret must be disclosed to the ten organisations. The government therefore produced a note that appeared to set out how the UK government handles intercepted material it receives from foreign governments. But the status of the note was unclear: was this part of a policy document, and, if so, was it the whole policy or a summary? The IPT refused a request for an explanation of what the document was and how the government had sought to rely on it in the closed hearing. Three different versions of the document were presented to the organisations at

People use masks with the face of former NSA contractor Edward Snowden during the testimony of Glenn Greenwald, before a Brazilian Congressional committee on NSA's surveillance programmes, in Brasilia, on 6 August 2013.
Photo: Reuters/Latinstock

various times, each with a different series of corrections. But no explanation of what the notes meant was forthcoming, from either the government or the IPT.[15]

Even with such obstacles, for the first time in its 11-year history the IPT made a finding against the government in the complaint filed by the ten human rights organisations. It held that the process that the UK government used for receiving information that the US government had gathered via PRISM or upstream collection had been unlawful for years – and was unlawful specifically because the safeguards for looking at any shared material were not sufficiently known to the public. But the court accompanied this finding with another concluding that, thanks to the disclosures made during the litigation, the safeguards were now sufficiently public and the regime was compliant with human rights. Those historic disclosures, according to the court, were the contents of the mystery note.

Disappointingly, the IPT decided that the UK government's mass surveillance programmes did not constitute a human rights violation. Rather, it stated that mass surveillance was in fact an 'inevitable' consequence of modern technology, and the powers granted in the Regulation of Investigatory Powers Act, 2000 allowed the British government to spy on foreign nationals without a warrant identifying the subject of surveillance.

However, in June 2015, the IPT delivered a further ruling in which it revealed that two of the plaintiff organisations had been subjected to unlawful surveillance by GCHQ. The LRC was one of the two organisations.[16] In relation to the LRC, the IPT found that 'communications from an email address associated with the [LRC] were intercepted and selected for examination pursuant to s 8(4) of [the Regulation of Investigatory Powers Act]. The [IPT] is satisfied that the interception was lawful and proportionate and that the selection for examination was proportionate, but that the procedure laid down by GCHQ's internal policies for selection of the communications for examination was in error not followed in this case'.

The IPT concluded that this was a violation of article 8 of the ECHR, but that it was satisfied that 'no use whatever was made by the intercepting agency of any of the intercepted material, nor any record retained.' Consequently, it ruled that the LRC had not suffered any material detriment, damage or prejudice, and no award of compensation was made.

As summed up by Janet Love, the National Director of the LRC, at the time of the ruling:[17]

[The LRC is] deeply concerned to learn that communications of our organisation have been subject to unlawful interception by GCHQ. As a public interest law firm, our communications are self-evidently confidential, and we consider this to be a serious breach of the rights of our organisation and the individuals concerned.
We can no longer accept the conduct of the intelligence services acting under such a pernicious veil of secrecy, and we will be taking immediate action to try to establish more information. We urge the South African and British governments to cooperate with us in this regard.

Domestically, following the IPT ruling, the LRC filed an access to information request to the State Security Agency, seeking the following information:

— any request for information relating to the LRC or its members received from the UK government;
— any response provided in reply to any such request for information;
— any agreement, memorandum of understanding or other document providing for, facilitating, encouraging or otherwise contemplating the sharing of information between South Africa and the United Kingdom;
— any request for information regarding the LRC or its members received from any other country, and any response provided in response thereto;
— any request for any order or direction sought in terms of the relevant legislation relating to the LRC or its members

To date, no response has been received to this request.

The IPT ruling left more questions than answers for the LRC, as well as for the other organisations involved in the complaint. As there is currently no right of appeal against judgments of the IPT and considering the gravity of harm posed by such a practice being deemed legal, the ten organisations have now taken this matter to the European Court of Human Rights (ECtHR). In December 2015, the ECtHR decided that it would hear the matter, and deemed it a 'priority.' The UK government responded in April 2016 and the claimants now have to respond by 26 September 2016.

