PRIVACY INTERNATIONAL

Their Eyes On Me

Stories of surveillance in Morocco

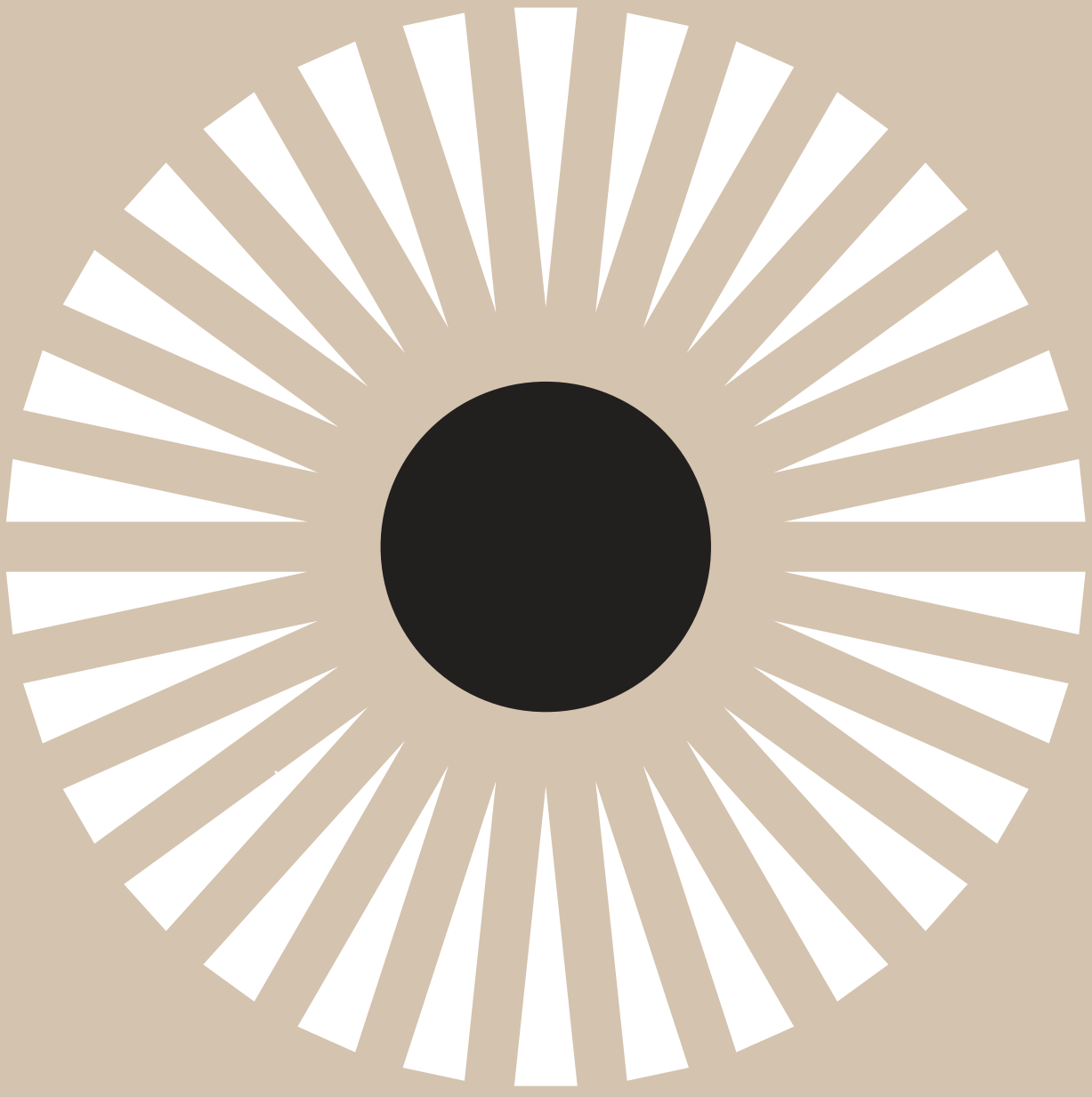




Photo © Anthony Drugeon

Their Eyes on Me

Stories of surveillance in Morocco

PRIVACY INTERNATIONAL

www.privacyinternational.org



Photo © Anthony Drugeon

Table of Contents

Foreword	07
Introduction	08
Hisham Almiraat	14
Samia Errazzouki	22
Yassir Kazar	28
Ali Anouzla	32



Photo © Anthony Drugeon

Foreword

Privacy International is a charity dedicated to fighting for the right to privacy around the world. We investigate the secret world of government surveillance and expose the companies enabling it. We litigate to ensure that surveillance is consistent with the rule of law. We advocate for strong national, regional and international laws that protect privacy. We conduct research to catalyse policy change. We raise awareness about technologies and laws that place privacy at risk, to ensure that the public is informed and engaged.

We are proud of our extensive work with our partners across the world. In particular, over the past year we have been working in 13 countries to assist local partner organisations in developing capacities to investigate surveillance and advocate for strong privacy protections in their country and across regions.

Morocco is one of the key countries of focus, having met with activists dedicated to defending the internet and more specifically the inviolability of electronic communications. Hisham Almiraat – both a subject of surveillance and a passionate privacy advocate – has been at the forefront of this battle, with his new organisation, Association des Droits Numériques.

In this report we present four stories of Moroccan citizens, including Hisham, placed under surveillance and the effect it has had on their lives and the lives of their families.

We feel that these stories say a lot about the current context of surveillance in Morocco. We hope they will serve as a medium to foster a much-needed public debate. We also hope that this debate will extend beyond Morocco as we all consider the dangers of unregulated surveillance and surveillance technology around the world.

Privacy International and the Association des Droits Numériques

Introduction

Surveillance creates power. Secret surveillance by Governments, state agencies and corporations is the most dangerous form because as individuals we cannot easily hold that power in check. The harm of covert spying is not always known to the individual. We can't see it. The violator does not have to be in the presence of the victim. Privacy is one of the few rights where the violation may leave no trace at all. It is sometimes impossible to identify the violator and hold them to account.

There's something extremely unsettling about having your personal space invaded and watched. It is like there is a person hiding in a dark corner wherever you go, recording everything you do. However, with modern technology it is now likely you will never see them, never know their names, never know their faces, and indeed never know their intentions.

