PRIVACY INTERNATIONAL

After the Gold Rush: Developing Cyber Security Frameworks and Cyber Crime Legislation to Safeguard Privacy and Security

August 2018

Contents

Introduction

The integration of technology into almost every aspect of our everyday lives has brought many changes, benefits and challenges. Governments around the world are playing catch up in terms of understanding the impacts and drafting appropriate regulation and legislation.

Technology of course advances faster than legislation; nevertheless, it is a government's responsibility to provide safety and security and to protect the enjoyment of human rights. Many governments around the world are therefore either updating national legislation governing technology, or starting from scratch. It is common for governments to use the terms "cyber security" and "cyber crime" when they do so. But what is the difference? What do these terms mean in practice? What does best practice look like? Why legislate at all? What should and should not be included in such legislation?

Both "cyber security" and "cyber crime" are terms widely used but often poorly understood. This confusion can lead to legislation that undermines human rights and neither secures nor protects people, their devices and the technological infrastructure we rely on.

The purpose of this Briefing Paper is to provide a brief overview of terminology, concepts and trends in addressing cyber security and cyber crime. It describes the differences between them and associated challenges for the protection of peoples' security and their human rights. In addition, it flags approaches that would, on the contrary, undermine security and human rights. It also highlights key elements and examples from cyber security frameworks and cyber crime legislation globally. The aim is to provide a basis for government and civil society to have an informed, evidence-based and constructive discussion of the effect of different approaches to cyber security and cyber crime, to arrive at frameworks and laws that protect both security and human rights.

The Difference Between Cyber Security and Cyber Crime

What is cyber security? Essentially, cyber security describes a technical approach to securing systems from attack and failure. Computer systems are complex and almost certainly contain flaws that affect the security of those systems. Good cyber security recognises that computer systems contain vulnerabilities and addresses the root causes of insecurity, by prioritising the identification and fixing of those vulnerabilities.[1] In addition, there is the need to consider and mitigate the human factor as key causes of cyber security failures, as well as technical factors.

What is cyber crime? While cyber security is concerned with technically securing systems from attack and failure, the core principle of cyber crime is punishing unauthorised access to computer systems with a specified intent, in order to ultimately prevent damage or alteration of systems and the data on it.

Why Should Cyber Security and Cyber Crime Be Considered Separately?

Governments are often tempted to cover everything to do with "cyber" in one law. But addressing cyber security and cyber crime is complex. It requires separate consideration of the issues and safeguards designed to address the unique privacy and security implications of each, which will be discussed in this paper. Failing to draw distinction between the two risks undermining security and diluting protection for everyone. For example, in 2014, the African Union adopted *The Convention on Cyber Security and Personal Data Protection*. It covers cyber security, cyber crime and data protection in one law. Member states have been slow to ratify it, possibly due to its length, complexity, unfamiliar terminology and lack of discussion of its content.

Cyber Security

What Should a Government's Approach to Cyber Security Look Like?

The first questions a government should ask to test their proposed approach to cyber security should be: Is it going to protect people, including their personal data? Does it address the insecurity of devices? Will it make the country's infrastructure more resilient to attack? If the answer is 'no' or 'don't know' to any of these questions, the approach should be revisited.

Good cyber security policies and practices put people and their rights at the centre and seek to strengthen and protect human rights rather than curtail them. There are two, core fundamental principles:

1. Cyber security as a public good: A government's approach to cyber security should first and foremost be to treat it as a public good – treating it in the same way it treats public health for example, where collective responsibility is promoted for the benefit of everyone.

2. Securing the individual helps secures everyone: In a cyber security context, to secure the individual, Privacy International believes that protecting and defending individuals, devices and networks should form the basis of any cyber security strategy.

Protecting individuals

As more of our lives are lived online, personal data has become increasingly valuable. The value of the data is exactly why companies and governments want to collect, access, and mine it, and criminals want to steal it. However, it is essential to avoid putting too much emphasis on the duty of individuals to protect themselves as this approach plays down the responsibilities of companies, governments and other stakeholders.

Companies and governments build systems, devices, networks and services that generate and accumulate vast data stores without proper regard to risk, security, or data minimisation. Therefore, cyber security frameworks must include data protection laws which safeguard against the exploitation of personal data collected by companies and public bodies.

BOX 1. Protecting Individuals: Data Intensive Project Risks and the Importance of Data Protection

Privacy International and partners have observed that governments are keen to develop data-intensive projects but fail to properly consider how they will secure the personal data those projects generate. For example, some countries without data protection laws are developing projects including smart cities (e.g. India and Indonesia) or biometric voter registration systems (e.g. Kenya).

Data breaches continue globally, and the numbers involved are staggering. Continued scrutiny of Aadhaar, the national identity project in India has revealed serious flaws in security, for example where Aadhaar identity numbers were published alongside personally identifiable information on several government websites.[2] Similarly, the personal information of over 55 million Filipino voters held by the electoral commission were made publicly available, the biggest data breach in the Philippines' history.[3] The personal information of over 93 million voters in Mexico,[4] including home addresses, were openly published on the internet after being taken from a poorly secured government database. This can be highly sensitive information in a context where there are severe abuses of human rights. For example, up to 100,000 people are reportedly kidnapped each year.[5] Making their home addresses publicly available potentially increased exposure to such risks.

Protecting devices

While it is cheap to connect devices to the internet, it is generally agreed among security experts that the security of devices such as routers, webcams and other household objects connected to the internet — known as the "Internet of Things" — is very poor. Many devices have poor security such as no or default passwords, and are difficult or even impossible for everyday users to change. Therefore, many of these internet-connected devices are vulnerable. Securing devices should be a key cyber security objective, both for the risk they pose in relation to the personal data they generate, collect and transmit and for the security risks they pose as integrated in or as part of a network.

BOX 2. Protecting Devices: The Impact of the 2016 Mirai Botnet

The failure to adequately protect both device and network security was famously demonstrated in October 2016 when malware, known as Mirai, powered a huge denial of service (DDoS) attack, enabled by a botnet of hundreds of thousands of infected internet connected devices, such as consumer webcams, baby monitors and even public CCTV cameras. It targeted the Dyn network that hosted a range of popular websites such as Twitter, Netflix and the New York Times, which were made inaccessible for a time.[6] Being unable to access these websites is inconvenient, but the real significance lies in the fact that the malware targeted and denied access and service to sections of a global network. This type of attack therefore raises questions about the security of network infrastructure as a whole. Denial of service at this scale could cripple critical infrastructure, particularly as we continue to connect systems to networks.