The decision of the ECtHR will constitute one of the first times that a regional human rights tribunal will rule on the lawfulness of speculative mass surveillance regimes in the post-Snowden era. In the face of government intransigence and stymied domestic legal systems, this is a key opportunity for the ECtHR to affirm and give content to the right to privacy, and insist on accountability from states.

notes

-

1. 'Greenpeace head Kumi Naidoo saddened at spying revelations,' The Guardian (26 February 2015). Available at: http://www.theguardian.com/world/2015/feb/26/greenpeace-head-kumi-naidoo-saddened-at-spying-revelations
2. Available at: http://www.theguardian.com/world/2015/feb/26/greenpeace-head-kumi-naidoo-saddened-at-spying-revelations
3. 'South Africa scrambles to deal with fallout from leaked spy cables,' The Guardian (24 February 2015). Available at: http://www.theguardian.com/world/2015/feb/24/south-africa-scrambles-to-deal-with-fallout-from-leaked-spy-cables
4. 'Greenpeace head Kumi Naidoo saddened at spying revelations,' Mail & Guardian (27 February 2015). Available at: http://mg.co.za/article/2015-02-27-greenpeace-head-kumi-naidoo-saddened-at-spying-revelations
5. Right2Know's activist handbook, 'Big Brother Exposed,' p. 2
6. Corruption Watch. 'Spy Tapes Saga: The Latest' (22 August 2013). Available at: http://www.corruptionwatch.org.za/spy-tapes-saga-the-latest
7. 'UPDATE: NPA files "spy tapes" papers,' eNews Channel Africa (3 July 2015). Available at: https://www.enca.com/south-africa/will-npa-file-spy-tapes-papers
8. 'Hawks bugged reporter's phone,' Mail & Guardian (2 October 2011). Available at: http://mg.co.za/article/2011-10-02-hawks-bugged-reporters-phone
9. 'International Principles on the Application of Human Rights to Communications Surveillance' (May 2014). Available at: en.necessaryandproportionate.org/text
10. Even once POPI is fully in force, there will still be a one year grace period before compliance is required, which can be extended further by the responsible Minister.
11. Vodafone. 'Law Enforcement Disclosure Report: Updated Legal Annexe February 2015.' Available at: https://www.vodafone.com/content/dam/sustainability/2014/pdf/operating-responsibly/law_enforcement_disclosure_report_2015_update.pdf. For an overview of the structure of the security services, see http://www.ssa.gov.za/AboutUs/LegislationOversight.aspx
12. ´Moderne tegnologie fnuik glo SA se spioene, ´Netwerk 24 (27 January 2016). Available at: http://www.netwerk24.com/Nuus/Politiek/moderne-tegnologie-fnuik-glo-sa-se-spioene-20160127
13. 'Hacking Team failed to crack SA,' IT Web (14 July 2015). Available at: http://www.itweb.co.za/index.php?option=com_content&view=article&id=144683
14. The American Civil Liberties Union, Amnesty International, Bytes for All, the Canadian Civil Liberties Association, the Egyptian Initiative for Personal Rights, the Hungarian Civil Liberties Union, the Irish Council for Civil Liberties, the Legal Resources Centre and Privacy International
15. Interestingly, around the same time, in a different case before the same court, the government was forced to publish what looked like the full policy document on which the note was based, but the IPT still would not require the government to produce the full document in this case.
16. [2015] UKIPTrib 13_77-H_2. The IPT initially indicated that the Egyptian Initiative for Personal Rights was the other organisation that had been subjected to unlawful surveillance. However, a few days after issuing this ruling, the IPT retracted its initial statement, and indicated that the affected organisation was Amnesty International instead. It remains unclear how such a mistake could have been made.
17. Available at: https://www.theguardian.com/uk-news/2015/jun/22/gchq-surveillance-two-human-rights-groups-illegal-tribunal

Surveillance at a glance in South Africa

Do citizens know more now than they did three years ago about the government's surveillance activities?
More. While much of the state's surveillance activities still take place in secret, more is known through investigative journalism and leaks of information that have taken place over recent years.