So it is a rare thing to meet the victims of surveillance, let alone know how they were spied on, for what purposes, and by whom. For over a year, Privacy International has met, spoken with, and recorded conversations with political activists and journalists in Morocco who were spied on by the Government and organisations associated with those in power. Working with our local partner organisation, the Association des Droits Numériques (Organisation for Digital Rights), we have documented several startling and unnerving cases of intrusive and ongoing surveillance in Morocco.

Some had been targeted by expensive and sophisticated spyware from the Italian surveillance company Hacking Team. The interdisciplinary laboratory Citizen Lab suspects that Hacking Team, based in Milan, has sold its spyware 'Remote Control System' to an estimated 21 countries in the last 12 months. The list of countries includes Azerbaijan, Egypt, Ethiopia, Kazakhstan, Saudi Arabia and Sudan, all known for their governments' poor records on the protection of human rights.

Some of the surveillance in Morocco was done through digital methods. Journalists and activists had their email and Facebook accounts hacked by groups of nationalist hackers – malicious activities that have been left unpunished.

And some of the surveillance was done through more traditional, yet intimidating and legally questionable, police tactics. Stories of neighbours and relatives being visited by law enforcement agencies to obtain information – or to intimidate activists – were told on several occasions. Cases of phone tapping were also described.

Surveillance Goal: Preventing the spread of a "Moroccan Spring"

The following stories are best read in light of what is already known about Morocco and its heavy investment in spying on its citizens activities and squashing dissent.

Morocco is officially a parliamentary constitutional monarchy. Moroccan citizens elect their members of parliament every five years. However, the executive – led by the King – has extensive powers that impact the legislative and judicial institutions, because he has the right of veto. The Monarchy and the on-going conflict in the disputed region of Western Sahara are the most sensitive political topics in the country. Limitations on freedom of expression remains one of the major human rights issues, which has been stressed multiple times by various civil society organisations and non-governmental organisations (NGOs).

The country is ranked 116 (out of 167) in the 2014 Economist Intelligence Unit Democracy Index – therefore falling into the "authoritarian regime" category. The index ranks countries based on criteria including electoral process and pluralism, functioning of government and civil liberties.

Privacy International has also witnessed and indeed experienced the increasing number of bans on events organised by NGOs in 2014. Privacy International had sponsored two workshops organised by our partner, Association des Droits Numériques (Organisation for Digital Rights) which had to be relocated because of police pressure on international hotels and conference venues.

The Government had already been exposed in 2011 for having invested €2 million in a surveillance system named Eagle, that allows the Government to perform censorship and mass monitoring of internet traffic, with a technique referred to as Deep Packet Inspection. Eagle was developed by Amesys Bull, a French company that infamously sold a similar technology to the Libyan government under Muammar Gaddafi.

More recently, following pressure from Privacy International and Swiss journalists, the Swiss government released a document that revealed the list of countries that bought surveillance technologies from Swiss companies. Among the purchasers of advanced surveillance technology was Morocco, that appeared to have tested mobile telecommunication interception or jamming equipment in 2013-14.

In Morocco, 2011 was characterised by the February 20th Movement, a series of protests demanding democracy and more accountability from the government. Surveillance by the Moroccan Government and other state agencies has increased considerably since the Arab Spring, and ramped up further since the February 20th Movement.

The police were keen to identify any activists related to the movement. Some of the activists we interviewed reported that the Police visited their relatives and neighbours to question them about their involvement in the February 20th Movement.

Maria Moukrim is a well-known journalist and the Editor-in-Chief of the publication Febrayer ("February"). When she launched her website in 2012 it was targeted by a nationalist hacker group. Moukrim told Privacy International that it was hacked specifically because the hackers believed that it was directly affiliated to the movement.

"They thought it was going to be the official website of the February 20th Movement. They hacked into my Gmail account to obtain the password to the server and then bought all the domain names containing the word "Febrayer." Then they hacked into my Facebook account and posted some very offensive content. They then redirected all the Febrayer URLs to my Facebook account. It was a very traumatic event for the launch of this publication."

€200,000: the price worth of a journalist's privacy

More intimately, this report aims at portraying the experiences of four journalists and activists who have been personally targeted by state surveillance. Three of them – Hishaam Almiraat, Samia Errazzouki and Yassir Kazar – were part of Mamfakinch, a collective of citizen journalists born out of the February 20th Movement who are critical of the Government. Mamfakinch was targeted using spyware developed and sold by Hacking Team. An email sent out via the contact form on the Mamfakinch website was forwarded to the whole editorial team. The email suggested the attached document would reveal a major scandal. What the attached document actually contained was spyware, which granted the attacker complete remote access to the target's computer. Such spyware allows the attacker to:

- Access any content stored on the computer
- Monitor in real time the use of the computer and what appears on the screen
- Log all the keys that are being hit, therefore giving away any passwords that are typed
- Capture screenshots
- Activate the computer's webcam and take pictures and videos.

The spyware costs an estimated €200,000. Hacking Team claims to sell solely to government and law enforcement clients.

Since February 2014, Mamfakinch has been inactive. The team is divided as to what led to the end of the publication. For some, it was a necessary break as the February 20th Movement it was originally meant to cover had ended. But for others, including co-founder Hishaam Almiraat, the team of Mamfakinch gradually left out of fear. The use of Hacking Team's spyware had suddenly raised the stakes: if the Government was ready to invest such vast amounts of money on discovering who was doing what, those who had a career to protect felt that it was time to leave.

Hacker militias: zealous citizens or intelligence agents by another name?

Our last portrait focuses on a well-known figure in Morocco, Ali Anouzla. Anouzla is an investigative journalist and Editor-in-Chief of the independent online media Lakome, blocked by the Moroccan government in October 2013 and now only accessible thanks to mirror websites. Anouzla's reporting frequently angered the regime; he was one of the rare journalists who dared to write about the monarchy and often investigated corruption scandals. But it was only in 2013 that his case became internationally known when he was sent to jail after being convicted of "glorifying terrorism."

Anouzla had posted a link to an article in Spanish daily newspaper El País which contained a video from Al Qaeda, the topic of his article. Many, including Anouzla, suspect his arrest was instead linked to his article revealing that the King had pardoned a Spanish paedophile. The revelation had caused an uproar in Morocco and led to major protests in Rabat.