Protecting networks

Securing networks is an integral yet often neglected part of cyber security policy discussions. Good network security means reducing the attack surface and then allowing only the right people through the right devices to access the right services on a network, while keeping everyone and everything else out. Protecting and defending a network can mean protecting a home Wi-Fi connection, a company's intranet, a telecommunications network accessed by the public, a bank's network, an industrial control system (ICS) in a factory, or a nation's critical infrastructure such as a power grid.

BOX 3. Protecting Networks: Lessons Learned from the 2015 Cyber Attack on Ukraine's Power Grid

Perhaps one of the most famous attacks on a network of the past few years is the 2015 attack on Ukraine's power grid, part of the country's critical infrastructure, which left over 200,000 people without power for several hours. Successful attacks on networks often require successful attacks on individuals and devices to make them happen, as highlighted in the resulting analysis of what happened in Ukraine.[7] The attack struck right at the heart of government fears of attackers leaving a country literally in the dark or escalating into "cyber warfare" (which is often an exaggerated claim). However, the attacks on Ukraine's power grid served as a wake-up call for the government. Ukraine adopted a cyber security strategy in 2016 which identified and prioritised key areas for the country's cyber security, updated legislation and improved technical capabilities. The lesson for governments here is: Don't wait or put off assessing and improving the country's cyber security protection.

Key Elements of Good Cyber Security Policy

Ensuring that our devices, networks and services are secure is a constant challenge. Security is hard and 100% security can never be guaranteed. Even multi-million dollar organisations get it wrong, evident in the continuing and widely reported global data breaches - from the theft of information from poorly secured databases in company and government networks to 'ransomware' spreading with relative ease through networks.

It must be stressed — over and over — that it is impossible to prevent all cyber attacks. Systems are inherently vulnerable and it is likely that systems will suffer some degree of attack at some point. Technologists are fond of saying that it is inevitable you will fail, but you need to fail well. "Resilience" is a key word in cyber security: preventing attacks as much as possible is of course important, but recovering well from an attack and ensuring no loss of data or permanent damage to a system is equally important.

Security requires multiple actors — particularly security researchers, industry and the government — to commit significant resources and cooperate with each other to achieve this goal. Much preparation and expertise are needed.

Cyber security comes in different forms and is made up of many different elements that improve resilience. Legislation may be just one of these elements. Although the law can provide for a framework to work in practice, it is not sufficient or appropriate to draft one law that attempts to cover everything to do with cyber security and a law is never enough if it is not accompanied by robust implementation.

Therefore, we would not expect to see "cyber security" law in isolation, rather a framework of different initiatives and approaches that complement each other and fit together. Below is a description of different measures governments take when devising their national cyber security framework:

Policies

Many elements of cyber security rely on non-legal mechanisms, such as minimum standards of security, investment in security research, security audits of key industries and public bodies. Government policy in this area can make a real difference in raising standards of security.

Governments often begin by drafting a guiding policy, such as a National Cyber Security Strategy, or an ICT Policy, which sets out a country's vision for their future and guides to priorities. It may contain all or some of the aspects below. However, while these policies may look good, in reality the legislation that follows often contradicts the objectives of strategies and policies.

BOX 4. Conflicts Between Policy and Legislation: The Example of Zimbabwe

Zimbabwe's detailed 2015 ICT Policy sets out a vision of a strong ICT sector and resilient infrastructure in Zimbabwe that brings economic benefit and ICT leadership in Africa.[8] It recognises the lack of a cyber security framework as a disadvantage and highlights the country's *"overall security objective is to ensure the availability, integrity and confidentiality of data in cyberspace,"* including *"identifying the need to adopt data protection and privacy."*

However, the resulting draft Cyber Security and Cyber Crime Bill (2017)[9] struck a very different tone, focusing instead on controlling social media and silencing dissent. As the Media Institute of Southern Africa (MISA) outlined in a briefing[10] *"the government is giving the impression of wanting to shield itself from criticism rather than protect the people from actual harm."* The draft Bill is a missed opportunity at a crucial moment in Zimbabwe's history to provides strong protections for people's privacy and security.

Identify and prioritise the security of a country's critical infrastructure

Critical infrastructure is largely defined as essential systems whereby their damage or loss would have a significant impact on the functioning of the State and the safety of the people. Sometimes governments overlook the fact that the security of a country's critical infrastructure is a key priority.

The historical origins of critical infrastructure may appear in some countries as legislation that refers to 'Key Point' protection. But the issue with Key Point legislation was that it was mostly biased towards protecting defense infrastructure and therefore shrouded in secrecy. A different approach is now appropriate, because modern critical infrastructure protection often requires the active participation and understanding of private companies as they own more of the infrastructure than before such as telecommunications, nuclear, water etc. Most critical infrastructure relies on ICT's to work (sometimes referred to as Critical Information Infrastructure). For example, the European Union Network Information Security (NIS) Directive (2016)[11] identifies essential services, and therefore the critical infrastructure that must be protected:

Energy (Electricity, Oil, Gas)
Transport (Air, Rail, Water, Road)
Banking
Financial market infrastructures
Health
Water
Digital Infrastructure

Each country may categorise critical infrastructure differently, and some countries include nuclear, food, emergency services and chemicals for example.

Once identified, a State may want to legislate to ensure the protection of a country's critical infrastructure, such as minimum safety standards, establish mechanisms for reporting security breaches, and plans for incident response and recovery.

BOX 5. Critical Infrastructure Controversies: The Case of South Africa

Critical infrastructure identification is usually not high on the list of challenges the human rights community faces in their daily work. However, the example of South Africa demonstrates that civil society should be vigilant. In 2017, a Critical Infrastructure Protection Bill[12] was presented to Parliament which seeks to replace the apartheid-era National Key Points Act,[13] which was passed in 1980 to deal with the perceived threat of sabotage to apartheid infrastructure.

The list of national key points was a closely guarded secret and a particular point of controversy. It was suspected that the list was used as a way to shield officials and institutions from public scrutiny and undermine accountability.

In 2014, Privacy International's partners in South Africa, Right to Know, and the SA History Archive brought a court case challenging this secrecy and the Ministry of Police was ordered to release the list of National Key Points to the public.[14] It came as no surprise that national key points extended to sites that would not be considered critical infrastructure. This revealed that the President at the time, Jacob Zuma's private Nkandla home had been declared a national key point, as well as the President's official residences, and he received public funds for "security upgrades" to his private home that had nothing to do with security - the most notable being a "fire pool", which looked suspiciously to everyone else like a luxury swimming pool.

