PRIVACY INTERNATIONAL

Securing Safe Spaces Online

Encryption, online anonymity, and human rights

PRIVACY INTERNATIONAL

ARTICLE 19

IHRC | INTERNATIONAL HUMAN RIGHTS CLINIC
HUMAN RIGHTS PROGRAM AT HARVARD LAW SCHOOL

This booklet is the result of a collaboration between Privacy International, ARTICLE 19, and the International Human Rights Clinic (IHRC) at Harvard Law School. IHRC conducted desk research as well as interviews with individuals working in civil society organisations in the four countries examined.

This booklet was written by Anna Crowe, Clinical Advocacy Fellow (IHRC), and clinical students Sarah Lee and Mark Verstraete. Carly Nyst, Legal Director of Privacy International, reviewed the booklet and provided editorial direction. Matthew Rice and Chris Weatherhead from Privacy International provided assistance. Bonnie Docherty, Senior Clinical Instructor, and Tyler Giannini, Co-Director of IHRC, reviewed the booklet for IHRC. Tutaev Design designed and printed the booklet. IHRC would like to thank Hisham Almiraat, Nighat Dad, Furhan Hussain, KS Park, and Byoung-Il Oh for their help in the booklet's drafting.

Contents

Executive Summary

As more of our lives are lived in the digital realm, communication security tools, such as encryption and anonymity tools and services, are increasingly important to the protection of human rights – particularly the right to privacy and the right to freedom of expression. Communication security tools give individuals access to safe and private spaces for personal development where they can communicate without unwarranted interference.

The June 2015 report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, is a significant first step in articulating the relationship between encryption, online anonymity, and human rights.[1] This booklet complements the Special Rapporteur's June 2015 report.

It highlights a variety of legal restrictions on and informal obstacles to personal use of encryption for communication and the exercise of anonymous speech online in four countries with diverse geographic, political, and socioeconomic backgrounds – Morocco, Pakistan, South Korea, and the United Kingdom. The booklet is not intended to give a comprehensive account of relevant law, policies, and practices.

Legal restrictions and informal obstacles impede the use of encryption and limit anonymous speech online across the four countries examined in a variety of ways. Legal restrictions on encryption include general bans on the personal use of encryption, as well as more targeted measures, such as the ability of state authorities to require individuals to decrypt information. The widespread perception that encrypting communications is technically difficult or an unnecessary burden is among the informal obstacles to personal use of encryption.

Meanwhile, online anonymity is hindered by "real name registration" laws, which require people to use their real names to register for certain websites, and bans on anonymity tools. Informal obstacles include websites requiring identity verification as a matter of corporate policy; additionally, lack of trust in the internet as a safe space to communicate and fear of surveillance can diminish confidence that online anonymity is possible.

There are opportunities for governments, the corporate sector, and civil society to eliminate or minimise obstacles to personal use of encryption and online anonymity. Governments should implement or reform laws and practices to promote rather than restrict encryption and guarantee anonymous speech online. While the right to privacy and the right to freedom of expression are not absolute, restrictions must conform with the requirements of international human rights law.[2] The corporate sector is also in a position to respect rights by promoting practices and developing products that preserve users' rights online. Finally, civil society groups should start using and actively promoting encryption and anonymity tools, as well as drawing attention to their relationship with human rights.

> ***Encryption and anonymity, separately or together, create a zone of privacy to protect opinion and belief.***
> **UN Special Rapporteur on Freedom of Opinion and Expression, June 2015**

Foreword

Why We Encrypt

Encryption protects our data. It protects our data when it's sitting on our computers and in data centres, and it protects it when it's being transmitted around the Internet. It protects our conversations, whether video, voice, or text. It protects our privacy. It protects our anonymity. And sometimes, it protects our lives.

This protection is important for everyone. It's easy to see how encryption protects journalists, human rights defenders, and political activists in authoritarian countries. But encryption protects the rest of us as well. It protects our data from criminals. It protects it from competitors, neighbours, and family members. It protects it from malicious attackers, and it protects it from accidents.

Encryption works best if it's ubiquitous and automatic. The two forms of encryption you use most often – https URLs on your browser, and the handset-to-tower link for your cell phone calls – work so well because you don't even know they're there. Encryption should be enabled for everything by default, not a feature you turn on only if you're doing something you consider worth protecting.

This is important. If we only use encryption when we're working with important data, then encryption signals that data's importance. If only dissidents use encryption in a country, that country's authorities have an easy way of identifying them. But if everyone uses it all of the time, encryption ceases to be a signal. No one can distinguish simple chatting from deeply private conversation. The government can't tell the dissidents from the rest of the population. Every time you use encryption, you're protecting someone who needs to use it to stay alive.

It's important to remember that encryption doesn't magically convey security. There are many ways to get encryption wrong, and we regularly see them in the headlines. Encryption doesn't protect your computer or phone from being hacked, and it can't protect metadata, such as e-mail addresses that needs to be unencrypted so your mail can be delivered.

But encryption is the most important privacy-preserving technology we have, and one that is uniquely suited to protect against bulk surveillance – the kind done by governments looking to control their populations and criminals looking for vulnerable victims. By forcing both to target their attacks against individuals, we protect society.

Today, we are seeing government pushback against encryption. Many countries, from States like China and Russia to more democratic governments like the United States and the United Kingdom, are either talking about or implementing policies that limit strong encryption. This is dangerous, because it's technically impossible, and the attempt will cause incredible damage to the security of the Internet.

There are two morals to all of this. One, we should push companies to offer encryption to everyone, by default. And two, we should resist demands from governments to weaken encryption. Any weakening, even in the name of legitimate law enforcement, puts us all at risk. Even though criminals benefit from strong encryption, we're all much more secure when we all have strong encryption.

Bruce Schneier
Berkman Center for Internet & Society
Harvard University

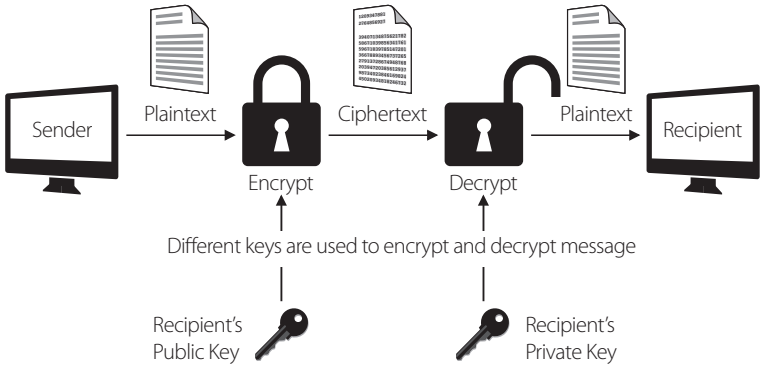
Cambridge, Massachusetts, United States of America
June 2015

> ***Encryption is the most important privacy-preserving technology we have.***
> **Bruce Schneier**

What is Personal Use of Encryption?