Ali Anouzla's stories of surveillance shed light on a network of hacker militias – the same who attacked Moukrim's website – who claim to be defending the values of the Moroccan kingdom by hacking into websites and personal accounts of opponents to the regime. The groups go by various names: The Monarchist Youth, the Moroccan Force of Repression, Moroccan Ghosts, and the Royal Brigade of Dissuasion. Some have also been known to target Algerian or Israeli websites, countries considered to be enemies of Morocco.

While it is unclear whether those groups receive any form of support from the Government, it is important to bear in mind that their activities are being reported on and celebrated by media outlets, who are themselves suspected of being tied to the intelligence agencies.

Hope for Morocco

We hope this series of portraits will help foster a much-needed debate in Morocco on the surveillance of journalists and political activists. We believe their stories provide even more evidence that the right to privacy is essential to a democratic society, and is key to activists seeking to ensure that their countries become true democracies.

This report provides a rare and unique opportunity to hear from, in their own words, those who have had their lives upended through surveillance. Some are defiant; others are indignant. But all agree that what happened to them is wrong, and that those who continue to spy on them and their families deserve to be brought to justice.

We hope that their stories and our efforts contribute to their fight for a free, inclusive and democratic society.

Methodology

This introduction was written by Privacy International staff in February 2015. The content is based on interviews with Hisham Almiraat, Ali Anouzla, Ahmed Benseddik, Samia Errazzouki, Yassir Kazar and Maria Moukrim. The interviews can be found in the following chapters of this report.

Below are links to articles and research mentioned in the paper as well as recommended reading.

For further reading on Hacking Team:

- https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/
- http://owni.fr/2012/09/14/lespion-etait-dans-le-doc/ (IN FRENCH)

2014 Economist Intelligence Unit Democracy Index:

- http://www.eiu.com/public/topical_report.aspx?campaignid=Democracy0115

For further reading Government banning civil society events in Morocco:

- http://www.amdh.org.ma/fr/communiques/liste-des-interdictions-des-activites-de-l-amdh-depuis-juillet-2014 (IN FRENCH)
- http://telquel.ma/2014/12/18/embargo-lassociation-adala-empechee-fois-dorganiser-reunion-les-autorites_1426709 (IN FRENCH)
- http://www.hespress.com/societe/239347.html (IN ARABIC)

For further reading on the Morrocan Government purchasing of Eagle:

- http://reflets.info/amesys-un-finger-de-pop-corn-pour-le-croco/ (IN FRENCH)
- http://reflets.info/maroc-le-meilleur-ami-de-la-france-se-met-au-dpi-grace-a-amesys-la-filiale-de-bull/ (IN FRENCH)

For further reading on the documents obtained from the Swiss government regarding exports of dual use technologies

- https://www.privacyinternational.org/?q=node/98

For further reading on the protests following the pardon of a Spanish paedophile

- http://www.theguardian.com/world/2013/aug/04/dozens-injured-morocco-protest-spanish-paedophile

For further reading on Moroccan Hacker groups

- http://www.slateafrique.com/97729/qui-se-cache-derriere-moroccan-ghosts-hacker-cyber-activiste (IN FRENCH)

Moroccan Hacker Groups

- https://twitter.com/moroccankingdom (Moroccan Force of Repression Twitter account)
- https://twitter.com/moroccanghosts (Moroccan Ghosts Twitter accounts)
- https://www.facebook.com/pages/-ةيبرغملاقلمح-ءاوللا-تاوق-ل-عدرلا398791140150215?sk=timeline&ref=page_internal (Royal Brigade of Dissuasion Facebook Page)



Photo © Anthony Drugeon

Hisham Almiraat



Photo © Anthony Drugeon

Hisham Almiraat, a medical doctor by training, co-founded the online citizen media outlet Mamfakinch in 2011 to cover and support the February 20th Movement, a series of protests that took place in Morocco around the time of the Arab Spring.

Mamfakinch won the Google Breaking Borders Award in 2012. That same year, all 15 members of the editorial team at Mamfakinch were targeted with spyware designed by the Italian surveillance company Hacking Team, which allows the attacker to gain complete remote access to the targets' computers. Hacking Team sells their software solely to law enforcement agencies and the intelligence communities, thus leaving little doubt that the attacker was a law enforcement or intelligence agency in Morocco.

Today, Hisham Almiraat is the president of the Association des Droits Numériques (Organisation for Digital Rights). ADN is part of Privacy International's global network of advocacy organisations.

Hisham Almiraat comes from a generation of Moroccans who developed their political awareness in the late 1990s. Indeed, as the previous King, Hassan II – the father of the current King, Mohammed VI – was dying he decided to loosen his control over the media to facilitate his son's transition to power. Freedom of opinion and expression – included in the Constitution – ceased to be ignored and many new publications emerged. "All of a sudden in Morocco, we started seeing investigations, papers were tackling all the religious and moral taboos," says Hisham, who was at the time a medical student in Paris.

Maria Moukrim, a renowned journalist and Editor-in-Chief of the publication Febrayer started her career during that same period. "People could write about anything. For instance, I published a scoop on a massive corruption scheme. I did not get any problem at the time"

However, as the new King Mohammed VI established his power, this era of media freedom soon came to an end. Maria adds "today things would be very different".

"Starting from 2001 to 2003 we witnessed a slow decline until we reached a situation where most media are either under the regime's direct control or under its economic grip. Either way the media was no longer free," says Hisham.

Given that it had become increasingly difficult to access objective information, with a media landscape largely dominated by publications tied to the regime, Hisham soon realised the importance the internet would play in transforming the

world. "It is the most revolutionary invention since the printing press because it gives ordinary people the opportunity to express themselves and to join the political debate. I am deeply convinced that if it is used properly it is a game changer, it can – still today – take down regimes."

Thrilled about this new field of opportunities, Hisham soon stepped up from being a news consumer to a full-fledged actor of the Moroccan citizen journalism landscape.

"I started blogging in 2007. I found it great that people could speak in their own name. They did not belong to any group or political party and did not receive any funding."

But the carefree enthusiasm for the internet did not last very long in Morocco. In 2008, Fouad Mourtada was jailed for creating a satirical Facebook page lampooning the King's brother. Mourtada, a promising computer engineer, thus became the first person to be jailed based on content posted on Facebook. He was accused of identity theft for having set up a Facebook page in the name of the King's brother. While he always argued that the humorous tone of the page clearly identified it as a spoof, he was nevertheless sentenced to three years in jail. Fortunately, Mourtada obtained a royal pardon and was released after 43 days in jail.