In the Critical Infrastructure Protection Bill, still making its way through Parliament at the time of writing, everything that was classified as a national key point will be transferred over and remain critical infrastructure by default for 5 years, pending a review. But there is no reason to believe that anything classifiable as a national key point will not also be classified as critical infrastructure by the end of the review. That could include the private residences of former Presidents - the homes of Mandela, Mbeki and de Klerk are all on the national key point list as well.

Establish incident response teams

These teams of experts are the frontline for when a security incident happens, in fact they probably uncovered it. The teams mostly deal with compromised devices or services that are enabling cyber attacks and their operations are underpinned by the rule of law.

There are many different kinds of incident response teams, some have national responsibilities, and some are sector specific. The most common is a Cyber Security Incident Response Team (CSIRT),[15] which handles security incidents that happen to ICT infrastructure. Most countries may have at least one, but it is often unclear how active they are.

Ideally, CSIRTs should be independent of government, but in reality are often housed in government ministries of intelligence agencies. The government should also support security researchers to help find vulnerabilities in systems so they can be fixed. FIRST, the global forum of incident response and security teams, conduct training workshops and have a lot of resources available on how to set up a CSIRT.[16]

Carry out a threat assessment and develop recovery plans

A threat assessment considers possible weaknesses, such as outdated infrastructure, that make the country more vulnerable to attack. Essentially, how can a government be confident that a country's infrastructure is resilient to attack if nobody knows what the actual threats are? Once threats have been assessed, this helps allocate precious resources to tackling the most acute threats. CSIRTS can help in making these assessments.

BOX 6. Example of a Cyber Security Framework: The European Union

A Cyber Security Strategy:[17]

This sets out priorities such as access for all, shared responsibility for cyber security, resilience of networks, reducing cyber crime, growing industry and fostering innovation, co-ordination between responsible actors.

Legislation:

- The proposed Cyber Security Act: Focuses on the security of products and services.[18]
- The Directive on the Security of Network and Information Systems (the "NIS Directive") 2018: Focuses on securing critical infrastructure[19]
- The draft ePrivacy Regulation: Focuses on the duty of electronic communications companies to secure confidentiality of electronic communications and protect their products/services against unauthorised access.
- The General Data Protection Regulation (the "GDPR") 2018[20]

Warning Signs in a Cyber Security Strategy: "Offensive" Approaches to Cyber Security

The approaches outlined above are considered "defensive" security – actions to secure systems from attack. However, there is a growing trend of governments around the world to focus on "offensive" security, that is focused mainly on increasing surveillance and other offensive capabilities. This raises a number of concerns:

- Critically, it is an approach that prioritises insecurity at the expense of security.
- Ramping up offensive powers at the expense of defensive capabilities and expertise is the wrong approach to cyber security. This will not secure a country's critical infrastructure and individuals in the long run. In Privacy International's experience of challenging government surveillance, we have observed that governments tend to presume that insecurity is acceptable if it enables their surveillance goals. It further shrouds cyber security in secrecy, as it is often led by intelligence agencies or the military, leaving the public and businesses at a disadvantage as they are not aware of the real threats and how they can protect themselves. This approach leaves the security of devices, networks, and services at risk. They are the opposite of cyber security.
- Because governments are combining cyber security with surveillance, they often perceive that they can adopt such actions with little public discussion and inadequate oversight or safeguards. A clear, accessible and comprehensive legal framework(s) should be established through primary legislation and debated in the legislative branch with public consultation and involvement of stakeholders as a matter of good governance and respect for the rule of law and human rights. But in this area, it is a particularly vital part of the policymaking process because many of the related processes will be carried out behind closed doors, without the opportunity for public scrutiny.

BOX 7. Example of a Cyber Security Law: Thailand and the Creation of a Cyber Security Committee

In some countries, cyber security laws are focused around one thing: creating a "cyber security committee". It may be the first piece of cyber security legislation a government drafts and may take some time to pass, holding up the essential work outlined above. Committee members are often made up of representatives from different government ministries. It can often be unclear what cyber security expertise these government representatives have. Therefore, real efforts must be made to ensure members have sufficient expertise — perhaps by including members from academia, civil society and even industry.

Committees may also include members from the national intelligence agency. While this is not necessarily a major issue, as they may be familiar with the threats, it does mean that activities relating to cyber security are less transparent. As intelligence agencies operate in secret, often without sufficient oversight of their activities, what is being done in the name of cyber security is not clear and open to abuse.

It is also unclear what action these Committees take in the interim while cyber security frameworks are being developed. There are also concerns around the powers that are given to Committees. In Thailand for example, the proposed Cyber Security Bill[21] is dedicated to setting up a National Cyber Security Maintenance Committee, outlining members (picked from government and public agencies) duties and powers.

The concern is that it gives the committee wide ranging powers to conduct communication surveillance and take down content without adequate safeguards and limitations in accordance with the principles of legality, necessity and proportionality. There is no judicial authorisation required, so the Committee just decides. As Thailand has no comprehensive surveillance law, this bill seems to be allowing surveillance by the back door by giving the Committee these powers.

Examples of "Offensive" Powers That Pose Challenges Both for Security and Human Rights

Hacking for surveillance[22]

A growing number of governments around the world are also embracing hacking to facilitate their surveillance activities. When governments hack for surveillance purposes, they are prioritising insecurity, undermining the security that is vital.

Because government hacking for surveillance purposes entails unique and extensive interferences with privacy and other fundamental rights and poses significant risks to the security of devices and networks, they may never be able to demonstrate that hacking as a form of surveillance is compatible with international human rights law, even where the hacking is in connection with legitimate surveillance activities, such as gathering evidence in a criminal investigation or intelligence. To date, however, there has been insufficient public debate about the scope and nature of these powers and their privacy and security implications.

Hacking is a complex issue and there is little room to go in-depth in this Briefing Paper. Privacy International has produced a set of 10 Hacking Safeguards and accompanying briefing with examples, designed to help interested parties assess government hacking in light of applicable international human rights law and to understand the security implications of this surveillance practice. By providing more detailed information on practices that are often carried out in secret and difficult for non-specialists to understand, the idea is to spur informed, public debate about the scope and nature of government hacking powers and their privacy and security implications and to engage governments in a constructive discussion about how they are balancing the many duties owed to citizens.[23]

Attempts to weaken or criminalise encryption[24]

Once the domain of solely the technologically savvy, end-to-end encryption is now readily available and a feature of some accessible communication applications such as Facebook's WhatsApp, OpenWhisperSystem's Signal, and Apple's iMessage. What is essential about end-to-end encryption is that the messaging content is secure even from the infrastructure provider itself – if these providers are compromised, the messages themselves should remain secure.