In this booklet, "personal use of encryption" refers to individuals using encryption to communicate privately with other individuals. Encryption is a key instrument to ensure that digital communications – ranging from online financial transactions to personal phone conversations and emails – are protected from unwarranted interference, helping to preserve the right to privacy, as well as other rights, such as freedom of expression and freedom of association. Without encryption, forming a secure channel for exchanging private information digitally is nearly impossible.

Encryption is a way of securing communications that uses mathematical algorithms to protect data while it is in transfer or storage.[3] Encryption relies on the process of merging a message ("plaintext" – the content of the message) with a passphrase or other arbitrary data such as a file (commonly referred to as an "encryption key") in order to produce a "ciphertext" that is indecipherable to users who do not have the encryption key. In order to make the message coherent, an individual must use a correct key to decrypt the ciphertext and convert it back to readable plaintext. In other words, the sender of the message uses their encryption key to turn a readable message into scrambled, unreadable text. In return, the message's recipient uses an encryption key to make the message readable. If the message is intercepted in transit, then it will be unreadable.



One of the strongest forms of encryption is "end-to-end encryption", which is provided by specifications such as "PGP".[4] With end-to-end encryption, a user encrypts the contents of a message on her own device and the email program sends an encrypted version of that message to a final recipient who then decrypts the message on her own device. Full end-to-end encryption provides only the intended recipients with access to the content of the message, making it secure.

Less secure forms of encryption also exist. For example, if an individual uses Gmail to send an email, Google uses HTTPS (Hypertext Transfer Protocol over an encrypted connection) to send that email between Google's servers and email users' inboxes. The use of HTTPS prevents unauthorised access to the email while it is in transit, but Google can still view a plaintext version of the email (the text of the email the sender wrote) while it is stored on its servers.

> ***Full end-to-end encryption provides only the intended recipients with access to the content of the message, making it secure.***

> ***It's all about making that choice, to encrypt or not encrypt. I want to be able to draw and define the limits for my public and private spaces.***
> **Furhan Hussain, Bytes For All, Pakistan**

> ***Without trust in the idea that anonymous contributions will remain anonymous, those who would otherwise participate in debates keep silent.***
> **Hisham Almiraat, Association des droits numériques, Morocco**

What is Online Anonymity?

In this booklet, "online anonymity" means the ability of individuals to conceal their identity when sharing and accessing information and opinions online. Anonymity is a deeply held value for many internet users and has contributed to a robust internet public sphere. The inventor of the World Wide Web, Tim Berners Lee, has proposed an online "Magna Carta" that would explore the principles of privacy, free speech, and responsible anonymity.[5] Expressing views anonymously online does not necessarily require the use of encryption; however, as tools that help internet users to remain anonymous often utilise encryption, anonymity and encryption are closely linked.

Anonymity has long been a means by which individuals could freely enjoy their right to impart and receive information. The use of pseudonyms, nom de plumes and pen names to conceal an author's identity has been common throughout history. Anonymity has been essential to the publication of works that critique governments or powerful actors, or expose wrongdoings. Equally, anonymity plays an important role in securing human rights online. In a 2013 report, Frank La Rue, then Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, noted that "[a]nonymity of communications is one of the most important advances enabled by the internet, and allows individuals to express themselves freely without fear of retribution or condemnation".[6] He also observed that "willingness to engage in debate on controversial subjects in the public sphere has always been linked to possibilities for doing so anonymously".[7]

United Kingdom

- Population (2013): **64 million**
- Number of internet users (2013): **90% of population**
- Human Development Index ranking (2014): **14**
- The government has proposed restricting strong encryption. No general legal restrictions on online anonymity.[8]

Morocco

- Population (2013): **33 million**
- Number of internet users (2013): **56% of population**
- Human Development Index ranking (2014): **129**
- Use of strong encryption is not widespread and law contains general restrictions. Many Moroccans do not view the internet as a safe space where they can speak freely and anonymously.

South Korea

- Population (2013): **50 million**
- Number of internet users (2013): **92% of population**
- Human Development Index ranking (2014): **15**
- No general legal restrictions on the personal use of encryption. Laws and corporate sector practices constrain online anonymity.

Pakistan

- Population (2013): **182 million**
- Number of internet users (2013): **11% of population**
- Human Development Index ranking (2014): **146**
- Use of strong encryption is not widespread and law contains general restrictions on the use of encryption and anonymity tools. Fear of surveillance is pervasive among those working in controversial areas.

This report has been updated due to a mistake concerning the border of Pakistan.

Legal Restrictions on Personal Use of Encryption

Legal restrictions on the personal use of encryption may be general – such as general bans on the use of encryption without government permission – or targeted, such as requirements for individuals to decrypt specific pieces of information. In Pakistan, a general ban exists, subject to an exception that allows individuals to seek permission from the government to use encryption. Moroccan law, meanwhile, is ambiguous on whether personal use of encryption requires prior government authorisation.

Legal methods that target specific individuals or pieces of information are more common than general restrictions. For example, "mandatory decryption laws" are laws that provide that in certain circumstances (usually subject to a judicial order) governments can order individuals to decrypt information they control and turn this readable information over to state authorities. Such targeted methods can serve legitimate purposes, but they should only be used in strict compliance with the requirements of international human rights law.

A more concerning type of targeted measure is "key disclosure". Key disclosure is when the government compels an individual to provide her encryption key to the government. This means that the government is able to access all information that can be made readable through the encryption key, which could include all her emails and not just those relating to the government's purpose. UK law provides for both mandatory decryption and key disclosure.

Other legal measures indirectly restrict personal use of encryption by diminishing the security of encrypted communications. Governments may require that technology companies build "backdoors" into their systems to allow government access to plaintext data. A backdoor is a pathway in a piece of technology that government agents can use to access messages that are sent using that technology.[9] For example, an email program that purports to send encrypted emails may have a technical vulnerability built into it that allows those who are aware of the vulnerability to access emails sent using the program. When technology has a backdoor built into it, not only government agents, but also cybercriminals and other third parties may be able to access data.[10] Another type of backdoor is the establishment of a "key escrow" regime, in which technology companies, third parties (such as corporations), or government authorities hold copies of encryption keys, which they may be required to hand over to law enforcement or intelligence agencies.[11]

United Kingdom

"No safe spaces for terrorists"

Recent developments suggest that the UK Parliament may soon enact new laws that imperil the security of encrypted communications or impose general restrictions on personal use. In January 2015, UK Prime Minister David Cameron stated that in the 2015-2020 term of Parliament he intends to introduce "a comprehensive piece of legislation that makes sure we do not allow terrorists safe spaces to communicate with each other".[12] In a direct challenge to the use of end-to-end encryption he questioned whether the UK government should "allow means of communications which it simply isn't possible to read."[13] Civil society organisations fear the Prime Minister's plans will include a requirement that technology companies install backdoors in their products.