Something positive did arise from this sinister event. The jailing of Mourtada inspired the creation of a community of people dedicated to defending online freedom of speech. "Free Mourtada was the first campaign I joined," says Hisham. "It was the first of many episodes that gathered a community of people, who would have otherwise never met, if it was not for the internet."

It was at that time that Hisham joined Global Voices, an international community of bloggers, citizen journalists and translators from 167 countries, where contributors report on stories from their own country. Four years later – in 2012 – Hisham would become Global Voices' Advocacy Director.

"Global Voices turned out to be a formidable crossroad for 'internet believers', who adopted the internet as a remarkable tool for political awareness," says Hisham.

And while the role of social media in the "Arab Spring" has now been well-documented, Hisham and his fellow bloggers had not yet realised what was ahead of them.

"Of course, 2011 took all of us by surprise. No one really expected it but in a way we were ready. We already had the networks, the information nodes, we knew each other through Twitter, we had followers, we followed people, we spoke and wrote in English... I remember very well that Global Voices was one of the very first platforms to understand something unusual was happening in

Tunisia."

Hisham followed with excitement the events unfolding in Tunisia and Egypt. And when protests were announced in Morocco, he felt he could play a part. "A group of activists announced several protests on February 20th. We knew people in Tunisia and Egypt who had been participating in the revolution. We learnt their communication methods, their uses of hashtags – all the things that would later on become very popular – and we did the same to try and foster the movement in Morocco.

"A couple of days before the protests, we started seeing the official press agency – Maghreb Arab Press – spreading lies about the movement. They wrote that the protests were going to be cancelled, that it was funded by foreign governments, that it was of a movement of 'homosexuals and atheists.' That was why we decided to create Mamfakinch on February 17th, three days before the protests. We were desperate for an independent platform, with no censorship. We did not mean to be objective because we sided with the movement, we wanted democracy – real, absolute, radical democracy.

"At first when we started there was about thirty people behind the project and we all wanted to engage, contribute, write and volunteer our time. We felt that the balance of power was tipping in favour of democracy."

Mamfakinch - Arabic for "not giving up" – started covering a movement that was otherwise ignored in the Moroccan mainstream media, even though tens of thousands of people were marching in the streets of large Moroccan cities every weekend. A million unique viewers visited Mamfakinch's website over the first four months, a remarkable success considering the limited penetration of the internet in the country. With articles, videos, interviewees, maps, op-eds, Mamfakinch soon became a multi-purpose platform that relayed information on the February 20th Movement but also grew into a space of free expression, where topics ranged from foreign policy to how-to guides on keeping a blog alive.

However, as a year went by and the movement was diminishing, Mamfakinch started struggling to keep their readers' attention. "We felt that we did not interest people anymore because everyone had gone back to their normal lives. They did not want to hear about revolutions any longer because things started looking horrendous in Syria and we saw the first refugees arriving ... The dominant mood in the Arab world is resignation: 'between the Islamists on one side and dictatorships on the other, I'd rather stay home and do nothing.' It impacted people's perception and it was difficult for us to remain popular but we kept on calling for radical reforms."

While Mamfakinch's popularity, and consequently its influence, decreased,

something strange began to happen. They started getting attacked.

In 2012, the website started being targeted with Distributed Denial of Service (DDoS) attacks. DDoS attacks aim to take down a server by overwhelming it with fake requests. To a website, it is as if hundreds of thousands of people are all trying to connect at the very same time; it cannot respond to all the requests and is brought down. The attacks generally took place when Mamfakinch was covering the February 20th protests, which were still occasionally taking place in 2012.

A few months later, Mamfakinch experienced an attack that not only silenced their critical opposition voice, but actually led to the organisation's destruction.

Just like websites, Mamfakinch hosted a contact page for readers to get in touch or story leads to be sent through to the editorial staff. On 13th July 2012 an email from 'i_imane11@yahoo.com' was sent though Mamfakinch's contact page, with the word "Dénonciation" (denunciation, in French) as a subject line.

The message, which contained an attachment entitled "scandale(2)", read:

> Svp ne mentionnez pas mon nom ni rien du tout je ne
> veux pas d embrouilles…
>
> (Please don't mention my name, nor anything else. I don't want to
> get in trouble...)

About 15 members of the editorial staff were forwarded the cryptic email. Of these, seven people opened the attachment and were surprised to find an empty page. It did not take long for the system administrator at Mamfakinch to realise the so-called scoop was actually a piece of malicious software.

Hisham and his team decided to send the malware to Citizen Lab. Citizen Lab is an interdisciplinary technology laboratory based at the University of Toronto that focus on the issues of information and communication technologies, human rights and global security. A core part of their work has been to identify spyware and surveillance technologies used against activists in non-democratic regimes.

The team at Citizen Lab ran a forensic analysis of the virus and eventually identified the signature as being the same as that from spyware created by an Italian company called Hacking Team.

The spyware – that reportedly costs €200,000 – could grant remote access to the computers of those who had been targeted. The attackers could therefore access all their documents, read everything as they typed, including

passwords, or everything they browsed on the internet, and even turn on the computer camera to watch them without the victim noticing.
"It deeply affected me. I felt literally violated because we were building something for other people. We tried to be smart about the way we used the internet to allow people to express themselves and what happened was the violation of a democratic enterprise."

The people whose computers were infected formatted them to erase the malware. All, except one, who decided not to. "I think he did not believe what this virus really meant" says Hisham. "He thought he had nothing to hide anyway. It is a complex cultural problem, some people – especially when they are older – just do not realise how much they actually use the internet. They will tell you 'I am only using my computer every so often, I don't put anything on there.' They don't realise how much metadata reveals about them. So they adopt a nonchalant attitude and tell you that if the government wants to get you, they will get you regardless."

Hisham and his team decided to fight back by improving their own security practices: "For the first time we realised that we needed security policies in place. I worked on an internal security plan with a form for everyone to fill. It was basic security practices to allow us to react efficiently in case we were targeted again. It was painful for me to realise that eventually it did not interest anyone. People thought we were asking too much when we asked for a physical address, when we asked them to share their password with someone else, in case they were arrested. Digital security is hard to sell. As a result though people end up losing trust in technology and just stop engaging. I have seen people finding excuses to stop working with Mamfakinch. I cannot blame them, their careers were at stake. Most people used pseudonyms because they were engineers, lawyers, etc. and had to protect their careers."