As encryption is increasingly used, some governments are seeking to limit its availability under the justification that they need to access encrypted communications in order to fight terrorism or prevent serious crimes, including the sexual abuse of children.

There are a number of concerns about this practice:

- Encryption is important for both privacy and freedom of expression and because it underpins the secure functionality of the internet and facilitating global online commerce.
- There are clear security risks of putting in 'backdoors' to encryption, that is, creating a weakness that allows governments (and other actors) to access encrypted information. The problem is that once a vulnerability is created in a tool like end-to-end encryption to allow for this exceptional access, it can introduce new weaknesses that can be discovered and exploited by others across many different services.

BOX 8. Examples of Government Attacks on Encryption

- In Morocco, the use of encrypted messaging services is restricted and "unauthorised" use can be punished with imprisonment and a $10,000 fine.[25]
- In Pakistan, the 2016 Prevention of Electronic Crimes Act established vague criminal prohibitions on the supply of computer software and the programming of computer systems, which could be broadly interpreted to crack down on the use of encryption tools and networks that provide anonymity (such as Tor and VPNs).[26]
- In Turkey, thousands of people were arrested on suspicion of being a member of the Gülen movement, based on alleged use of an encrypted messaging service called Bylock. The list of those arrested stretches to business people, engineers, nurses, civil servants, teachers, doctors, civil servants, employees of the Turkish Telecommunications Authority and the Turkish Financial Regulatory Authority, judges, lawyers and police officers. A Turkish judge at the International Criminal Court was sentenced to seven years and six months in prison for membership of the Gülen movement, based on his use of Bylock.[27]

Cyber Crime

What Should Be in a Cyber Crime Law?

A narrow interpretation

As outlined at the start, cyber crime is distinct from cyber security. Yet cyber crime has become a catch all term and often confused with cyber security. While cyber security is concerned with technically securing systems, the core principle of cyber crime is punishing unauthorised access to computer systems with a specified criminal intent, in order to ultimately prevent damage or alteration of systems and the data on it. This means that the focus of cyber crime is actually quite narrow: first and foremost, crimes that can only be committed using a computer or device, known as **"cyber dependent crime"**.

BOX 9. Examples of Cyber Dependent Crimes

- Breaking into the computer systems of, for example, a nuclear facility with the intention of shutting it down.
- "Phishing"; sending out fake emails pretending to be a bank in order to gain people's passwords and details.
- Spreading viruses and trojans, such as "ransomware", which once downloaded onto a computer locks users out of their files until a ransom has been paid to restore access.
- Initiating a distributed denial of service ("DDOS") attack, which can disable websites.
- Distributing malware which can, for example, record key strokes and steal passwords for online bank accounts.

However, cyber crime legislation tends to be much broader, covering a vast array of crimes. As we explore in the rest of this briefing, this can cause problems when governments open the list of crimes.

Cyber enabled crimes

Most cyber crime laws do include the narrow interpretation mentioned above, of punishing unauthorised access. Then the list of crimes begins to grow. Most cyber crime also include "cyber enabled crimes." Cyber enabled crimes refer to established crimes committed in a new way using technology, essentially crimes that could be committed online or offline.

Box 10. Examples of Cyber Enabled Crimes

- Fraud
- Distribution of child abuse images
- More recently, distributing intimate images without consent (known as "revenge porn")

As cyber crime knows no borders, cross border co-operation is often required for effective action. A narrow list of crimes is certainly useful in prompting harmonisation in identifying and defining cyber crime, which could allow quicker cross border cooperation to solve these crimes.

However, inclusion of cyber enabled crime in a cyber crime law is not the end of the story. For example, distributing child abuse images is a crime whether using a computer or not. Therefore, it should be included as part of a comprehensive child protection legal framework where the crime can be defined more precisely and importantly, where the crime can be contextualized in its broader context – alerting the authorities and those trying to avoid committing the crime to the core concerns and tools the authorities have in tackling the crime. Essentially, it doesn't make sense to only have child abuse images online a crime without a wider child protection framework.

Crimes which are not crimes

Opening up the list of crimes beyond cyber dependent crimes to anything involving a computer is problematic. The risk is that some governments start to extend that list to include criminalising behaviour which is not a crime and in doing so, results in violations of international human rights law.

BOX 11. Examples of Misuse of Cyber Crimes Legislation

- The Computer Misuse Act (2011) in Uganda has been used to criminally charge a journalist investigating government corruption.[28]
- The Computer Crime Act (2016) in Thailand has been used to prosecute cases of "lese-majeste", involving expression about the Royal Family that is perceived as negative.[29]
- The Prevention of Electronic Crimes Act (2016) in Pakistan regulates what is perceived as 'hate speech'.[30]
- The new 2018 Cyber Security Law in Vietnam prohibits "the use of cyberspace" to *"prepare, post, and spread information"* that *"has the content of propaganda opposing the State of the Socialist Republic of Vietnam,"* or *"offends the nation, the national flag, the national emblem, the national anthem, great people, leaders, notable people, and national heroes"* (Articles 8 and 15)".[31]
- Egypt passed the *Law on Combating Information Technology Crimes* in June 2018. Article 25 punishes anyone who *"frequently sends a large number of emails"* or insults *"family principles and values in Egyptian society"* with five months in prison, essentially criminalising criticism of the government. Moreover, the law permits authorities to issue travel bans to anyone who might "attempt" to commit a crime outlined in the law. This effectively allows the government to punish any internet user in Egypt.[32]

Warning Signs: Concerns about Cyber Crime Laws and Uninformed Use of the Budapest Convention

The Council of Europe's Convention on Cyber Crime 2001 (known as the "Budapest Convention") has influenced cyber crime laws in almost all of the 47 Member States in the Council of Europe, in 15 other countries that are not CoE Member States but have ratified it, as well as among a wider set of other countries that have not ratified the Convention but may be heavily influenced or simply "copying and pasting" sections of the Budapest Convention into their own laws without necessarily understanding the full implications. The section below unpacks the significance of this so that readers can recognise the influence of the Budapest Convention on their own country's cyber crime framework and become familiar with the challenges this presents from a human rights perspective.