Civil society organisations and others are concerned about Cameron's proposal.[14] Jim Killock, Executive Director of the Open Rights Group, observes that Cameron's "broad and unclear" remarks have "set in motion an unhelpful debate about whether law enforcement and security services should always be able to read every communication".[15] He notes, "the reality is that they can't always be able to read or find a record of every communication – and it shouldn't be compulsory for us to record every time we talk to someone, online or offline". Independent overseer of information rights in the UK, Information Commissioner Christopher Graham, has also warned against "necessarily concluding that we must give [the security services] access to more and more of our private information".[16]

Targeted measures to work around encryption already exist in UK law. The Regulation of Investigatory Powers Act 2000 ("RIPA") allows authorities to obtain notices that require individuals to disclose encryption keys or decrypt specific information, usually in the context of a criminal investigation.[17] The grounds for issuing notices are broad and vague: disclosure must be necessary in the interest of national security, crime prevention or detection, the UK's economic well-being, or "for the purpose of securing the effective exercise or proper performance by any public authority of any statutory power or statutory duty".[18]

A person who knowingly fails to comply with a RIPA notice may be punished with up to two years' imprisonment.[19] In 2009, a 33-year-old man became the first person to serve time in prison for failing to comply with a notice; news reports describe the man as "a science hobbyist with no previous criminal record", who suffered from serious mental health problems.[20]

Pakistan
Ban on use of encryption

The government of Pakistan has moved towards outlawing the personal use of encryption. Directives issued to internet service providers by the Pakistan Telecommunications Authority (PTA) – a state agency – in 2010 and 2011 have the effect of banning individuals from using encryption except in limited circumstances and with the government's permission.[21]

The directives are confusing and their legal authority is uncertain.[22] Regardless, the PTA actively publicises its message that "non-standard means of communication" that are "hidden" or "[mechanisms] which conceal communication to the extent that prohibits monitoring" are presumptively illegal.[23] The 2010 directive annexes a form that individuals or companies can use to seek authorisation from the PTA to send encrypted communications when "essentially required".[24] If the PTA's instructions are taken at face value, individuals and companies are expected to fill in this form – which asks for information including the purpose of the communication and the number of bytes it comprises – each and every time they wish to send an encrypted communication, such as an email or WhatsApp message.

The PTA refers to any traffic (information flowing across networks) that cannot be read in plaintext as "grey traffic" and the monitoring of this traffic, which includes encrypted traffic, is carried out by the Directorate for Inter-Services Intelligence (ISI), Pakistan's largest intelligence agency.[25] The ISI operates under the remit of the military. Although the ISI has an extensive surveillance apparatus and employs thousands of people, it is essentially an extra-legal body, lacking formal powers under legislation. All internet traffic in Pakistan flows through one central point to enable the ISI to monitor it comprehensively.[26]

Human rights activists fear that various intelligence agencies are watching people who use encryption to protect their communications. Although no one is known to have been arrested for using encryption, Nighat Dad, Director of the Digital Rights Foundation (Pakistan), describes the ban on encryption as "a sleeping provision against individuals: if they want to target an individual or … they have suspicions about that person, they can invoke that provision against him or her".[27] Furhan Hussain from Bytes for All (Pakistan) describes a "general sense of unease in your life" that comes from "knowing anything you do can be used against you, or interpreted in a malicious way."[28]

Morocco
Ambiguous legal framework

In Morocco, people do not know whether they are breaking the law when they use encryption without a military body's permission. The law states that buying or using encryption technology requires obtaining authorisation from a military body. However, it is unclear whether this requirement applies to personal use of encryption.

Law 53-05 (2007) restricts the "import, export, provision, exploitation, or use of cryptography", for the purposes of preventing its use for illegal means and preserving national defence interests.[29] According to this law, whose original purpose was to regulate commercial transactions, parties must notify the relevant authority when encrypted digital signatures or certifications are used to authenticate transactions or guarantee data integrity.[30] Parties must obtain authorisation when they seek to use encryption for other purposes by registering with the relevant authority.[31]

In practice, there has been no indication that this law applies to personal use of encryption.[32] However, the law is ambiguous on its face.[33] Notably, personal use does not appear in a list of exceptions to the requirement to obtain authorisation contained in a subsequent decree.[34] This absence of clarity means that people do not know whether they might face prosecution for using encryption. The penalty for failing to notify or register is imprisonment of up to one year and a fine of up to 100,000 DH (around 10,000 USD).[35]

Compounding the atmosphere of uncertainty, the notification and registration regime is administered by a military body that eschews transparency. In January 2015, the government transferred the administration of the regime from a civilian agency to a military body, the General Directorate for the Security of Information Systems.[36] This transfer took place without public debate or consultation and has led civil society actors to question the government's motivations. Hisham Almiraat, President of the Digital Rights Association (Morocco), asks, "why would the military and intelligence services have the authority to regulate something that originally had to do with commercial transactions?"[37] His organisation views the change as "indicative of a police state mentality".

Legal Restrictions on Online Anonymity

Legal measures that restrict people from remaining anonymous when they speak on the internet are on the rise. General measures include laws that mandate real name registration and bans on tools that help internet users remain anonymous online. Other general measures include data retention laws and policies requiring the mandatory registration of SIM cards.

Real name registration laws require that all individuals provide identifying personal information – and sometimes a government-issued identity number – to access certain websites and services online. In South Korea, for example, real name registration laws enable the government to identify online users who engage in activities or make statements that the government considers illegal or unacceptable.

Other general measures include restrictions on access to tools – such as Virtual Private Networks (VPNs) – that make users unidentifiable to anyone monitoring internet traffic. A VPN is a program that allows an individual to use the internet to access a private network and has the effect of making that individual's internet activity anonymous. Pakistan's encryption ban explicitly applies to encrypted VPNs, and implicitly to "ToR", a free piece of software and open network that offers the strongest guarantee of online anonymity.