Slowly and gradually, Mamfakinch stopped publishing and has been inactive since February 2014. Some at Mamfakinch think it is the logical conclusion for a website that was created to cover a movement that has now disbanded. But according to Hisham, Hacking Team must be held at least partly responsible: "They poisoned this wonderful technology that allowed us to express ourselves anonymously and fearlessly. They killed this. People started thinking 'the rules have changed. I am not going to take any more risks'."

"I am angry and I think Hacking Team deserved to be sued. First because they violated our privacy and also because those companies are destroying the extraordinary tool that the internet is. I am afraid they are turning the internet into something mediocre, only used for commercial purposes. What I see is that the stakes have been raised for ordinary people who want to express themselves. Those who do not want to cause any troubles and who have a lot to lose if their identity is revealed. Those who want to protect their privacy. It is a great loss

for democracy that those people are discouraged from using the internet as a tool for expression. Because on the other hand people who have nothing to lose – like ISIS – will embrace the internet. That is my theory: they have turned the internet into something dangerous for those who wanted to take part in the public debate but had something to lose."

"Repressive regimes have understood that the internet is not something to be left in the hands of citizens. They realised censorship is pretty obvious and so those companies are offering them a magic toy that instil fear among people and lead them to self-censorship. The very thought of being surveilled lead people to decide by themselves to withdraw."

Methodology

This article was written in January 2015. It is based on an interview with Hisham Almiraat via Skype on January 13th 2015. The interview was conducted in French and translated into English.

Below are links to companies, articles and research mentioned in the paper as well as recommended reading.

Mamfakinch

- https://www.mamfakinch.com/

Google Breaking Borders Award

- http://googlepublicpolicy.blogspot.co.uk/2012/07/breaking-borders-for-free-expression.html

Hacking Team

- http://www.hackingteam.it/index.php/about-us

For further reading on the Mourtada affair

- http://en.wikipedia.org/wiki/Fouad_Mourtada_affair
- http://news.bbc.co.uk/1/hi/world/africa/7258950.stm
- http://news.bbc.co.uk/1/hi/7304361.stm

For further reading on the coverage of the February 20th Movement

- http://anneemaghreb.revues.org/1537?lang=en (IN FRENCH)

For further reading on metadata

- https://www.privacyinternational.org/?q=node/53
- http://www.theguardian.com/technology/interactive/2013/jun/12/what-is-metadata-nsa-surveillance#meta=0000000

Samia Errazzouki



Photo © Anthony Drugeon

The daughter of two Moroccans who immigrated to the United States, Samia Errazzouki was no stranger to the political and social struggles ongoing in her parents' homeland. She is now a postgraduate student at Georgetown University in her hometown of Washington DC. Back in 2011 Samia was in the midst of writing a paper on Morocco when the February 20th Movement began. Though her parents warned her that the Government was unforgiving toward political opponents, she started covering the protests for Mamfakinch from the US, and became an integral part of their staff.

And when Mamfakinch's editorial team was targeted with the Hacking Team spyware, she realised that even 4,000 miles across the Atlantic she was not safe from the regime's repressive measures.

"I was doing research for an undergraduate paper on the political economy in Morocco, when the February 20th Movement started," says Samia. "I became really in touch with what was going on and I wanted to get involved because I genuinely believed in the goals they were calling for. I noticed this website called Mamfakinch, which seemed to be the only media that was keeping up with the February 20th Movement in a critical way."

The first paper that Samia published in Mamfakinch was the academic paper she was working on when the movement started. "People could submit articles so I sent them that paper on the private sector in Morocco and they really liked it." A couple of months later, Hisham Almiraat contacted her to ask if she would join the editorial team. "They needed someone to do more writing in English and translating. I started in December 2011."

Samia thus started covering the protests from the US and realised that her geographical distance did not prevent her from becoming a full-fledged member of the team. "It was a loose structure and everyone was equally involved. It was useful to have the time difference because sometimes protests would happen late at night and none of [the other team members] were awake, so I would log in and report on them."

As the movement was largely organising through social media, she discovered there was much to write about by simply observing what was unfolding on Twitter and Facebook. "Especially considering the media situation in Morocco, which is heavily controlled by the Moroccan government, Twitter and Facebook became important tools for getting information on protests when no publication or website or newspaper was writing on them."

While she enjoyed her new responsibilities as a citizen journalist, she always bore in mind that her work came with risks, and the number one risk was being spied on. "Surveillance is not surprising to me, I knew of that risk and my parents always told me about it. I knew that risk when I became an activist and I made a conscious decision when I started."

Surveillance was actually never a foreign concept to Samia. "In the US I live only 20 miles away from the NSA headquarters," she laughs. But she knew the situation would be different in Morocco.

"You realise that when you're dealing with a country that is very authoritarian – and that has a legacy of imprisoning journalists who are providing information the Government doesn't want out – you're opening yourself up to a certain sort of oppression. But I felt that I had the privilege of living in the US, of having US citizenship and that I could do a little bit more than what someone else could in Morocco."

That sense of privilege however quickly faded away. The summer after she joined, Mamfakinch was targeted with Hacking Team spyware reportedly worth €200,000, a major investment that only a government could have made to target a group of citizen journalists. "I expected this level of surveillance, especially with Mamfakinch because there was no hierarchy, and a lot of the members of Mamfakinch were anonymous. I am sure the Moroccan Government was very curious to know who was behind this."

Even though she was nearly 4,000 miles away from the country her parents had left, her links to the February 20th Movement put her in the cross hairs. Hacking Team's spyware is borderless.

"The articles and documents that people could submit to Mamfakinch were forwarded to all of us. We received an email that said 'Hey, we have important information that you may be interested in looking into.' It was in French. I didn't download it because I didn't have time at that particular moment and then it became clear what it was.

"I felt like when I was in DC I was protected from the Moroccan state but then this showed me I wasn't. It doesn't matter where I am, that I have a US passport, I could be in Antarctica, somehow if the Moroccan state wants to keep an eye on me it will.

"It pulled me closer to my colleagues, those who were in Morocco and those who were in Europe. We all felt equally targeted. There is always a concern for those who are based in Morocco. A number of them have received visits from state agents or they know they are being followed."

But after the Hacking Team targeting, Samia discovered that the regime had other unpleasant surprises for her and her family back in Morocco.

"My own family and my neighbours got visited by state agents on several occasions. They'd come and say 'Can we talk to you for a minute? We have questions about Samia and her work.'