BOX 12. A Note on the Budapest Convention

The Budapest Convention entered into force in 2004 and Council of Europe Member States are expected to translate the Budapest Convention into their national laws. All 47 Member States have ratified the Convention, with the exception of Sweden, the Russian Federation, Ireland and the micro-state of San Marino.[33]

The Council of Europe intended for the Budapest Convention to, "serve as a guideline for any country developing comprehensive national legislation against Cybercrime and as a framework for international cooperation between State Parties to this treaty."[34]

The Budapest Convention contains the following three major aspects:

- **A List of Crimes:** It includes a list of crimes that each member country must have on its books. (Articles 2-11).
- **Investigative Powers:** It requires each participating nation to grant new powers of search and seizure to its law enforcement authorities, including the power to force an ISP (Internet Service Provider) to preserve a citizen's internet usage records or other data, and the power to monitor a citizen's online activities in real time (Articles 16-22).
- **Cross Border Assistance:** It requires law enforcement in every participating country to assist police from other participating countries by cooperating with "mutual assistance requests" from police in other participating nations "to the widest extent possible" (Articles 23-35).

The Budapest Convention is open to non-member States for ratification. Currently, it has been ratified by Argentina, Australia, Cabo Verde, Canada, Chile, Costa Rica, Dominican Republic, Israel, Japan, Mauritius, Morocco, Panama, Philippines, Senegal, Sri Lanka, Tonga and the USA.[35]

Missing the broader human rights framework of protection that should accompany the Budapest Convention

Council of Europe Member States that have ratified the Budapest Convention must also have adopted the European Convention of Human Rights and European Data Protection Legislation. In other words, it was assumed that the Budapest Convention would be complemented by a broader legal framework that would underpin safeguards binding on the Member States. The Council of Europe has developed many other accompanying guidance documents based on this, such as guides for law enforcement on how to protect personal data while combatting crime,[36] that would be expected to be followed in implementing the Budapest Convention.

While Council of Europe Member States are all parties to the European Convention on Human Rights which offer strong protection on human rights backed up by legally binding judgments of the European Court of Human Rights, such protection is absent for non-Council of Europe states which ratify the Budapest Convention.

When the Budapest Convention is ratified or sections copied and pasted by non-member States, these safeguards are lost as non-member states are not bound by the European Convention on Human Rights, may not have their own system of safeguards and importantly, may not even be aware of the importance of such accompanying safeguards — nor will their citizens. Instead, what is left is therefore legislation that includes very intrusive measures in the absence of these balancing safeguards.

In other words, the Budapest Convention assumes a level of human rights protection in a State's existing legislation that is not a reality in some countries. Nor is the Convention explicit about this expectation to alert governments, citizens and civil society of the need to adopt or reinforce complementary measures. As a result, copying and pasting the Budapest Convention has become an accelerator of legislating for increased surveillance, minus the safeguards, rather than the balanced approach to protecting against cyber crime that was no doubt originally intended by an organisation (the Council of Europe) that has a long history of protecting human rights.

Opening the door for an extended list of "crimes"

The Budapest Convention provides a list of cyber crimes.[37] A list is certainly useful in prompting harmonisation in identifying and defining cyber crime, which of course knows no borders, and therefore often requires international cooperation for effective action. Several crimes in the list relate to "unauthorised access" and "interference" with data and systems. These would be considered "computer dependent" crimes as highlighted above.

The list of crimes also includes so-called "cyber enabled" crimes. One of the main points of the Budapest Convention is to include a list of cyber enabled crimes in order to help harmonise laws across jurisdictions and assist effective cross border co-operation in solving the crimes.

In the case of the Budapest Convention, the cyber enabled crimes listed are fraud, child abuse images and copyright offences. The first additional protocol adopted in 2003 focuses on "criminalisation of acts of a racist and xenophobic nature committed through computer systems".[38]

However, if cyber-enabled crimes are copied and pasted without understanding the cross-border context, and particularly if governments are starting their cyber crime legislation from scratch, the temptation set by the example of the Budapest Convention is to extend this list to include every crime that is committed using a computer and then some.

This is problematic because it draws attention away from the core principle of cyber crime — that of unauthorised access — and can end up being used to sweep in a far wider range of offences that are broadly defined, or criminalise behavior which shouldn't be a crime in the first place.

The drafters of the Budapest Convention intended countries ratifying the convention to translate the provisions into domestic law. It is unclear whether the drafters intended all these crimes to be in one law, or spread across several laws as appropriate. The perhaps unforeseen consequence is that governments mix cyber dependent and cyber enabled crimes into one cyber crime law, which provides the temptation to open up the list of crimes into those which are not actually crimes.

Intrusive investigative powers without accompanying safeguards

It is reasonable to assume that in legislating for new cyber dependent crimes, law enforcement will also need to be authorised to investigate these crimes. The Budapest Convention provides for investigatory powers, which grants law enforcement new powers of search and seizure, including the power to force an ISP (Internet Service Provider) to preserve a citizen's internet usage records or other data, and the power to monitor a citizen's online activities in real time to have access to systems of service providers in order to access people's data to investigate crimes. These are broad surveillance powers, and it may be the first time law enforcement has officially been given these powers.

Many countries' communications surveillance powers are already very intrusive and lacks sufficient safeguards and oversight that protect fundamental rights. Some countries have no communications surveillance legislation at all, but nonetheless carry out surveillance. Therefore, authorising surveillance powers in a cyber crime law can represent a huge leap in a country's surveillance regime because it greatly expands the type of crimes for which surveillance is authorised. If a government has expanded the list of crimes to include not only cyber dependent crimes but also cyber enabled crimes (essentially any crime using a computer) this dramatically expands the scope of authorised surveillance. Where that is not accompanied by procedural safeguards and other human rights protections within the law itself, or via a wider set of safeguards that would apply, then this surreptitiously introduces significantly intrusive surveillance laws, without any safeguards or human rights protections at all.

The Budapest Convention implicitly assumes a level of legislation governing communications surveillance is already in place that contains safeguards outlined in international human rights law, such as adhering to the principles of legality, necessity and proportionality. Therefore, investigative powers to deal specifically with computer dependent crime are an add-on to another legislative framework already in place. But for many non-member States, this will be the first time any surveillance legislation is on the books, and as such, without the accompanying legislation providing safeguards, this creates another area of significant concern. It is of course noted that many Council of Europe member states have inadequate surveillance legislation too! A cyber crime law is not the place to expand a country's surveillance regime and is often used as an excuse to introduce mass surveillance powers.

BOX 13. Charting the Influence of the Budapest Convention in Kenya

In May 2018, the government of Kenya passed the Computer Misuse and Cybercrimes Act. The structure and content is similar to the Budapest Convention, and raises a number of concerns as outlined in this briefing.

Missing the Broader Human Rights Framework of Protection: In the Act there is no reference at all anywhere to protections provided either by Kenya's Constitution or international obligations to protect human rights (privacy, access to information, freedom of expression etc.)

