Cybercrimes and Cybersecurity Bill

Consultation Response from Mozilla

Dear Mr Robbertse,

Thank you for the opportunity to comment on the draft Cybercrimes and Cybersecurity Bill.

Mozilla is a non-profit Foundation which produces the Firefox web browser and Firefox OS mobile ecosystem, together adopted by half a billion individual Internet users around the world. Mozilla also educates and empowers Internet users to be the Web's makers, not just its consumers. To accomplish this, Mozilla functions as a global community of technologists, thinkers, and builders, including thousands of contributors and developers, and millions of users in South Africa, who work together to keep the Internet alive and accessible. And, as in this case, we also engage with policymakers to help shape legislation to promote and protect the opportunities the Internet provides to users everywhere.

As written today, this legislation would significantly and substantially harm South Africa's citizens and businesses by introducing penalties for commonplace and noncriminal actions which use computers and the Internet. While well-intentioned, this draft has fundamentally flawed construction, and the Government of South Africa should use its learnings from this consultation process to start over with new text, readdressing this agenda with a better grounding in the technical underpinnings of the Internet.

The Cybercrimes and Cybersecurity Bill appears intended to prevent or punish malicious behaviours, including the commission of fraud, deliberate damage or forced access to systems, or the interception or modification of data by a third party not intended by sender or recipient to be included in the data exchange. We recognize the importance of protecting Internet users and businesses from harm arising from such actions. But the approach in this bill will itself harm South Africa's Internet economy and society, not help them.

The draft bill reflects the following major structural problems:

1. Overbroad definitions create unworkable scale.
2. Vague qualifiers cannot resolve issues with overbroad definitions.
3. Computer usage appears presumptively wrong.
4. Careful policy balances are overturned.

In an attempt to be comprehensive in its coverage, the bill can readily be interpreted to render almost any use of a computer or the Internet illegal. The common qualifiers "unlawful" and "intentional" fail to limit this overbreadth, in part because these qualifications are considered only in the Offences chapter rather than in the Definitions chapter of the bill. Historically, in many other countries and contexts, well-intentioned but overbroad legislation addressing similar cybersecurity and cybercrime topics has been used in ways far outside

the initial intended scope. Failing to learn from these lessons of the past risks significant harm to South Africa's Internet future.

If such a broad swath of actions - seemingly anything involving a computer or the Internet - come to be of questionable legality, computer use by South Africans and related investment across South Africa is at risk, both practically and as a result of chilling effects, with significant resulting economic impact. This bill has the potential to significantly burden the use of technology by the very groups that could benefit the most from it. Overbroad laws lead to wide prosecutorial discretion, which itself runs the risk of enabling social and economic discrimination.

Please find in the attached annex more details on our concerns about definitional breadth and overcriminalization of common online activities. We urge the National Assembly to reconsider the entire text and approach of the bill in collaboration with technical experts from academia, industry and civil society, in order to better address the technical realities of the digital economy and the rights of South Africans. Mozilla of course stands ready to assist in any way we can.

Yours sincerely,

Gervase Markham
Policy Engineer, Mozilla
gerv@mozilla.org

Chris Riley
Head of Public Policy, Mozilla
mchris@mozilla.com

November 30th, 2015

Annex: Structural Analysis of Draft Bill

1. Overbroad definitions create unworkable scale

Key definitions in the draft bill are extremely broad, leading to almost any action using a computer or the Internet to be covered as a crime. Presumably, the primary target scope of a cybercrime bill would be exceptional and harmful actions, rather than commonplace, ordinary behavior. However, many definitions in this draft are fundamentally overbroad. The definitions around online actors and their behaviours are far more expansive than necessary to target malicious acts and actors, and this overbreadth creates a chilling effect that would extend to normal, economically and societally beneficial computer use. For example:

- **General users are not Electronic Communications Service Providers.** The draft bill defines Electronic Communications Service Providers in section 1[1] in such a broad way that it covers any South African who has installed a public wireless access point, anyone involved in a community mesh network, anyone running peer-to-peer data sharing software[2] and almost anyone running a network server. It would also cover libraries, Internet cafes, and hotels which provided WiFi.