Did the Snowden disclosures lead to meaningful public debate in your country about the proper limits on government surveillance?
Yes. More organisations have become actively engaged in issues relating to surveillance, which in turn has led to an impetus towards meaningful public debate and demands for more openness and accountability more broadly.

Since the Snowden disclosures, have any whistleblowers come forward to inform the public about government surveillance activities?
Yes. Information has been leaked to the media about surveillance activities taking place.

In the last three years, have the government's national-security surveillance authorities been narrowed, expanded, or neither?
Unsure. Although there has been significant restructuring of the intelligence services, it is difficult to ascertain whether this has involved the authorities being narrowed or expanded.

In the last three years, have new structural checks (e.g. new transparency requirements) been imposed on intelligence agencies?
Not in terms of national legislation.

If the legislature/parliament is considering new legislation relating to government surveillance, would that legislation narrow the government's surveillance powers or expand them?
N/A

If the legislature/parliament is considering new legislation relating to government surveillance, would that legislation impose new structural checks?
N/A

Over the last three years, have the government's national-security surveillance authorities been the subject of domestic litigation, including in constitutional courts?
No

Over the last three years, have the courts rejected as incompatible with constitutional or human rights law any aspect of government surveillance?
No

Over the last three years, do you think the public has come to trust the intelligence agencies more, less, or neither?
Less. This is speculative, but in view of the increased awareness of the nature and scale of surveillance activities, and what appears to be rising public concern in this regard, it would seem that the public is more circumspect about the intelligence agencies.

conclusion and recommendations

conclusion and recommendations

Argentina, Canada, Hungary, India, Ireland, Israel, Kenya, Russia, South Africa, the United States: all of these countries are democracies, some of them long-established, some recently emerging from more authoritarian systems and still struggling to develop stable, sustaining democratic institutions. All of them, old and new democracies alike, have seen dramatic expansions of surveillance powers and activities in recent years.

And as this report vividly illustrates, there have been real harms from these expanding powers: harms to individuals and their civil and human rights; harms to public trust and to the climate for political activism and dissent; and harms to the rule of law and the very fabric and structures of democratic states.

The cases of Ibraheim 'Abe' Mashal from the United States, the military veteran who found he was barred from flying on the basis of innocuous personal emails, and of Rateb Abu-Krinat from Israel, a minority rights activist called in for a meeting with state security agents who insinuated they were monitoring his communications and activities, read like stories from behind the Iron Curtain, where citizens suddenly came face to face with a vast, subterranean surveillance state. The case of Re (X), two Canadian citizens whose identities we do not know and who themselves will likely never know they were being monitored both by their government and its foreign partners, suggests how borderless and faceless surveillance powers can be in the digital age. And the South African case of Kumi Naidoo shows how, in this new age, such transnational co-operation can turn one country's respected activist into a surveillance target for another country.

In even the most entrenched democracies, powerful new surveillance tools and technologies are opening or reopening vulnerabilities for communications and institutions that depend on confidentiality – as when new surveillance technologies are used to monitor conversations of opposition politicians in India, or when

an ombudsman empowered to oversee Ireland's national police comes to believe that the watchdog is the one being watched.

Meanwhile, in countries with emerging democracies and fresh memories of authoritarian regimes, the new surveillance powers can seem as much of an extension of the repressive habits and structures of the past as a new threat to privacy and personal security. A country like Argentina that has struggled to rebuild a democratic state after the crimes committed during the dictatorship finds that its intelligence services' surveillance powers remain potent and murky political tools. The security services in Hungary, a country that only recently shrugged off decades of political oppression, are now testing an all-seeing surveillance system that seems like the modern embodiment of its communist-era surveillance state. In an emerging democracy such as Kenya, which is struggling with a dire terrorism threat, intelligence gathered with new digital powers leads not to more effective policing and convictions but instead to a resurgence of death squads and extrajudicial killings. And in Russia, domestic spying on rights activists is a vivid reminder that its transition to democracy was never complete.

