ELECTRONIC FRONTIER FOUNDATION
Protecting Rights and Promoting Freedom on the Electronic Frontier

November 30, 2015

Advocate Mthunzi Mhaga
Ministry of Justice and Correctional Services
SALU Building
28th Floor, 316 Thabo Sehume Street
Pretoria
South Africa
By email: cybercrimesbill@justice.gov.za

Dear Mr Mhaga,

Cybercrimes and Cybersecurity Bill

The Cybercrimes and Cybersecurity Bill, 2015 (the Bill) will affect users' free expression rights by restricting what an individual is allowed to do with its own computers, devices or electronic communication networks.

Overbroad definition of unlawful access

The bill provides in clause 4 that anyone is guilty of an offense when they "**unlawfully and intentionally access** the whole or any part of (a) data (b) a computer device; (c) a computer network; (d) a database; (e) a critical database; (f) an electronic communications network; or (g) a National Critical Information Infrastructure.

The bill then states in clause 2 that this "**may not be regarded as unlawful if it falls within the written authority** which was granted by the person who has the lawfully authority to consent to such act; And (b) **must be regarded as unlawful if it exceeds the written authority** which was granted by the person who has the lawful authority to consent to such act." (Clause 2)

Mens Rea

The bill as its currently stands may indeed constitute a disproportionate encroachment into users' free expression rights and freedom to innovate.

Clause 2 of the proposed text is **too broad and vague** regarding what constitutes an offense. The proposed Bill should affirmatively protect good faith activities that are need for security testing even if the security researcher **does not have a "written authority to**

access the system granted by the person who has the lawfully authority to consent to such act" (clause 2 (2) (a) (b)). It's very important that criminal law be precise on what constitute both unlawful and **criminal malicious intent** *(mens rea)*.

As an initial matter, we suggest clarifying Clause 2. First and foremost, the perpetrator must commit the offense with malicious criminal intent, for example, an intent to defraud and not just any intent to commit a general act. This is vitally important since some of those acts are usually carried out by legitimate security researchers and academics doing valid security work.

Unlawful Offense (Clause 2) and Unlawful Access (Clause 4)

The text of the bill must be precise on what constitutes lawful activity (Clause 2). Lawful activity should not be limited only to those who have the written authority to access the whole or any part of data; computer device; computer network; database, critical database (Clause 2: "**may not be regarded as unlawful if it falls within the written authority** which was granted by the person who has the lawfully authority to consent to such act); This definition left out many legitimate and security research that does not constitute criminal offenses and are not carry out without the written authorization. Moreover, implied authorization must be permitted too.

For example a woman who signed up for a social media account using a fictitious name and age obtained "intentional access" to her own social media account. However, that intentional access is not necessarily malicious. Moreover, her conduct can be interpreted as an unlawful access since she use a pseudonymous, which is forbidden expressly in the social media term of service. As the bill is currently written, her conduct can be interpreted as a criminal offense because she violated the social media's terms of service by accessing unlawfully and internationally an electronic communication network.

The bill must be written in a way that **violations of Term of Services are not computer crimes.** This is a real problem because the public would not have adequate notice about what behavior is illegal, and the government would be able to cherry-pick cases to prosecute at its whim.

This wording approach also threatens to put the immense coercive power of criminal law in the hands of those **who draft contracts and term of services**. This means that private parties, rather than lawmakers, would be in a position to determine what conduct is criminal, simply by prohibiting it in an agreement. That is particularly troubling for website terms of use, which are typically arbitrary and confusing agreements of adhesion that users may "agree" to without ever having read. Criminalizing breaches of website terms of use could turn millions of Internet users into criminals for typical, everyday activity, simply because the drafter of the contracts decides that it will be so.

The language of Clause 2 and Clause 4 also restrict what an individual is allowed to do with its own computers, devices or electronic communication systems by criminalizing

violation of terms of services. For example, an operator of a ticket reselling service, who purchased tickets through a Ticket service website, is using an automated means to buy the tickets. According to the vague wording of the bill, the reseller might be violating the websites terms of service, and hence unlawfully and intentionally accessing a website although there is no criminal malicious intent. That provision would harm innovators and the development of the market economy in South Africa.

In a similar line of cases, we insist the current language of clause 2 and 4 should be precise to not allow any possible interpretation that **violations of corporate policies** are computer crimes per se. For example, if a former employee of a company convinced a current employees to access the company's proprietary database and pass along information that he could use for competitive advantage. In this scenario, the man's accomplices had authority to access the database for some purposes, it might exceeded that authority when they accessed it for a purpose that violated corporate policy, which said that employees were only allowed to access the database to further the company's business interests.

While the perpetrator commit the act with malicious intent, what is seriously dangerous is to to grant employers the legal power to make certain behavior criminal just by stating in a written policy what an employee is not allowed to do. Criminal behaviors need to be in criminal law, and not be dictated by private parties via contracts. For example, a worker could be sued or prosecuted for reading personal email or checking the score of a game if her employer's policy says that company computers may be used only for work. It is our strong belief that contract law is already sufficient and what is at core an employment dispute should not be made a matter of criminal law.