Opening the Door for an Extended List of "Crimes": Part III of the Act includes an overwhelming number of offences jumbled together, featuring a mixture of cyber dependent and cyber enabled crimes, plus the creation of offences that should not be considered crimes under international human rights law: The list includes: Unauthorised access, unauthorised interference, unauthorised interception, unauthorised disclosure of passwords, cyber espionage, false publications, child abuse images, cyber terrorism, wrongful distribution of obscene or intimate images, computer forgery, computer fraud, cyber harassment, publication of false information, cybersquatting, identity theft and impersonation, phishing, interception of electronic messages or money transfers, willful misdirection of electronic messages and fraudulent use of electronic data.

There is no distinction as to what is cyber dependent, what is cyber enabled, and therefore useful for cross border cooperation. In May 2018, the High Court suspended 26 provisions of the Act, relating to offences that threaten freedom of expression, freedom of the media and the right to privacy, such as false publications and publication of false information as well as the new investigative powers below.[39]

Intrusive Investigative Powers without Accompanying Safeguards: Part IV of the Act not only grants new investigative powers, such as real time collection of traffic data and interception of content, but grants them to police officers. This is a huge leap in Kenya's surveillance regime, essentially hidden in a cyber crime law. Under Kenya's existing surveillance legislation, the National Intelligence Services Act 2012 only permits the Director General of the National Intelligence Service (NIS) the ability to intercept an individual's communications subject to prior application to the High Court for a warrant. The Prevention of Terrorism Act 2012, grants police officers above the rank of a Chief Inspector the power to request an interception of communications order from the High Court.

Cross border assistance frameworks in flux

As outlined above, one of the main reasons for the Budapest Convention is to facilitate the issue of cross border assistance in addressing cyber crimes.

As cyber crime is international and knows no borders, it is logical that law enforcement in one country may need to ask law enforcement in another country for assistance in solving cyber crimes. This may involve requesting data from a particular service provider based in one country that will assist law enforcement in another help solve a crime by providing data from, for example, email or social media accounts.

However, the issue of cross border assistance is broader than investigations into cyber crimes. There is currently a global debate underway on cross border access to data to assist in solving crimes. The agreements on how this assistance works in practice are often governed by Mutual Legal Assistance Treaties (MLATs) between countries. Most MLAT's involve the USA, as most of the companies that hold data are based there. The MLAT system is judicially controlled therefore providing safeguards and essentially works, but it has come under criticism for being slow and outdated. In addition, the Microsoft Ireland case highlighted the extraterritorial issues that arise when a warrant is served from a court in one country to access servers in another country.[40] Plus, the standards that govern access to evidence in one country may differ from another, something that bilateral agreements should seek to reconcile.

There are three reforms underway that focus on the USA and Europe and it is currently unclear what the impact of these agreements will be globally and how safeguards will be applied in absence of judicial control.

These three reforms regarding how law enforcement deal with the important issue of cross border cooperation are in the early stages of either implementation, as with the CLOUD Act, or development, as with the e-Evidence initiative and the Second Additional Protocol to the Budapest Convention. It is yet to be seen how these new laws and proposals will be implemented in the US and Europe, let alone the rest of the world, and what challenges civil society will bring. It is also yet to be seen how these three frameworks will complement or contradict each other.

It will be some time before these agreements are finalised and filter to the rest of the world. In the footnotes below we provide links so that readers are aware of the debate.[41]

Key Considerations for Cyber Security Frameworks and Cyber Crime Legislation

Cyber security is hard and cyber crime is a new and evolving issue that many States are grappling with. Therefore, a government would be expected to use a range of approaches that make up a robust framework, one which puts people at the centre and promotes and protects human rights rather than undermine them. Here are some key points for discussion:

- **Start by separating cyber security from cyber crime.** As outlined in this Briefing, they are not the same, or interchangeable. They are distinct and each require their own considerations. Cyber security is about technically securing computer systems, while the core principle of cyber crime is punishing unauthorised access to those computer systems.

- **Don't be tempted to cover everything in one law.** Governments often fail to draw the distinction between cyber security and cyber crime, use the term interchangeably and lump both issues together in one law. As this Briefing has demonstrated, the issues are complex and distinct enough to require safeguards designed to address the unique privacy and security implications of each issue.[42]

- **Be transparent about the process and consult with civil society.** Civil society organisations, academics and independent technical experts are largely frozen out of the conversation when it comes to deciding on cyber security priorities, policies and laws. In many countries, there is little transparency on how decisions regarding cyber security strategies and cyber crime laws are made and by whom. Civil society and technologists rarely have a seat at the decision-making table. This exclusion inevitably leads to an adversarial relationship between governments and civil society, resulting in many initiatives being sent back to the drawing board.[43] Cyber policy and law making is in its infancy and requires the input of different stakeholders. Truly effective security must be done as a collaboration and no one actor can claim to have the solution. This requires trust and efforts to understand different stakeholder perspectives.

Developing a Strong and Rights-Respecting Cyber Security Approach

DO:

- **Prioritise protecting and defending individuals, devices, and networks.** This must form the basis of any cyber security strategy. Good cyber security policies and practices put people and their rights at the centre and seek to strengthen and protect human rights rather than curtail them.

- **Establish a cyber security "framework" rather than one law in isolation.** Cyber security is made up of different, complementary initiatives and approaches. Legislation may be just one of these elements. Many elements of cyber security rely on non-legal mechanisms, such as minimum standards of security, investment in security research, security audits of key industries and public bodies. Government policy in this area can make a real difference in raising standards of security.

- **Identify and prioritise critical infrastructure.** This refers to essential systems whereby their damage or loss would have a significant impact on the functioning of the State and the safety of the people, for example energy (electricity, oil, gas), transport (air, rail, water, road), banking, financial market infrastructures, health, water, digital infrastructure.

- **Establish incident response teams.** These teams of experts are the frontline for when a security incident happens, and mostly deal with compromised devices or services that are enabling cyber attacks. Ideally, they should be independent of government departments.

- **Undertake a proper threat assessment.** A threat assessment considers possible weaknesses, such as outdated infrastructure, that make the country more vulnerable to attack, and helps in decision-making and prioritisation.

- **Adopt and implement a comprehensive data protection law.** Cyber security frameworks must include data protection laws which safeguard against the exploitation of personal data collected by companies and public bodies. Without legal obligations to protect personal data from abuse by companies and public bodies, people will be left vulnerable to situations in which their data is excessively collected, poorly secured and ultimately at risk of being stolen.

DON'T

- **Ramp up offensive powers at the expense of defensive capabilities.** Investing in offensive powers such as monitoring and surveillance equipment instead of defensive capabilities and expertise is the wrong approach to cyber security. This approach leaves the security of individuals, devices and networks at risk, and will not provide security in the long run.