Both internationally and in each of these countries, there are laws that limit surveillance powers. International law – including, in particular, the International Covenant on Civil and Political Rights (ICCPR) – requires that states ensure that any interference with the right to privacy comply with the fundamental principles of legality, proportionality and necessity. And each of the ten countries in this report has a body of domestic law that is meant to protect privacy and keep surveillance in check. But in seeking to ensure that their governments meet these standards in conducting the surveillance operations described in this report, the ten contributing INCLO member organisations and our colleagues in the civil and human rights communities have encountered a common set of challenges.

We have faced poorly defined legal frameworks regulating surveillance powers and safeguarding individual rights. We have contended with a lack of transparency regarding laws and practices governing traditional and digital surveillance in our countries, and we have dealt with feeble or insufficient mechanisms for overseeing intelligence gathering operations. And when individual rights have been violated, we have struggled to find legal avenues to pursue redress and accountability.

In cases where the surveillance operations have been conducted extraterritorially, we have discovered troubling discrepancies in the ways that governments protect the privacy rights of their own citizens but disregard those of people living beyond their borders. We have found that the same pervasive secrecy, poor oversight and lack of accountability plague these new and expansive powers, and yet we find we have even fewer measures to challenge and rein in transnational spying and to prevent the sharing of unlawful surveillance across borders.

Ending such abuses, and preventing them in the future, will require concerted action at both the national and international level. At the national level, states need to take additional steps to better protect the right to privacy and other human rights in their surveillance practices; prohibit mass surveillance; enhance oversight of intelligence services and surveillance powers; impose limitations on extraterritorial surveillance and information sharing; and enhance protections for national-security whistleblowers. At the same time, in a world where digital surveillance powers can and often do have a global reach, more must be done to articulate a strong, clear framework that protects the fundamental human right to privacy internationally. To this end, we are urging all states to support additional clarifications and global standards to ensure that the citizens of all nations enjoy equal protection from unwarranted surveillance.

recommendations to governments worldwide

Respect and ensure the human right to privacy, both offline and online

Respect and ensure for all individuals within its territory and subject to its jurisdiction and control, the right to privacy – both online and offline – and ensure it is more fully articulated in national and international laws, including Article 17 of the ICCPR, without distinction of any kind such as race, colour, sex, language, religion, political or other opinion, national or social origin, birth or any other status.

Recognise a legal duty to respect and ensure the right to privacy and other human rights of persons outside its territory when it acquires, processes, uses, stores or shares their personal data.

Respect and ensure the right to privacy in information sharing between governments

Disclose information necessary for assessing the compatibility of intelligence sharing agreements and practices with human rights obligations, including the right to privacy of affected individuals, and prohibit all such agreements or practices that violate those standards.

Ensure that privacy and other human rights principles underpin information sharing agreements and practices, including limitations on use, retention, dissemination, access and destruction of information. Information sharing should be subject to written caveats to ensure these safeguards are observed.

Narrow the scope of surveillance powers

Review all laws, policies and practices to ensure that all intelligence activities, including surveillance operations, are consistent with international human rights obligations, in particular the rights to privacy and freedom of expression.

Ensure that surveillance and other intelligence activities are conducted on the basis of a legal framework that is publicly accessible, precise, comprehensive, non-discriminatory and clearly defined.

Ensure that all surveillance operations are carried out in accordance with publicly available laws, policies and practices and pursuant to judicial authorisation and, at a minimum, are a necessary and proportionate means of pursuing a legitimate governmental objective and are minimally intrusive of the right to privacy – even in relation to surveillance for national security purposes.

End and prohibit mass surveillance

Recognise that mass, bulk or indiscriminate surveillance is an unlawful and practically always disproportionate interference with the right to privacy. Adopt measures to end and prohibit such practices.