> ***According to the South Korea Constitutional Court, real name registration requirements violate freedom of expression and privacy, and freedom of the press.***

South Korea

Real name registration laws

Over the last decade a number of "real name registration" laws have established an online environment that makes commenting anonymously on Korean websites very difficult. The government argues that banning anonymity helps to prevent vicious online attacks and cyber bullying, social concerns that have resonance in Korean society.[38] Additionally, the political climate is dominated by national security concerns that favour moderating online speech: the National Security Act 1948 effectively outlaws any expression that "praises, incites or propagates the activities of an anti-government organisation", namely North Korea.[39]

In 2004, the first in a series of real name registration laws came into force, requiring internet users to verify their identity before they could post comments concerning electoral candidates.[40] In 2007, the real name registration regime was dramatically extended by a law that required all internet users to verify their identity – in practice, through their government-issued identity number (the "resident registration number" or RRN)[41] – to be able to sign up to and comment on any website with more than an average of 100,000 visits per day – in other words, all major Korean news, entertainment, and social media websites.[42]

In a 2012 decision, the South Korea Constitutional Court found that the real name registration requirement in the 2007 law violated constitutional provisions on freedom of expression and privacy, as well as freedom of the press.[43] In addition to rights violations, the Court was concerned about the data security risks posed by multiple websites accumulating massive amounts of sensitive personal information, such as RRNs. As a result of data breaches at various websites that compromised the RRNs of millions of South Koreans, in 2012 the law was amended to prohibit internet companies from collecting RRNs.[44]

Nonetheless, the practice of real name registration continues. Laws still require the identification of online users in particular circumstances, such as when they comment on election candidates during campaign periods, use online games, or access adult websites.[45] Because websites cannot predict in advance whether their users' behaviour will trigger the real name requirement, in practice major websites prefer implementing real name registration for all users all the time. Many smaller websites, even those that lack adult content, games, or any political aspect, have opted to disable comment functions during election campaign periods to avoid the real name requirement. This reduces the number and range of online forums that allow individuals to engage in political discussions.[46]

Pakistan
"VPN" ban

Pakistan's ban on encryption applies to "mechanisms including encrypted VPNs" that help people to remain anonymous online.[47] Additionally, civil society groups are concerned that broadly worded provisions in a proposed new law, the draft Prevention of Electronic Crimes Act, may be used to criminalise the use of encryption tools that enable online anonymity, such as ToR.[48] Anonymisation tools, such as VPNs and ToR, serve an important role in Pakistan, where expressing controversial opinions, especially in relation to religion, can trigger violence and persecution.[49]

Large numbers of people in Pakistan use VPNs because they are a means to access websites that have been blocked by the government, such as YouTube. Ordinary web users cannot access blocked websites: when they attempt to visit a blocked website they receive an "access denied" message. Because VPNs often use encryption to keep information secure, encrypted VPNs are very common. Communicating through an encrypted VPN makes the VPN user unidentifiable and means their internet traffic cannot be easily monitored. VPNs are therefore a type of anonymisation tool.

Anyone seeking to use a VPN must go through an application process run by the Pakistan Telecommunication Authority (PTA). The application form and information provided by the PTA suggest that the authorisation process is directed primarily at companies, rather than individuals. There does not appear to be a process designed for individuals to seek authorisation to use a VPN. The criteria on which applications are approved or declined are not public.

Furthermore, there are indications that the PTA is cracking down on unauthorised VPN usage. In February 2015, users of Nayatel, a popular internet service provider, received a notification that the PTA "has started blocking of IP addresses that are carrying unauthorized Voice over IP (VoIP) or Encrypted Virtual Private Networks (EVPNs), through an automated system".[50] This message reinforced advertising the PTA ran in national newspapers in 2014, advising people to stop using unauthorised VPNs.

Informal Obstacles to Personal Use of Encryption

Informal obstacles limit the uptake of strong personal encryption technologies. For example, there is a common perception that encryption technology is accessible only to tech savvy people or inconvenient to operate, Similarly, there is often lack of knowledge about which encryption tools offer the most security. Another barrier is the idea that constantly evolving technology makes it difficult to stay updated about proper use. Additionally, people may be indifferent to their communications being monitored.

While popular email services use weak forms of encryption, utilising the strongest form of encryption – end-to-end encryption – is a niche practice. Because weaker forms of encryption allow people other than those sending and receiving information (such as the email provider) to read communications, those communications remain insecure. Ultimately, end-to-end encryption is only a useful tool if a significant number of people use it.[51]

United Kingdom
Press responsibility to protect sources

While the use of strong encryption should be a minimum requirement for any newsroom, it is not widespread among members of the UK press. Alan Rusbridger, former editor-in-chief of *The Guardian*, has stated that "[strong] encryption is difficult for most journalists and it is quite time consuming and most journalists don't do it".[52] Although encryption alone is insufficient to protect sources, better encryption practices should be adopted by the press.

Poor digital security practices can have dramatic consequences. In 2011, British journalist and reporter Sean McAllister was detained by Syrian security agents while he working on a documentary about underground activists in Syria.[53] The agents seized his laptop, mobile phone, and other possessions that contained identifying information about the activists he had interviewed and communicated with. Subsequently, several of the activists were forced to flee the country, others were arrested, and one disappeared.[54]

Pakistan and Morocco

Civil society groups at risk when using encryption

In Morocco and Pakistan, the fact that informal obstacles – such as lack of knowledge about encryption – prevent a large number of people from using strong encryption has significant implications for the small number of people who do use strong encryption. When encrypted data traverses communications networks, it displays distinctive characteristics that make it conspicuous, allowing anyone who is monitoring that traffic to specifically target encrypted data.

Consequently, when human rights defenders and other civil society actors – those who most need to keep the content of their communications private – use encryption, they are not able to always entirely secure their communications, and in fact may put themselves at an increased risk of identification simply by using encryption. For example, when tools that encrypt the content of communications, such as PGP, are used, they nevertheless leave a trail of "metadata", data that in some cases can reveal information that can be used to identify the sender or recipient of a communication. Metadata such as the subject line and the email addresses of the sender and recipient of an email delivered using PGP are not encrypted, for instance.

On the other hand, if civil society actors fail to encrypt their communications, they also put themselves and those they communicate with at risk. Hisham Almiraat from the Digital Rights Association (Morocco) explains, "part of the reason why everyone should be using encryption is because if that doesn't happen only the usual suspects will use encryption and will raise traditional flags".[55] Similarly, Nighat Dad from the Digital Rights Foundation (Pakistan) notes, "not many people are using [strong encryption], so it's really easy for [authorities] to identify the individuals".[56]

Nonetheless, Nighat believes that people continue to use encryption in Pakistan to protect their communications. She notes, "the rights to privacy and freedom expression go hand in hand: if you can't express something to a colleague, family, or friend without fearing that authorities will eavesdrop on you, your rights are endangered." Furhan Hussain from Bytes for All (Pakistan) similarly considers that the choice to encrypt is something that every person should be able to make: "It's all about making that choice, to encrypt or not encrypt. I want to be able to draw and define the limits for my public and private spaces."[57]

Informal Obstacles to Online Anonymity

Extra-legal factors, such as corporate real name identification practices, impede people's ability to express themselves anonymously online. For example, in South Korea, the corporate sector makes it difficult for people to access information or express their views online anonymously because websites seek to verify users' identities. Additionally, lack of trust in the internet and fear of surveillance erode confidence in the anonymity of communications. In Morocco, many people lack trust in the internet as a safe space where they can speak freely and anonymously.