Promote Competition and Spur the Market Economy

The wording of the bill shouldn't allow companies to use the imprecise language of Clause 2 and 4 to stymie competitors who create new tools that would spur the economic market and give consumers more choice. For example, if a service allowed users to aggregate their information from a variety of social networking sites and view it in a single browser. Facebook, in the United States in a case against a website Power.com (Power), argued that Power violated the computer crime laws because it allowed users to access Facebook by automated means, which violated Facebook's Terms of Use. Facebook has also gone a step further, claiming that Power unlawfully designed its service to use multiple IP addresses to access Facebook's servers with the intention of defeating IP blocks. In other words, the mere creation of a tool that could be used to circumvent a technical barrier, even when a technical barrier doesn't exist, creates liability under the proposed bill. South Africans should encourage more innovation and spur their tech market.

The legitimate need to access a system without written authorization

In our view, accessing the whole or any part of data, computer device, computer network,

database, critical database without ***malicious mens rea (for example, intent to defraud***) should not be punishable as criminal offenses. Examining computers without the explicit permission of the owner is necessary for a vast amount of useful research, which might never be done if permission were required.

The proposed text should affirmatively protect those activities as lawful activities, with a particular emphasis on protecting access for purposes of security testing even if the security researcher **does not have a "written authority to access the system** granted by the person who has the lawfully authority to consent to such act" (clause 2 (2) (a) (b)).

Why we are so concerned?

The criminalization of demonstrating vulnerabilities gives vendors of flawed products the ability to deny the existence of flaws, even months or years after those flaws have been discovered, or to wrongly suggest that the vulnerabilities are merely theoretical. This puts the personal information of many South Africans at risk. We need to fix this.

The provision also provides vendors with enhanced legal leverage to frighten researchers into silence. This harms the public by allowing insecure and broken technology to remain unpatched and be used, sometimes, by millions of persons.

The wording of the bill must not criminalize the legitimate activities and use of tools needed for independent security research, academic study, and other good-faith activities that serve the public interest and ultimately make the public more safe.

No Criminalization of Security Tools

We believe that clause 6 regarding "unlawful acts in respect of software or hardware tools" must be deleted completely. The current draft will severely curtail commercial "penetration testing" firms that are critical for the modern economy, academic scholarship, legitimate security research, and other activities that benefit society.

The bill must not criminalize the creation, possession and distribution of tools that are fundamentally designed for the purpose of carrying out an attack. These tools also have legitimate, socially desirable uses, such as identifying a practical vulnerability. An example of software written essentially to carry out an attack or demonstrate a practical vulnerability is password-cracking programs such as Crack and John the Ripper. These tools are often used by system administrators to determine when users have chosen an insecure password that need to be changed. Academics and other researchers—who are studying password security—may also use them. Far from having malicious criminal intent, these researchers use password-cracking programs to investigate how passwords might be made more secure.[1]

1 See , e.g. , Robert Morris and Ken Thompson, Password Security: a Case History, Commun. ACM, 22(11):594 – 597, 1979; Joseph A. Cazier and B. Dawn Medlin, Password Sec urity: An Empirical

Moreover, nearly all of those technologies can be used for good and bad purposes. Some of those purposes, such as access to a computer system-without malicious criminal intent (Clause 4), are legitimate activities as explained above. Security tools are usually designed for the purposes of penetration (access to a computer system), so according to the Bill, all tools will be **intentionally** manufacture, assemble, obtain, sell, purchases, makes available or advertises any software or hardware tool for the purposes of contravening the provisions of the bill. This, in turn, will make many security tools, regardless of its malicious intentional use, unlawful.

It is tempting to believe that a definition could be crafted that would capture the "bad" tools, while still permitting the manufacture, sale, and use of the "good" tools. Unfortunately, such a definitional solution is impossible. The very same tools are at issue and no effort to ban "bad" tools while leaving the "good" ones legal can be successful.

A classic example is a packet sniffer like Wireshark, which could be used both for illegal wiretapping and for helping network administrators debug network configuration problems and identifying software bugs. The development and use of these tools are necessary for research and testing, including for "defensive" security efforts to determine the feasibility of attacks on a system.

As another example, a bank may hire a security consultancy to use a product like Metasploit to probe the bank's systems and report on vulnerabilities that need to be fixed. Since these tests are carried out with the bank's authorization, they are not a violation of the law, but they require the use of tools and techniques absolutely identical and indistinguishable from those used by malicious attackers. Penetration testing —accessing a company's network with permission to detect security holes—is a critical security business, and security researchers will not be able to perform their jobs if the distribution of network utilities is criminalized.