Enhance oversight of intelligence agencies and surveillance operations

Ensure that effective, independent, accountable and transparent oversight and review bodies for intelligence activities are established for all intelligence agencies and other government bodies involved in surveillance operations, and ensure that they are properly resourced.

Disclose all surveillance laws, policies and practices and relevant legal interpretations of those authorities to the oversight/review bodies, and take all other steps necessary to ensure effective oversight of intelligence agencies and other government bodies involved in surveillance operations.

Provide redress for violations of the right to privacy

Provide effective legal and procedural guarantees against excessive, inappropriate or non-judicially authorised collection and use by intelligence agencies of personal information.

Provide access to effective judicial and other remedies for persons – irrespective of their national origin or country of residence – who have a reasonable basis for believing that they have been under surveillance in violation of their rights.

recommendations to the united nations

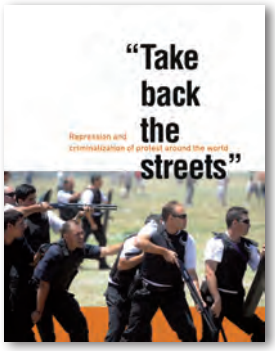
Enhance protections for national-security whistleblowers

Strengthen legal protections for national-security whistleblowers and prohibit the prosecution of those who are not government employees or contractors for disclosing information that exposes official wrongdoing or information of great interest to the media, where the public interest in disclosure outweighs any specific harm to national security or a comparable state interest caused by disclosure.

The UN Human Rights Committee should review and update General Comment 16 to Article 17 (right to privacy) of the ICCPR to provide guidance to states on their obligations to respect and guarantee the right to informational privacy under the ICCPR.

Support the United Nations Special Rapporteur on the right to privacy in clarifying relevant standards and enforcing those standards globally, including in particular standards applicable to mass digital surveillance.

OTHER REPORTS BY INCLO ARE

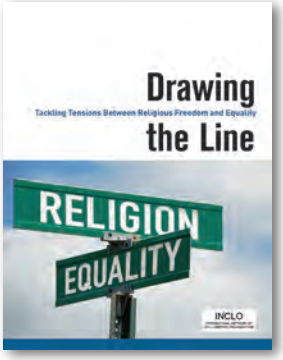


"Take back the streets: Repression and criminalization of protest around the world" includes case studies with contemporary examples of distinct state reactions to activism and protest in unique domestic contexts. The cases highlight instances of excessive use of force resulting in injury and death, and discriminatory treatment and criminalisation of social leaders. All the cases show the integral role played by civil society organisations in protecting these fundamental democratic rights.

You can find the report online at:
http://www.inclo.net/pdf/take-back-the-streets.pdf

"Lethal in disguise: The health consequences of crowd-control weapons" This is a joint report between INCLO and Physicians for Human Rights, which documents the health consequences of crowd-control weapons, examines their role and limitations in protest contexts, and makes recommendations for their safe use. The aim of the publication is to raise awareness about the misuse and abuse of this type of weapons, their detrimental health effects, and the impact of their use on the meaningful enjoyment of the rights to freedom of assembly and expression.

You can find the report online at:
http://www.inclo.net/pdf/lethal-in-disguise.pdf



"Drawing the line: Tackling tensions between religious freedom and equality" draws on the expertise of INCLO members across five continents in analysing cases where religion and equality claims have competed in the courts. It proposes resolutions to tensions in three areas: LGBT rights, reproductive rights and religious appearance. The report articulates a fundamental principle for resolving tensions between religion and equality: religious freedom means the right to our beliefs, a right that is fundamental and must be vigorously defended; however, religious freedom does not give us the right to impose our views on others, including by discriminating against or otherwise harming them.

You can find the report online at:
http://www.inclo.net/pdf/drawing-the-line.pdf

INCLO

INTERNATIONAL NETWORK OF
CIVIL LIBERTIES ORGANIZATIONS