Morocco

Lack of trust in the internet as a safe space

When people lack trust in the internet as a safe space to communicate, or fear surveillance, their confidence that actions they take anonymously online are truly anonymous is eroded. In this environment, fewer critical voices are present in important public debates.

During the Arab Spring of 2011, as a wave of demonstrations seeking political reform began in Morocco, Mamfakinch.com emerged as a new citizen media platform facilitating the uncensored disclosure of information to the public. It soon became a popular online forum that aggregated written contributions by bloggers and Moroccan activists – all of whom used pseudonyms – who dared to challenge Morocco's authoritarian regime. Mamfakinch Co-Founder Hisham Almiraat notes, "among our regular columnists, we had engineers and individuals with high-level government positions who had a lot to lose if their identities were disclosed".[58]

In 2011, Mamfakinch journalists were victims of a "malware" attack – a sophisticated computer program that sends data from the targeted computer to a third party, while hiding its operation. The attack compromised the identity and security of those who ran the website and anyone who had been in communication with them.[59] The malware allowed its controllers to "secretly take screenshots, intercept e-mail, record Skype chats, and covertly capture data using a computer's microphone and webcam,

all while bypassing virus detection".[60] This attack fundamentally damaged Mamfakinch's contributors' trust in the internet as a safe space where they could express themselves without fear. Hisham Almiraat observes:

> **All of a sudden, people couldn't trust our ability to protect them anymore. People started to be cautious and we couldn't convince people to be as forthcoming as they once were. … We could buy new computers but the fear remained there. The well was already poisoned and it was very hard to convince people that it was okay for them to participate online again.**

Hisham emphasises that without trust in the idea that anonymous contributions will remain anonymous, those who would otherwise participate in debates keep silent.[61]

Indeed, scrutiny does follow those who speak out. In May 2015, following the publication of a Privacy International report that describes Hisham's experience at Mamfakinch, he received news that the Moroccan Ministry of the Interior had launched an investigation into "a group behind a report that allegedly accuses the intelligence services of spying on rights activists and journalists".[62]

South Korea
The role of corporate actors

Corporate actors require online users to verify their identity across a variety of South Korean websites, perpetuating an environment that makes speaking anonymously on the internet very difficult. Additionally, some companies routinely voluntarily hand over information to the government that allows their users to be identified.

The 2012 Constitutional Court ruling that declared the 2007 law mandating real name registration for major websites illegal resulted in a reduction of the number of websites requiring users to verify their identities.[63] However, the ruling did not make it illegal for commercial websites to continue requiring their users to identify themselves, and law still permits certain categories of companies to require users to submit government-issued identity numbers (RRNs) for identity verification purposes[64] Activist Byoung-Il Oh from Korean civil society organisation Jinbo Net notes that real name identification "has become so commonplace that Koreans are used to providing identifying information in many different settings without fully realizing the serious implications this has for their rights".[65]

Additionally, Korean law permits website and telecommunications operators to provide "user identifying data" to government authorities on a voluntary basis. Companies frequently comply with government requests for such data, in the absence of a court order or warrant requiring them to do so. In 2014, websites and telecommunications companies complied with 10 million such requests, a significant number for a country of 50 million people.[66] KS Park, a professor at Korea University and director of Open Net Korea, believes "the ready and warrantless availability of user identifying data is a significant threat to Koreans' ability to communicate anonymously online".[67]

> ***The ready and warrantless availability of user identifying data is a significant threat to Koreans' ability to communicate anonymously online.***
> **Professor KS Park, South Korea**

Opportunities

This booklet has highlighted a variety of legal restrictions and informal obstacles to the personal use of encryption and the exercise of anonymous speech online through examples from four countries. Alongside these challenges, there are also opportunities for governments, corporate actors, and civil society to better safe-guard individuals' and groups' ability to communicate privately and convey opinions anonymously online.

Governments

Governments need to assess whether laws, policies, and practices that affect personal use of encryption and online anonymous speech are consistent with their international human rights obligations. As a first step, governments should dismantle legal regimes that require state permission to use encryption or anonymity tools.

Governments should also do more to mainstream encryption. In certain areas, some governments already actively promote encryption and they can build on existing public messaging that encryption helps keep information secure. In South Korea, a series of hacking and online theft incidents led to a revision of data protection legislation.[68] The law now mandates that entities that handle personal information use appropriate technological means, including encryption, to protect that information.[69] Similarly, UK data protection legislation includes the principle that those controlling data must take "appropriate technical and organisational measures" to keep personal data secure and the UK Information Commissioner recommends encryption for "portable and mobile devices . . . used to store and transmit personal information, the loss of which could cause damage or distress to individuals".[70]

Corporate Actors

Major companies in the technology industry, such as Apple, Google, and Yahoo, are in a position to set the terms of policy debates around encryption. They can respect rights through a focus on user privacy supported by strong encryption.[71] Privacy needs to be "baked in" to products in order to protect users from cybercrime and overreaching government surveillance. Apple's iOS 8 already encrypts all the data on users' devices and other companies are also rolling out more secure products.[72] Additionally, companies should take a firm stance against building "backdoors", such as security vulnerabilities, into their product design.[73] Technology companies that have previously been complicit in the United States' ubiquitous spying programs now have an opportunity to make amends by refusing to craft insecure products.

Corporate actors who have real name identification policies in place should revisit the decision to require users to verify their identities. They should assess the impact their policies have on the exercise of anonymous speech online.

Civil society

Over two dozen organisations, including Privacy International, ARTICLE 19, Access, and PEN America, responded to the January 2015 call of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression for submissions on encryption and anonymity in digital communications.[74] This strong response illustrates civil society's belief that encryption and anonymity tools are important to the protection of human rights.

Civil society has an opportunity to champion the use of encryption and anonymity tools. Just as the Special Rapporteur's June 2015 report highlights that the United Nations system needs to improve its data security measures, civil society organisations too must ensure they use communication security tools in their daily work to better protect the constituencies they serve.

Civil society must promote and protect access to communication security tools and should mobilise its resources to identify obstacles to personal use of encryption and online anonymity. Civil society organisations must also become advocates for widespread adoption of encryption and anonymity tools and publicly make the case for their importance to protecting human rights. As internet use skyrockets, securing safe spaces online is an imperative civil society must champion before poor policies, practices, and laws become embedded.

> ***Securing safe spaces online is an imperative we must champion before it's too late.***

Endnotes

1 David Kaye, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/29/32 (22 May 2015), available at http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx.

2 See, Article 17 (right to privacy) and Article 19 (right to freedom of expression) of the International Covenant on Civil and Political Rights.