"The act of going to ask people questions is not to have answers or information. It is just to intimidate me so I can get the message. It is just about 'We want you to know that we're watching you, not just online but in person.' The fact that they are asking my concierge or my neighbours about my work, who have no idea what I do, this means that they are doing it to intimidate me.

"I still have my family here in Morocco and after the police visited them, there was pressure coming from them. 'What are you doing? Turn it down!'"

As she recalls these events, Samia is sitting at a café in Rabat. She is in Morocco for a couple of days, which she will spend with her family before she returns to the US.

"You think that you can protect your family from what it is that you do. Why should my family be held accountable for my actions? They have nothing to do with what I am doing! But they do it because that's the way they can get to you psychologically. They raise the stakes because you start to get worried not so much for yourself – because you have already made that decision to get involved in this and you know the risks for yourself – but because you never thought that those you love could also get hurt. You start thinking 'What could they do next to my family? What's the next step?'"

Even after Mamfakinch, Samia has kept on writing and committing herself to political activism in Morocco. And the regime is partly responsible for that. "I realised I mattered and that the work we're doing is important because they wouldn't be targeting us if it wasn't. If Hacking Team affected me in any way, it's been positive. It pushed me to keep on doing what I was doing."

Samia is however well aware of the impact that her political choices had on her life, and more specifically on her academic career. Indeed, her post-graduate research focuses on a controversial chapter of Moroccan recent history and being under surveillance makes her confront important dilemmas. "I have a responsibility to protect the identity and the safety of the people I interview for my research. Anyone I speak to here, I put them at risk of being targeted because I could take all possible steps to protect my communications but physically they can still follow me. And if they follow me they see I am going to a source's house, they see I am meeting with them and that means I am subjecting that person to a risk I can't protect them from."

Samia has been discussing her story with academics, who have faced similar dilemmas, and who have all advised her to put on hold her activist work. She knows that if she eventually does so, it will be for the sake of her academic pursuits, not because she would be giving in to political pressure.

"Is this the point where I need to start questioning what I do? I am still not convinced though, I think I can still succeed as an academic while remaining an activist. I am not ready to give it up yet."

Methodology

This article was written in January 2015. It is based on an interview with Samia Errazzouki conducted in Rabat on December 12th 2014. The interview was conducted in English.

Samia's article on the private sector in Morocco

- https://www.mamfakinch.com/morocco's-political-private-sector/



Photo © Anthony Drugeon

Yassir Kazar



Photo © Anthony Drugeon

Yassir Kazar was a staff manager at an IT consulting firm and a lecturer in business intelligence at Université Paris Descartes when the February 20th movement started. He joined Mamfakinch without knowing how much the experience would transform his life. Outraged by the Hacking Team spyware attack, he would eventually leave his job to start a business in computer security.

Yassir Kazar was living in Paris and working as a lecturer on business intelligence when the Arab Spring started. "It is funny because a few months before everything kicked off in Tunisia I had written one of my first articles on a journalist who had been arrested in Tunisia, Taoufik Ben Brik," says Yassir. "I had started reading authors like Chomsky and I was realising that quite a few people were very willing to criticise their own country. I decided it was too easy to criticise other countries and that it was time for me to look at what was going on in Morocco. I think I was meant to join a collective like Mamfakinch that wanted to address those issues."

When calls to protest on February 20th 2011 started emerging, Yassir decided he did not want to experience this through TV and took a last minute plane to Casablanca. He wrote about his experience of the protests on Facebook and first heard his friends' defiance. "They would tell me 'Why are you doing that? Think about the motherland! You're a traitor!' I thought that was part of a sickening spiral, after all we were not asking for anything crazy!"

Shortly after the first protests, Yassir met with the Mamfakinch team and joined the editorial team in its early days. A year later, came the event that would deeply affect the rest of his life.

"We had a contact form where we often received submissions from people, suggestions for articles and support messages. One day we received something labeled 'scandal,' and the author of the email wrote something along the lines of 'Don't mention my name. I don't want to be tied to this.' Of course it all turned out to be bogus. There was a doc file attached. I saw the email but I did not open it because I was used to opening everything on Google Drive, I was already quite paranoid at the time. A few people started opening it and were saying 'That's weird the document is empty.' Then all the red alerts started blinking in our heads and we asked people to not open it by any means.

"We sent the virus to a team of experts for them to run a diagnostic. They told us it was a Hacking Team spyware with a key logger and the ability to turn on the camera of our computers. We understood we had been targeted. It was not your average virus you can randomly get."

The attack took the Mamfakinch team by surprise. At that time, no one knew anything about Hacking Team. The people who had been affected were looking for answers and the editorial team as a whole started thinking about a security strategy.

"There is a gap between hearing about this story or reading about it and really experiencing it. It is a bit like an assault, you can listen to a story, feel sympathetic for the victim but when you really experience an assault it is deeply traumatising. But we all react differently to trauma. Some people manage to transcend it and to turn into a positive experience and others remain traumatised, especially if technology was not their cup of tea in the first place. I think for some people it was a real slap in the face."

And while it was a surprise, it was not the first time Yassir was surveilled by the Government. A few months before receiving the infected email, his neighbour had been visited by the Police to be asked about his habits, if he drank alcohol, if he was going to the mosque.

"That was already hard to deal with because you suddenly realise it is not just about you. If they start with your neighbour, the ones most impacted by what you do could be your friends, your acquaintances..."

Yassir was surprised and shocked that the government was ready to invest €200,000 on spyware to target Mamfakinch. Yet, just like others in the editorial team, he was quick to appreciate the positive side: at least their work was so important and disturbing that the Government was ready to invest a substantial amount to try and target them.

"It really changed my life. I realised how topical computer security was. If I started my own business it is because I told myself 'There is a real problem and a real issue at stake. We are no longer at all talking about a criminal issue that you can just solve with an anti-virus. We are talking about a real challenge for society, where individuals can be targeted, where you can be targeted, where you can be sent something that will scan and forward all your data.' I think either you embrace that and you decide you face up to it and learn how to work things out or it can be deeply traumatising and completely modify your experience of the internet."

But having been part of a group targeted by such a spyware also raised important questions around the ethics of journalism.

"You realise that if they want to go after you they will find any excuse to arrest you and that is why you must be extremely responsible with what you write. So that when they arrest you, you know what you have written is intellectually

honest, you have not written anything to insult or defame anyone."