Hate Speech

The proposed Cybercrimes and Cybersecurity Bill, in clause 17, also unfairly imposes

Investigation into E-Commerce Passwords and Their Crack Times, Information Systems Security, 15(6):45 – 55, 2006; David C. Feldmeier and Philip R. Karn, UNIX Password Security-Ten Years Later, In CRYPTO '89: Proceedings of the 9th Annu al International Cryptology Conference on Advances in Cryptology, pages 44 – 63, London, UK, 1990; Daniel Klein, 'Foiling the Cracker': A Survey of, and Improvements to, Password Security, In Proceedings of the 2nd USENIX Security Workshop, pages 5 – 14, 1990; Arvind Narayanan and Vitaly Shmatikov, Fast Dictionary Attacks on Passwords Using Time-Space Tradeoff, In CCS '05: Proceedings of the 12th ACM conference on Computer and communications security, pages 364 – 372, New York, NY, USA, 2005; Philippe Oechslin, Making a Faster Cryptanalytic Time-Memory Trade-Off, Advances in Cryptology-CRYPTO 2003, 2003; Matt Weir et al., Password Cracking Using Probabilistic Context-Free Grammars, In SP '09: Proceedings of the 2009 30th IEEE Symposium on Security and Privacy, p ages 391 – 405, Washington, DC, USA, 2009; Aleksandar Kasabov and Jochem van Kerkwijk, Distributed GPU Password Cracking, System and Network Engineering research group, Informatics Institute, Faculty of Science, University of Amsterdam, 2011

harsher penalties for the dissemination of hate speech when it occurs online.

South Africa's Promotion of Equality and Prevention of Unfair Discrimination Act (2000) already excludes hate speech from free expression, prohibiting the publication, communication, or other dissemination of speech that could be reasonably construed to demonstrate a clear intention to 1) be hurtful 2) be harmful or to incite harm or 3) promote or propagate hatred.

According to the 2000 Act, cases involving hate speech are to be referred to the equality court, which is authorized to hold an inquiry and make an "appropriate order." The Act lists a number of possible orders which the court could make, ranging from an "unconditional apology" to payment of damages.

South African common law also provides for penalties for "*crimen injuria*," or "unlawfully and intentionally impairing the dignity or privacy of another person."

The proposed Cybercrimes and Cybersecurity Bill would automatically impose criminal penalties (of a fine and/or up to two years imprisonment) for the unlawful and intentional distribution of any “data message which advocates, promotes or incites hate, discrimination or violence." This treatment of online speech as inherently separate from speech which takes place offline.

The imposition of harsher penalties for online speech has become common as States attempt to grapple with the expansion of the public sphere into cyberspace. In the aftermath of the horrific attacks on Charlie Hebdo this past January, France proposed an anti-terrorism bill that would provide for harsher penalties for the glorification of terrorism if it took place online. Similarly, the rationale that online speech is inherently more dangerous has been used to push for laws restricting anonymous online speech in a range of countries.

We must be wary of any attempt to impose additional penalties on speech due purely to the medium through which it takes place.

Copyright Enforcement

The Bill also provides (in clause 20) for the criminalization of most online acts of copyright infringement. We say this because the proscribed acts of selling, offering for download, distributing or otherwise making available a copyright work online covers essentially anything that a user could possibly do with a copyright work online, other than up or downloading it for their own personal use.

The offense requires that the user knows that the work is subject to copyright, and that they don't have the copyright owner's authority to put it online—however there so many instances in which copyright owners tolerate their works being published online that this could criminalize an entire generation of fans and remixers.

The clause does impose a further condition: that the offender knows that putting the work online "will be prejudicial to the owner of the copyright." But how is "prejudice" measured? Copyright lobbyists often claim that every time a work is downloaded without authorization, the owner loses a sale (a claim at which economists scoff).[2] However, are users expected to believe these exaggerated claims? Or, conversely, if the user doesn't believe that the copyright owner suffered any material prejudice, would a court accept that at face value? The Bill provides no guidance.

This is an unwarranted extension of criminal liability for a broad range of non-commercial infringements, that goes far beyond international norms. Criminal penalties for copyright infringement have traditionally limited these to large scale, for-profit infringement, such as the production of pirated CDs or DVDs. Some recent instruments (such as the Trans-Pacific Partnership) stretches this by including an elastic definition of "commercial scale" infringement that encompasses non-profit activities, but even those still have to be undertaken on a large scale. The Bill does not require even this. Potentially uploading a single file is criminalized, so long as the user can be found to have known that this would prejudice the copyright owner.

This provision of the Bill is to overreaching and vague, and should be deleted. The right place for copyright enforcement measures is not in a cybercrime law, it is in the copyright law—which is already under review in South Africa. And the copyright law already contains comprehensive criminal enforcement measures, to which this latest proposal would add nothing—other than newly criminalizing individual users for isolated and small-scale infringements.

Conclusion

The Cybercrimes and Cybersecurity Bill creates several new offenses that are both over-broad, and vaguely defined. If passed in its present form, it will criminalize innocent activities of ordinary users, will chill speech, and will inhibit innovation. We recommend that the Bill be significantly revised in the respects that we have suggested above before it is presented to Parliament.

Yours faithfully,

ELECTRONIC FRONTIER FOUNDATION
Katitza Rodriguez, International Rights Director
Jillian York, Director for International Freedom of Expression
Jeremy Malcolm, Senior Global Policy Analyst

2 See Schruers, Matt. Not Buying the Lost Sale “Baloney” (2013), available at http://www.project-disco.org/intellectual-property/080113not-buying-the-lost-sale-baloney/.