3 See, Danielle Kehl, "Encryption 101", *Slate*, 24 February 2015, available at http://www.slate.com/articles/technology/safety_net/2015/02/what_is_encryption_a_nontechnical_guide_to_protecting_your_digital_communications.html. The Electronic Frontier Foundation's "Security Self-Defense" offers "Tips, Tools and How-tos for Safer Online Communications", including explanations of how encryption works and can be used: https://ssd.eff.org/en.

4 Free end-to-end encryption tools are available at https://gpgtools.org/ and http://gpg4win.org/.

5 Jemima Kiss, "An online Magna Carta: Berners-Lee calls for bill of rights for web", *The Guardian*, 12 March 2014, available at http://www.theguardian.com/technology/2014/mar/12/online-magna-carta-berners-lee-web.

6 Frank La Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/23/40, (17 April 2013), para 23.

7 Ibid, para 53.

8 World Bank: "Population, Total", http://data.worldbank.org/indicator/SP.POP.TOTL?order=wbapi_data_value_2013+wbapi_data_value+wbapi_data_value-last&sort=asc, "Internet users", http://data.worldbank.org/indicator/IT.NET.USER.P2. The Human Development Index country rankings are available at http://hdr.undp.org/en/countries.

9 See, Kim Zetter, "Hacker Lexicon: What is a Backdoor", *Wired*, 11 December 2014, available at http://www.wired.com/2014/12/hacker-lexicon-backdoor/.

10 See, Cory Docotrow, "Encryption won't work if it has a back door only the 'good guys' have keys to", *The Guardian*, 1 May 2015, available at http://www.theguardian.com/technology/2015/may/01/encryption-wont-work-if-it-has-a-back-door-only-the-good-guys-have-keys-to-. Doctorow notes, "It's impossible to overstate how bonkers the idea of sabotaging cryptography is to people who understand information security". See also, Danielle Kehl, "OTI Policy Director Kevin Bankston Offers Ten Reasons why Backdoor Mandates are a Bad Idea", *Open Technology Institute*, 28 April 2015, available at http://www.newamerica.org/oti/oti-policy-director-kevin-bankston-offers-ten-reasons-why-back-door-mandates-are-a-bad-idea/. The most notorious backdoor installation effort was documented by Edward Snowden in 2013 and revealed a sustained effort by UK and US intelligence agencies to pressure technology companies to install systems that would allow these agencies to secretly access user data: Kim Zetter, "Hacker Lexicon: What is a Backdoor", *Wired*, 11 December 2014, available at http://www.wired.com/2014/12/hacker-lexicon-backdoor/.

11 In the early 1990s, the US government attempted to mandate backdoors, but backed away from proposals that included key escrow. See, Cory Doctorow, "Crypto wars redux: why the FBI's desire to unlock your private life must be resisted", *The Guardian*, 9 October 2014, available at http://www.theguardian.com/technology/2014/oct/09/crypto-wars-redux-why-the-fbis-desire-to-unlock-your-private-life-must-be-resisted.

12 "David Cameron says new online data laws needed", *BBC News*, 12 January 2015, available at http://www.bbc.co.uk/news/uk-politics-30778424.

13 David Kravets, "UK prime minister wants backdoors into messaging apps or he'll ban them", *arstechnica*, 13 January 2015, available at http://arstechnica.com/tech-policy/2015/01/uk-prime-minister-wants-backdoors-into-messaging-apps-or-hell-ban-them/.

14 See, for example, Samuel Gibbs and Alex Hern, "David Cameron in 'cloud cuckoo land' over encrypted messaging apps ban", *The Guardian*, 13 January 2015, http://www.theguardian.com/technology/2015/jan/13/david-cameron-encrypted-messaging-apps-ban.

15 Privacy International/IHRC correspondence with Jim Killock,19 May 2015. See also, Jim Killock, "What Does David Cameron Really Want?" *Open Rights Group Blog*, 13 January 2015, https://www.openrightsgroup.org/blog/2015/what-does-david-cameron-want.

16 Nigel Morris, "Information commissioner calls for protection of private data amid calls for 'snooper's charter'", *The Independent*, 13 January 2015, available at http://www.independent.co.uk/news/uk/politics/information-commissioner- calls-for-protection-of-private-data-amid-calls-for-snoopers-charter-9976278.html.

17 Regulation of Investigatory Powers Act 2000, available at http://www.legislation.gov.uk/ukpga/2000/23/contents.

18 Ibid, section 49(2)(b)(i)(ii). During the 2013-2014 period, the relevant authority granted 76 approvals out of 76 applications made to issue notices. Ultimately, 33 notices were issued and in 17 cases, individuals refused to comply with the notices, although only a small number were prosecuted. Office of Surveillance Commissioners, *Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to the Scottish Ministers for 2013-2014*, HC 343 SG/2014/92, September 2014, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/350857/Annual-Report-of-the-Chief-Surveillance-Commissioner-for-2013-2014-laid-4-September-2014.pdf.

19 Regulation of Investigatory Powers Act 2000, section 53. The maximum term increases to five years in cases relating to national security or a child indecency.

20 Christopher Williams, "UK jails schizophrenic for refusal to decrypt files: Terror squad arrest over model rocket", *The Register*, 24 November 2009, available at http://www.theregister.co.uk/2009/11/24/ripa_jfl/?page=1.

21 A copy of the 2010 directive, which has the subject line "Use of VPNs/Tunnels and/or Non-Standard SS7/VoIP Protocols" and is dated 2 December 2010, is available at http://www.ispak.pk/Downloads/PTA_VPN_Policy.pdf. A copy of the 2011 directive, which has the subject line "Usage of Encrypted VPNs" and is dated 21 July 2011, is available at http://twicsy.com/i/NoxrL.

22 The December 2010 directive states that "use of any non-standard means of communication… and non-standard protocols including all mechanisms the means of which communication becomes hidden or modified to the extent that it cannot be modified, is a violation of [regulations issued under a 1996 Act]". The second directive, which the PTA issued in July 2011, states that the first directive "had not been followed in true letter & spirit" and demands that service providers inform their users about the PTA's "instructions". The regulations are the PTA's Monitoring and Reconciliation of International Telephone Traffic Regulations 2010, available at http://www.pta.gov.pk/media/monitoring_telephony_traffic_reg_070510.pdf. The Act is the Pakistan Telecommunication (Re-Organization) Act 1996, available at http://www.pta.gov.pk/media/telecom_act_170510.pdf.

23 2010 and 2011 PTA directives.

24 2011 PTA directive.

25 Ansar Abbasi, "Grey phone traffic: IT authorities passing the buck to ISI", *The International News*, 5 December 2013, available at http://www.thenews.com.pk/Todays-News-13-27079-Grey-phone-traffic-IT-authorities-passing-the-buck-to-ISI.