Today, with his own business, DefensiveLab, Yassir gets to train people in digital security to help them be safer online and learn how to protect others. He has also remained an activist on open data and open government issues, who feels dedicated to the right to information. The challenge between facilitating information flow and protecting the privacy of sources was precisely one he discovered with Mamfakinch.

"The issue of source protection obviously came up with Hacking Team. There were anonymous members at Mamfakinch and we spoke to external sources. As far as I am concerned I am open about what I do and I take the responsibility for it. But if my foolishness leads to my sources and someone else ends up spending the rest of his life in jail, how am I supposed to live with that? Will I go in the street to talk about justice and say it is not fair? It would be a tragedy!"

Methodology

This article was written in January 2015. It is based on an interview with Yassir Kazar conducted in Rabat on December 13th 2014. The interview was conducted in French and translated into English.

Ali Anouzla



Photo © Anthony Drugeon

If you say the name Ali Anouzla in Morocco, chances are you will get a reaction. Well known to the public and reviled by the powerful, Ali is a renowned journalist and Editor-in-Chief of the online publication Lakome. He was awarded the Leaders for Democracy prize from the Project on Middle East Democracy in 2013 – despite pressure from Moroccan diplomats to strip him of the prize – and selected by Reporters Without Borders to be part of their campaign "Information Heroes" in 2014. Lakome is now inactive, after it was banned by the Government in October 2013. However, it remains accessible via mirror websites.

In September 2013, Ali was writing a piece on Al Qaeda to which he added a link to an El País article that featured a video from the terrorist organisation, in which they threatened Morocco. Because of this article, Ali was charged for "glorifying terrorism" and immediately sent to jail. While he was released after five weeks, he remains on probation and the charges have still not been dropped. According to Ali, King Mohammed VI was simply angered that Lakome revealed a political scandal a month before, involving the release of a Spanish paedophile, which led to violent protests across the country. The protests reflected the anger of various groups from child-protection organisations, to religious organisations, and to pro-democracy groups, outraged by the dysfunctionality of the Moroccan judicial system.

Ali Anouzla shares with Privacy International his many tales of surveillance from phone tapping to hacked Facebook accounts.

While much attention today has been paid to the surveillance of digital communications, Ali Anouzla likes to remind people that he's been a victim of spying of all types. "There have been cars following me outside of Rabat, someone once came to film the keyhole of my flat – it turned out that he worked for the secret services. And obviously phones are tapped."

Ali has multiple stories of phone tapping. One of them involved a Belgian senator who phoned him to say she wanted to meet during a trip to Morocco. The two agreed on a time and location and told nobody about the planned meeting. Shortly afterwards, the senator received a phone call from the Moroccan Ministry of Foreign Affairs asking her to cancel the meeting. While they did not provide any explanation as to how they had found out about the meeting, phone tapping conducted by the secret services is the most likely answer.

"To be honest surveillance only has a limited impact on my professional and

private life," says Ali. "But it is true that knowing your phone conversations are constantly listened to is disturbing. It restrains my private life: for instance even though I don't drink, I know I cannot go to a place where people drink alcohol because I could be photographed and in a Muslim country, this could be used to shock people. Other than that it never prevented me from saying and writing anything."

Beyond the phone tapping and other violations of his private life, Ali discovered the intricacies of obscure partnerships between certain online media and the secret services.

"Sometimes I read in certain online media information on my private life that could have only been obtained from intercepting my phone communications. They write about my travels, who I have been seeing ... For instance, one day someone called me to invite me to attend a conference abroad. I did not tell anyone about it. Yet the day after it was in one of those publications."

It is said that there are three forbidden topics in Morocco: the King, religion and Western Sahara. The region has been disputed since 1963 between Morocco, which claims its ownership, and the Polisario Front, the Sahrawi national liberation movement. In Morocco, questioning the issue of Western Sahara – like Ali Anouzla has – can have serious consequences.

In April 2013, several of the online media organisations that reported stories based on phone tapping, published a story in the middle of the night announcing that Ali Anouzla had killed himself following a UN resolution favourable towards Morocco on Western Sahara.

"It deeply affected my family, I spent the whole night picking up phone calls to reassure people. I did not bother suing those websites because I had tried doing it in the past and it never was conclusive."

"The following day, some journalists called me and asked me what was going on, I told them I refused to engage with publications that were manipulated by the secret services. Some of them quoted those words, headlining 'Ali Anouzla: Those websites are manipulated by secret services.' The Ministry of Interior then published a press release to declare that no media were manipulated by the secret services and a week after the ministry filed a law suit for defamation."

The court first rejected the Ministry's complaint. The Ministry appealed and Ali Anouzla was given a suspended sentence of one month in jail. However, Ali was never made aware that the hearing was taking place and is therefore appealing the decision.

"When I sue the media that violate my privacy, they are acquitted. When I say they are tied to the secret services I get condemned. That is quite the paradox!"

it is not just Moroccan law enforcement and security services that are conducting surveillance or violating people's privacy. Several hacker collectives have gone after activists or journalists critical of the current regime. The groups go by names such as Les Jeunesses Monarchistes (the Monarchist Youth), Force de Répression Marocaine (Moroccan Repression Force) and Groupe Nationaliste Marocain (Moroccan Nationalist Group). Their "victories" are then advertised in the same online media that Ali suspects to be tied to the secret services.

Moroccan hacker groups are well known on the internet for targeting anything that they perceive as "unpatriotic" or betraying the kingdom's traditional values. Their targets are therefore sometimes erratic, and have included not only Algerian and Israeli websites but the French national lottery, la Française des Jeux. The latter had been attacked by a group known as Moroccan Ghosts, which had put up a message to remind "believers" that gambling was ungodly.

Another well-known figure of independent journalism in Morocco – who did not wish to be named – has for instance had her computer infected with malware after clicking on a link sent to her by the Force de Répression Marocaine.[4] She subsequently discovered that they could for instance switch on the camera in her laptop and take photos of her.

They also targeted Ali's online accounts.

"My Facebook and Gmail accounts were both hacked. It was partly my fault for having used the same password. I never managed to regain the control of any account. After the accounts got hacked one of those online media announced that the Brigade Royale de Dissuasion (the Royal Brigade of Dissuasion) – a group inspired by the Jeunesses Monarchistes – had successfully hacked into my Facebook account and had attacked websites of the Polisario and Algerian websites. For them, it is a heroic act of nationalism. They consider that someone who has different opinion than that of the regime on Western Sahara is necessarily pro-Polisario."