- **Shroud cyber security in secrecy.** A clear, accessible and comprehensive policy and legal framework(s) should be established and debated with public consultation and stakeholder involvement. The public and businesses must have an idea of the real threats they face and contribute to the discussion on how they can protect themselves.

Developing a Strong and Rights-Respecting Cyber Crime Approach

DO:

- **Underpin legislation with human rights protection and safeguards.** Cyber crime law should be consistent with a country's national constitution and in line with international obligations to protect human rights.

- **Narrowly interpret cyber crime.** The core principle of punishing unauthorised access focuses on crimes that can only be committed using a computer or device, known as "cyber dependent crime" e.g. breaking into the computer systems of, for example, a nuclear facility with the intention of shutting it down, "phishing" and DDoS attacks.

- **Establish comprehensive legal frameworks around "cyber enabled crime".** This refers to established crimes committed in a new way using technology, such as fraud or distribution of child abuse images. The standard inclusion of these kind of crimes in cyber crime laws aids cross border co-operation in solving them. However, these crimes should not only appear in a cyber crime law. For example, distributing child abuse images is a crime whether using a computer or not. Therefore, it should be supported by a comprehensive child protection legal framework where the crime can be defined more precisely, and importantly, contextualised in its broader context.

DON'T

- **Expand into criminalising behaviour that isn't a crime.** A cyber crime law should not be an excuse to include an extended list of crimes that ultimately violates international human rights law. Examples of crimes that are not cyber crime include criticising the government on social media and using encrypted messaging services.

- **'Copy and paste' the Budapest Convention into domestic cyber crime law.** The Budapest Convention is underpinned by human rights safeguards that are lost if sections are cherry picked and copied and pasted into domestic law. What is left is legislation that includes very intrusive measures in the absence of these balancing safeguards.

- **Use cyber crime law to establish or expand surveillance legislation.** Surveillance is an intrusive act and interferes with a range of human rights. Therefore, it is essential that surveillance legislation is drafted in line with international human rights law and to ensure any surveillance is legal, necessary and proportionate. A cyber crime law is not the place to legislate for surveillance.

End Notes

1 See more resources from Privacy international on cyber security here: https://privacyinternational.org/topics/cyber-security

2 The Centre for Internet and Society (CIS) Information Security Practices of Aadhaar (or lack thereof): documentation of public availability of Aadhaar Numbers with sensitive personal financial information http://cis-india.org/internet-governance/information-security-practices-of-aadhaar-or-lack-thereof-a-documentation-of-public-availability-of-aadhaar-numbers-with-sensitive-personal-financial-information-1

3 Privacy International and The Foundation for Media Alternatives (FMA), State of Privacy: The Philippines, January 2018 https://www.privacyinternational.org/state-privacy/1009/state-privacy-philippines

4 Dell Cameron, Private Records Of 93.4 Million Mexican Voters Exposed in Data Breach, The Daily Dot, 22 April 2016 http://www.dailydot.com/layer8/amazon-mexican-voting-records/

5 Vladimir Hernandez, Our World: Kidnapped in Mexico, 15 March 2017 http://www.huffingtonpost.com/vladimir-hernandez/our-world-kidnapped-in-mexico_b_9462258.html

6 Dyn, Dyn Analysis Summary of Friday October 21 Attack, 26 October 2016 http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/ ; New York Times, Hackers Used New Weapons to Disrupt Major Websites Across the UK, 21 Oct 2016 https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html?_r=0

7 For a full account of the attack on Ukraine's power grid, see Privacy International (2016) Cyber Security In The Global South: Giving The Tin Man A Heart pp 11-12 https://privacyinternational.org/sites/default/files/2017-12/Cybersecurity_2017.pdf

8 Zimbabwe National ICT Policy (2015) https://www.techzim.co.zw/wp-content/uploads/2015/12/Zimbabwe-Draft-National-ICT-Policy-2015-.pdf

9 Zimbabwe Cybercrime and Cybersecurity Bill (2017) https://t792ae.c2.acecdn.net/wp-content/uploads/2017/08/CYBERCRIME-AND-CYBERSECURITY-BILL2017.pdf

10 Media Institute of Southern Africa (MISA) Policy Brief: Zimbabwe's Draft Cybercrime and Cybersecurity Bill: Trudging Down The Wrong Path http://crm.misa.org/upload/web/Trudging%20Down%20the%20Wrong%20Path-%20Zimbabwe%20Cyber%20crime%20and%20Cyber%20security%20Bill%202017.pdf

11 DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (the "NIS Directive") http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

12 Republic of South Africa, Critical Infrastructure Protection Bill, 15 September 2017 https://www.parliament.gov.za/storage/app/media/Docs/bill/a46ae407-aa2b-481d-af12-0afd97e9d629.pdf

13 Republic of South Africa, National Key Points Act 102 of 1980, https://www.gov.za/documents/national-key-points-act-24-mar-2015-1016

14 Right2Know Campaign, Statement: R2K & SAHA welcome ruling on National Key Points list, 3 December 2014 https://www.r2k.org.za/2014/12/03/statement-r2k-saha-welcome-ruling-on-national-key-points-list/

15 Also known as Computer Emergency Response Team (CERT). CERTs were first established by Carnegie Mellon University in the USA in 1988, and own the trademark to this day.

16 See https://www.first.org/ and slides on how to set up a CSIRT www.first.org/education/trainings

17 European Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 7 February 2013 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN

18 18 European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") September 2017 https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en

19 DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (the "NIS Directive") http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

20 European Commission, 2018 reform of EU data protection rules, May 2018 ; https://privacyinternational.org/feature/2054/why-and-how-gdpr-applies-people-globally ; GDPR infographic https://ec.europa.eu/justice/smedataprotect/index_en.htm

21 Unofficial translation by Thai Netizen Network of the National Cybersecurity Bill (the draft approved by the Cabinet on 6 January 2015) March 2015 https://thainetizen.org/wp-content/uploads/2015/03/cybersecurity-bill-20150106-en.pdf

22 The term “hacking” is difficult to define. Hacking is essentially an attempt to understand a system better than it understands itself, and then nudging it to do what the hacker wants. Hacking is an act or series of acts, which interfere with a system, causing it to act in a manner unintended or unforeseen by the manufacturer, user or owner of that system. System refers both to any combination of hardware and software or a component thereof.