26 While some press reports have suggested this regime may be dismantled, there are no indications that this is occurring. See, for example, "Curbing grey traffic: Govt to discontinue to ICH regime", *The Express Tribune*, 18 June 2014, available at http://tribune.com.pk/story/723892/govt-to-discontinue-to-ich-regime-to-curb-gray-traffic/.

27 IHRC interview with Nighat Dad, 12 March 2015.

28 IHRC interview with Furhan Hussain, 24 April 2015.

29 Loi 53-05 relative à l'échange électronique de données juridiques, Article 13, available at https://droitmaroc.wordpress.com/2008/01/29/loi-n%C2%B0-53-05-relative-a-lechange-electronique-de-donnees-juridiques-integrale/.

30 Ibid.

31 Ibid.

32 In 2014, Freedom House noted that "[t]here are no indications that the purchase and use of encryption software by private citizens or companies is restricted." Freedom House, *Freedom On The Net 2014*, at p 590, available at https://freedomhouse.org/sites/default/files/FOTN_2014_Full_Report_compressedv2_0.pdf

33 Law 53-05 requires notifying or receiving authorisation from the government in order to "use" cryptographic technologies. If interpreted as such, this legislation could be the basis to prosecute individuals who do not go through the appropriate approval mechanisms in order to encrypt communications.

34 Decree 2-08-518 of 2009 lists encryption tools falling within the purview of Law 53-05, Article 13(a), which requires prior notification to the government, as including means specifically designed and limited to serve in banking or financial operations, used for the creation and verification of electronic signatures, and conceived and limited to ensure software or online data security against unauthorised copying or usage. Decree 2-13-881, 21 May 2009, Annex I, available at http://www.mcinet.gov.ma/EconomieNumerique/Telecommunications/Documents/D%C3%A9cret%20n%C2%B0%202-08-518%20pris%20pour%20l%27application%20des%20articles%2013,%2014,%2015,%2021%20et%2023%20de%20la%20loi%20n%C2%B0%2053-05.PDF. Annex II in the same decree explicitly lists some types of encryption that are exempt from prior notification or approval requirements but does not explicitly include in the list the private use of encryption.

35 Law 53-05, Article 32.

36 This change took place through Decree 2-13-881 of 2015, which modified Decree 2-08-518. The change transferred powers from the civilian National Telecommunications Regulatory Agency (ANRT) to the military General Directorate for the Security of Information Systems (DGSSI). Decree 2-13-881, 20 January 2015, Article 1, available at http://adala.justice.gov.ma/production/html/Fr/liens/..%5C188896.htm.

37 IHRC interview with Hisham Almiraat, 11 March 2015.

38 See, for example, Marcel Rosenbach and Hilmar Schmundt, "Internet Evolution: the War on Online Anonymity," *Spiegel Online*, 5 August 2011, available at

http://www.spiegel.de/international/spiegel/internet-evolution-the-war-on-web-anonymity-a-778138.html. In addition, Freedom House notes that defamation is a criminal offence. Freedom House, *Freedom on the Net 2014*, pp 716-717, available at https://freedomhouse.org/sites/default/files/FOTN_2014_Full_Report_compressedv2_0.pdf.

39 National Security Act 1948, Article 7, available at http://www.law.go.kr/lsInfoP.do?lsiSeq=116750&efYd=20120701#0000. See, Amnesty International, T*he National Security Law: Curtailing Freedom of Expression and Association in the Name of Security in the Republic of Korea, 2012*, available at http://www.amnestyusa.org/research/reports/the-national-security-law-curtailing-freedom-of-expression-and-association-in-the-name-of-security-i.

40 Public Official Election Act. See, Freedom House, *Freedom on the Net 2014*, p 717.

41 An RRN is a 13-digit number assigned to a Korean citizen at birth that combines six digits of the individual's date of birth and seven uniquely assigned numbers. The seven uniquely assigned numbers appear random, but actually correspond to the person's sex (1 digit), place of birth (4 digits), order of birth (1 digit) and an authentication code (1 digit). These numbers were first issued in 1968 for the government to more easily identify communist spies, though their purpose has evolved over time. Resident Registration Act, Law N. 10733, Article 1, available at http://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A3%BC%EB%AF%BC%EB%93%B1%EB%A1%9D%EB%B2%95%2810733%29.

42 Information and Communications Network Act, Article 44(5). See, Freedom House, *Freedom on the Net 2014*, p 717.

43 Korean Constitutional Court, 2010 Hyun-ma 47, 23 August 2012, available at http://law.go.kr/%ED%97%8C%EC%9E%AC%EA%B2%B0%EC%A0%95%EB%A1%80/%282010%ED%97%8C%EB%A7%8847,20120823%29. In this ruling, both the majority and minority recognised that anonymity is necessary to ensure citizens' rights to freedom of expression and opinion: the majority included the right to express one's opinions and thoughts anonymously as part of the scope of freedom of expression granted in Article 21 of the Korean Constitution, while the minority articulated the core role of anonymity as a tool for political minorities to voice their opinions and critiques against authorities without fear of retaliation.

44 See, "Hackers steal, sell data on 8.7 million Korea Telecom subscribers", *The Verge*, 29 July 2012, available at http://www.theverge.com/2012/7/29/3200338/korea-telecom-data-breach-hackers-telemarketers. Legislation amending the Information and Communications Network Act 2012 that forbid the collection of RRNs on information networks (except for purposes with legal bases) entered into force in February 2013. Additional legislation, that forbid the collection of RRNs in general, except for purposes that have a legal basis, came into force in August 2014. The limiting of RRN collection since 2012 is not related to the Constitutional Court ruling.

45 Public Official Election Act, Law 12844, 19 November 2014, Article 82(6), available at http://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B3%B5%EC%A7%81%EC%84%A0%EA%B1%B0%EB%B2%95. The online portal is also required to delete any such postings that are not from an identified user.

46 In October 2014, South Koreans' ability to communicate anonymously online was further eroded by a mandatory SIM registration law. This is significant because an increasing number of Koreans use smartphones to access the internet. IHRC correspondence with KS Park, 20 May 2015.

47 2011 PTA directive.

48 See, Article 19 and the Digital Rights Foundation (Pakistan), "Pakistan: New Cybercrime Bill Threatens the Rights to Privacy and Free Expression", April 2015, p 6, available at

http://digitalrightsfoundation.pk/wp-content/uploads/2015/04/Pakistan-Cybercrime-Joint-Analysis_20-April-2015.pdf. See also, Privacy International, "Privacy International's Comments on the draft Prevention of Electronic Crimes Act, 2015 (Pakistan)", April 2015, available at https://www.privacyinternational.org/sites/default/files/Prevention-of-Electronic-Crimes-Bill-2015%20Legal%20Analysis_0.pdf.