Online media Chaabpress had in fact published the press release from the Royal Brigade of Dissuasion, where Ali is referred to as "the official mouthpiece of the suspicious movement" (the February 20th Movement). The rest of the Lakome staff were also threatened:

"This is a warning to all the staff of the Lakome website: know that breaking into your website is easy [for us] but because of our belief in freedom of expression, which you do not respect, we preferred not to prejudice you since you are

Moroccans. But rest assured that in the event that you cross our red lines you will taste our wrath."

Ahmed Benseddik, a notable political activist we interviewed in Rabat, feels that the Police are reluctant to go after those groups. He filed a complaint after a video had been posted on YouTube by the Monarchist Youth calling for his death, along with nine other journalists and activists, but the Police have not followed up on the case since June 2014.

Benseddik too saw his private accounts hacked into and the content of some of his emails published. He mentions an ironic email he had sent to a female journalist that the hacker had used to claim Benseddik had had an affair with her. "Their goal is to harm people's reputation and to destroy households with immoral dirty tricks," says Benseddik.

Exposing the real motives of those hacker groups – and who is behind them – will now be the work of local investigative journalists and activists.

"As a journalist I cannot claim that those hacker groups are tied to the secret services because I don't have any proof," says Ali. "I was working on an investigation on the matter before I was sent to jail. I hope to one day resume working on that."

Methodology

This article was written in February 2015. It is based on two interviews with Ali Anouzla conducted in Rabat on August 29th 2014 and December 13th 2014. It also contains elements from an interview with Ahmed Benseddik on August 28th 2014 in Rabat and an interview with Maria Moukrim on August 29th 2014 in Rabat. The interviews were conducted in French and translated into English.

Below are links to articles and research mentioned in the paper as well as recommended reading.

For further reading on the protests following the pardon of a Spanish paedophile

- http://www.theguardian.com/world/2013/aug/04/dozens-injured-morocco-protest-spanish-paedophile
- http://uk.reuters.com/article/2013/08/03/uk-morrocco-spain-protest-idUKBRE97202520130803

Article from Chaabpress containing the press release of the Royal Brigade of Dissuasion

- http://chaabpress.com/news4466.html

Privacy International would like to thank Antony Drugeon for the pictures featured in this report



Photo © Anthony Drugeon

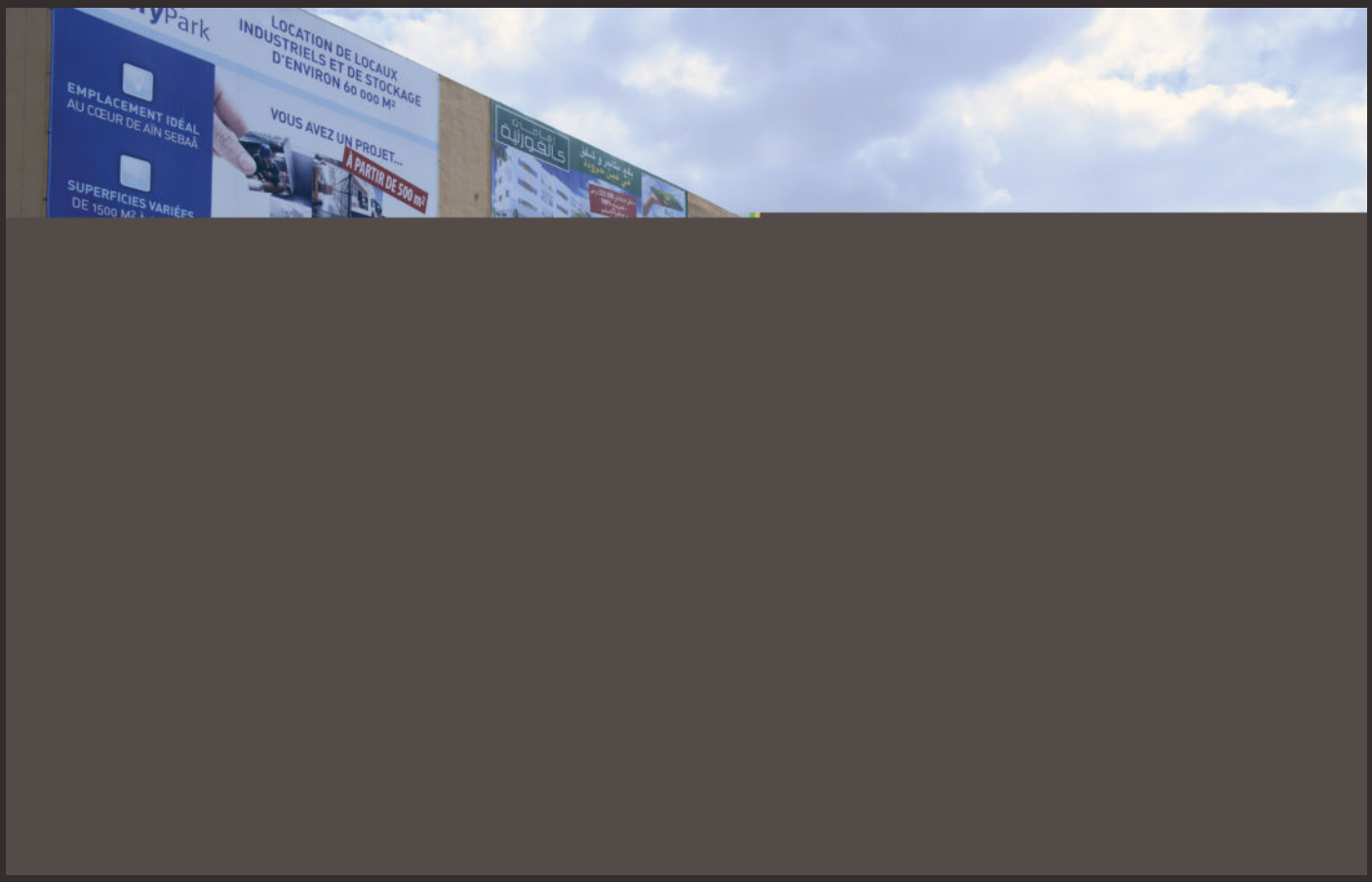


Photo © Anthony Drugeon



Privacy International
62 Britton Street, London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422 4321
www.privacyinternational.org
Twitter @privacyint

UK Registered Charity No. 1147471