23 Privacy International, Hacking Safeguards and Legal Commentary, January 2018 https://privacyinternational.org/advocacy-briefing/1057/hacking-safeguards-and-legal-commentary
Privacy International, Pay No Attention to That Man Behind the Curtain: Exposing and Challenging Government Hacking For Surveillance, June 2018 https://privacyinternational.org/sites/default/files/2018-06/Pay%20No%20Attention%20to%20That%20Man%20Behind%20the%20Curtain%20-%20Exposing%20and%20Challenging%20Government%20Hacking%20for%20Surveillance.pdf; Accompanying podcast on Soundcloud: https://soundcloud.com/privacyinternational/challenging-government-hacking

24 Privacy International has written extensively about the importance of encryption for privacy and freedom of expression, underpinning the secure functionality of the internet and facilitating global online commerce. See, Privacy International, Securing Safe Spaces Online: Encryption, online anonymity and human rights (2015) https://privacyinternational.org/report/1634/securing-safe-spaces-online-encryption-online-anonymity-and-human-rights
Privacy International, Giving the Tin Man a Heart: Cyber Security in the Global South (2017) https://privacyinternational.org/sites/default/files/2017-12/Cybersecurity_2017.pdf Section 2.6 Attempts to Weaken Encryption pp16-17

25 State of Privacy report for Morocco (updated 2018) https://www.privacyinternational.org/state-privacy/1007/state-privacy-morocco

26 United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Research Paper 1/2018, Encryption and Anonymity follow-up report (June 2018), para 11 https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf

27 Privacy International, Encryption at The Centre Of Mass Arrests: One Year on From Turkey’s Failed Coup, July 2017 https://medium.com/@privacyint/encryption-at-the-centre-of-mass-arrests-one-year-on-from-turkeys-failed-coup-e6ecd0ef77c9

28 Uganda v. Nyakahuma (2013) http://www.ulii.org/ug/judgment/high-court-criminal-division/2013/30-0 The case was dismissed in 2015 due to lack of evidence https://freedomhouse.org/report/freedom-press/2016/uganda

29 Reuters, Thailand jails man for 11 years for royal defamation, cybercrime January 27 2017; https://uk.reuters.com/article/uk-thailand-lese-majeste/thailand-jails-man-for-11-years-for-royal-defamation-cyber-crime-idUKKBN15B0ZF

30 See Section 10a on hate speech in the Prevention of Electronic Crimes Act in Pakistan. http://www.na.gov.pk/uploads/documents/1470910659_707.pdf

31 Ibid

32 SMEX, Egyptian Parliament Passes Cybercrimes Law to Legitimize its Efforts to Curb Free Speech, June 14 2018 https://smex.org/egypt-passes-cybercrimes-law-to-legitimize-its-efforts-to-curb-free-speech/?utm_source=Social+Media+Exchange+%28SMEX%29+Newsletter&utm_campaign=25029d9146-EMAIL_CAMPAIGN_2018_07_03_01_52&utm_medium=email&utm_term=0_de3253d538-25029d9146-77187171

33 Council of Europe, Chart of signatures and ratifications of Treaty 185 Convention on Cybercrime Status as of 01/06/2018 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=to7zo4Qj
Council of Europe, The Convention on Cyber Crime of the Council of Europe, (CETS No. 185), known as The Budapest Convention. https://www.coe.int/en/web/cybercrime/the-budapest-convention

34 Council of Europe, Chart of signatures and ratifications of Treaty 185 Convention on
35 Cybercrime Status as of 01/06/2018 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=to7zo4Qj

36 Council of Europe, Practical Guide on the use of personal data in the police sector: how to protect personal data while combatting crime, 15 February 2018 https://rm.coe.int/practical-guide-use-of-personal-data-in-the-police-sector/1680789a74

37 Articles 2-11

38 Council of Europe, Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, Strasbourg, 28.I.2003 https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680008160f

39 CIPESA, Sections of Kenya's Computer Misuse and Cybercrimes Act 2018 Temporarily Suspended, May 30, 2018 https://cipesa.org/2018/05/sections-of-kenyas-computer-misuse-and-cybercrimes-act-2018-temporarily-suspended/

40 On 18 January 2018, Privacy International, together with 26 human and digital rights organizations and legal scholars, filed an amicus brief to the United States Supreme Court in United States v. Microsoft Corp. https://privacyinternational.org/sites/default/files/2018-03/U.S.%20v.%20Microsoft%20Brief%20FINAL.pdf

41 United States: The Clarifying Lawful Overseas Use of Data ("CLOUD") Act.
Scarlet Kim, Mailyn Fidler, The Weak Link in a Double Act: U.K. Law is Inadequate for Proposed Cross-Border Data Request Deal, Lawfare, 11 July 2017 https://www.lawfareblog.com/weak-link-double-act-uk-law-inadequate-proposed-cross-border-data-request-deal
European Union: e-Evidence Initiative
European Commission, E-evidence - cross-border access to electronic evidence, 2017 https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en
Council of Europe: The Second Additional Protocol to the Budapest Convention
Council of Europe, Cybercrime Convention Committee (T-CY) (DRAFT) Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime https://rm.coe.int/-draft-terms-of-reference-for-the-preparation-of-a-draft-2nd-additiona/168071b794 EDRI, Global Civil Society Letter to the Council of Europe: Cyber crime Negotiations and Transparency, 3 April 2018 https://edri.org/files/letter-cybercrimenegotiations-and-transparency_20180403_EN.pdf

42 In 2014, the African Union adopted The Convention on Cyber Security and Personal Data Protection. It covers cyber security, cyber crime and data protection in one law. It is a huge piece of legislation, and member states have been slow to ratify it, possibly due to its complexity, unfamiliar terminology and lack of discussion of its content. https://ccdcoe.org/sites/default/files/documents/AU-270614-CSConvention.pdf

43 In 2015, a draft encryption policy in India was withdrawn after 24 hours due to public outcry over the requirement for end users to store plaintexts of communications for 90 days. See Yuthika Bhargava, Government To Withdraw Draft Encryption Policy, The Hindu, 28 March 2016 http://www.thehindu.com/news/national/govt-to-withdraw-draft-encryption-policy/article7677348.ece In South Africa, civil society successfully prevented a draft cybercrime law from being passed due to the lack of a public interest defense and perceived criminalisation of journalists and whistleblowers. See Privacy International State of Privacy report, South Africa https://www.privacyinternational.org/state-privacy/1010/state-privacy-south-africa. In Pakistan, civil society organisations campaigned for 18 months to try and force a rethink of the Prevention of Electronic Crimes Bill. See Privacy International, How Not to Draft Legislation: Prevention of Electronic Crimes Bill from Bill to Act https://www.privacyinternational.org/node/1028

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