49 See, for example, "Bad-mouthing: Pakistan's blasphemy laws legitimise intolerance", *The Economist*, 29 November 2014, available at http://www.economist.com/news/asia/21635070-pakistans-blasphemy-laws-legitimise-intolerance-bad-mouthing; "Pakistan: Investigate Killing of Rights Lawyer, 'Blasphemy' Law Fosters Persecution, Violence, and Murder", *Human Rights Watch*, press release, 14 May 2014, available at http://www.hrw.org/news/2014/05/14/pakistan-investigate-killing-rights-lawyer.

50 Email sent to Nayatel customers, 27 February 2014 (on file with IHRC).

51 The surprisingly small number of individuals who help maintain encryption tools is also a threat to generalised use of strong encryption, as the maintenance of the technology relies on the volunteer efforts of a limited number of people. Many encryption tools are open source – a regime that allows anyone to access the underlying code and help improve the technology. Software developer Werner Koch nearly single handedly maintains the free email encryption client GPG. Koch has experienced significant financial difficulties as a result of maintaining GPG on a volunteer basis. Julia Angwin, "The World's Email Encryption Software Relies on One Guy, Who is Going Broke", *ProPublica*, 5 February 2015, available at http://www.propublica.org/article/the-worlds-email-encryption-software-relies-on-one-guy-who-is-going-broke.

52 Dominic Ponsford, "Rusbridger on how no journalist's sources are safe, joining IPSO and why he would have kept News of the World open", *Press Gazette*, 28 March 2014, available at http://www.pressgazette.co.uk/rusbridger-how-no-journalists-sources-are-now-safe-joining-ipso-and-why-he-would-have-kept-news. *The Guardian* uses "SecureDrop" "an open-source whistleblower submission system that media organizations can install to accept documents from anonymous sources", which relies in part on strong encryption. SecureDrop can be accessed at https://securedrop.org.

53 Matthieu Aikins, "The spy who came in from the code: How a filmmaker accidentally gave up his sources to Syrian spooks", *Columbia Journalism Review*, May/June 2012, available at http://www.cjr.org/feature/the_spy_who_came_in_from_the_c.php?page=all.

54 Ibid.

55 IHRC interview with Hisham Almiraat,11 March 2015.

56 IHRC interview with Nighat Dad, 12 March 2015.

57 IHRC interview with Furhan Hussain, 24 April 2015.

58 IHRC interview with Hisham Almiraat,11 March 2015. Mamfakinch means "not giving up" in Arabic.

59 An email sent to Mamfakinch journalists included a Word document purporting to contain insider information on a scandal. The document in fact contained a hidden file. For more information on the malware attack against Mamfakinch, see, Morgan Marquis Boire, *Backdoors are Forever: Hacking Team and the Targeting of Dissent*, The Citizen Lab, October 2012, available at https://citizenlab.org/wp-content/uploads/2015/03/Backdoors-are-Forever-Hacking-Team-and-the-Targeting-of-Dissent_web-sitepdf.pdf.

60 Ryan Gallagher, "How Government-Grade Spy Tech Used a Fake Scandal to Dupe Journalists", Slate, 20 August 2012, available at http://www.slate.com/blogs/future_tense/2012/08/20/moroccan_website_mamfakinch_targeted_by_government_grade_spyware_from_hacking_team_.html.

61 For more information on surveillance in Morocco, see Privacy International, *Their Eyes on Me: Stories of Surveillance in Morocco*, April 2015, available at https://www.privacyinternational.org/?q=node/554.

62 See, Privacy International, "Statement about the Moroccan government's intimidation of civil society", 13 May 2015, available at https://www.privacyinternational.org/?q=node/583.

63 Since then, for instance, one of the main Korean internet portals, Daum (http://www.daum.net/), has ceased real name identification.

64 The law contains an exception for a certain category of businesses and entities (notably, mobile service providers), but incorporates fines of up to KRW 500 million (around USD 455,000) for failing to protect this information. Because telecommunications companies are allowed to continue collecting RRNs, they can provide identity verification services to internet companies that operate real-name systems.

65 IHRC interview with Byoung-Il Oh, 5 March 2015; correspondence with Byoung-Il, 23 May 2015.

66 South Korea Ministry of Future Planning and Science, Press Release, 19 May 2014, available at http://www.xn--vb0b54r8od4wb7yz1lfqqs.com/www/brd/m_211/view.do?seq=1736&srchFr=&srchTo=&srchWord=&srchTp=&multi_itm_seq=0&itm_seq_1=0&itm_seq_2=0&company_cd=&company_nm=&page=2. IHRC correspondence with KS Park, 20 May 2015.

67 IHRC correspondence with KS Park, 20 May 2015. IHRC interview with KS Park, 4 March 2015. See, KS Park, "Communications Surveillance in Korea", *Open Net Korea*, available at http://opennetkorea.org/en/wp/main-privacy/internet-surveillance-korea-2014?ckattempt=1.

68 For example, "[in] January 2014, a computer contractor working for a credit bureau stole unencrypted personal data, including [resident numbers] and credit card details, belonging to 20 million South Koreans". "Credit Card Details on 20 Million South Koreans Stolen", *BBC News*, 20 January 2014, available at http://www.bbc.com/news/technology-25808189.

69 The Personal Information Protection Act (PIPA) governs the requirements and procedures for handling personal information online. Failure to appropriately protect personal information can result in penalties ranging from a fine to imprisonment. Personal Information Protection Act 2011, Articles 2.1 and 71, available at http://www.law.go.kr/lsEfInfoP.do?lsiSeq=142563#0000.

70 Data Protection Act 1998, Schedule 1, Part I, available at http://www.legislation.gov.uk/ukpga/1998/29/contents; UK Information Commissioner's Office, "Encryption", https://ico.org.uk/for-organisations/encryption/.

71 See, The UN Guiding Principles on Business and Human Rights, available at http://business-human-rights.org/en/un-guiding-principles.

72 Ken Gude, "The FBI Is Dead Wrong: Apple's Encryption Is Clearly in the Public Interest", *Wired*, 17 October 2014, available at http://www.wired.com/2014/10/fbi-is-wrong-apple-encryption-is-good/. Similarly, Apple rolled out strong encryption by default for iMessage and FaceTime, making security easily attainable for a large group of people as users did not have to take any steps on their own to encrypt their messages. See, Apple, "Privacy", https://www.apple.com/privacy/privacy-built-in/.

73 Yahoo's CISO Alex Stamos, for example, has been a vocal critic of backdoors equating them to "drilling a hole in a windshield". Dan Goodin, "Yahoo exec goes *mano a mano* with NSA director over crypto backdoors", *ArsTechnica*, 23 February 2015, available at http://arstechnica.com/tech-policy/2015/02/yahoo-exec-goes-mano-a-mano-with-nsa-director-over-crypo-backdoors/.

74 Submissions are available at http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx

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