  In addition, any person who transmits, receives, processes or stores the data of "any other person" would also be defined as an ECSP. This definition would cover any online interaction with another person or entity, including visiting a website, saving a website's content to read later, or exchanging email with a friend. Therefore, under this draft bill everyone who accesses information or services via the Internet is an ECSP.

---

[1] Section 1:

> *"electronic communications service provider" means any—*
> *(a) person who provides an electronic communications service under and in accordance with an electronic communications service licence issued to such person under Chapter 3 of the Electronic Communications Act, 2005 (Act No. 36 of 2005), or who is deemed to be licensed or exempted from being licensed as such in terms of the Electronic Communications Act, 2005;*
> *(b) 'financial institution' as defined in section 1 of the Financial Services Board Act, 1990 (Act No. 97 of 1990); or*
> *(c) person or entity who or which transmits, receives, processes or stores data—*
> *(i) on behalf of the person contemplated in paragraph (a) or (b) or the clients of such a person; or*
> *(ii) of any other person;*

Under clause (a), an ECSP includes anyone who provides an electronic communications service. Such a service is defined in the Electronic Communications Act, 2005 as:

> *any service provided to the public, sections of the public, the State, or the subscribers to such service, which consists wholly or mainly of the conveyance by any means of electronic communications over an electronic communications network, but excludes broadcasting services;*

[2] Peer-to-peer networks have many legal applications where users wish to distribute large volumes of data that would otherwise be cost-prohibitive to serve.

- **Not all infrastructure is critical.** Definitions in section 1[3] allow broad designation of National Critical Information Infrastructure (NCII). The definition includes any government building with a computer or network system, and any network belonging to any body which has been given any responsibility in South African law (a list which it would be almost impossible even to compile). If everything is critical, then in practice, nothing is.

  Most offences in the bill are worded such that the maximum sentence is doubled if NCII is affected. The over-broad definition of NCII means that penalties which are intended to be exceptional will instead be commonplace, further instilling fear into the ordinary user of technology and making them nervous of interacting with government computer systems.

- **Malware is malicious and must be defined as such.** Malware as a phrase is a portmanteau of “malicious software,” meaning software that is both harmful to, and acting outside of the expectations of, the user. Harm is a critical part of the definition. Malware, as defined in the draft bill in section 9.4[4], would encompass any software at all - since software, by nature, “modifies” - clause (b) - data and databases on a computer. In addition, many common and welcome computer functions would fall under other parts of this definition. Content blockers, for example, “interfere with the ordinary functioning of” web browsers in order to stop them downloading certain content - albeit at a user’s request. Secure deletion tools clearly “impair” or “compromise the availability of” data - that’s the intention, and it is necessary in order to securely erase data once it is no longer needed. A security monitoring program on

---

[3] Section 1:

"National Critical Information Infrastructure" means means any data, computer data storage medium, computer device, database, computer network, electronic communications network, electronic communications infrastructure or any part thereof or any building, structure, facility, system or equipment associated therewith or part or portion thereof or incidental thereto—
(a) which is specifically declared a National Critical Information Infrastructure in terms of section 58(2) of this Act; or
(b) which, for purposes of Chapters 2 and 4 of this Act, are in possession of or under the control of—
(i) any department of State or administration in the national, provincial or local sphere of government; and
(ii) any other functionary or institution exercising a public power or performing a public function in terms of any legislation,
irrespective whether or not it is declared a National Critical Information Infrastructure as contemplated in paragraph (a);

[4] Section 9.4:

"malware" means any data, electronic, mechanical or other instrument, device, equipment, or apparatus that is designed specifically to—
(a) create a vulnerability in respect of;
(b) modify or impair;
(c) compromise the confidentiality, integrity or availability of; or
(d) interfere with the ordinary functioning or usage of,
data, a computer device, a computer network, a database, a critical database, an electronic communications network, or a National Critical Information Infrastructure.

a network may “interfere with the ordinary functioning of” another network device or program by shutting it down if it suspects that it has been exploited or misused.

2. Vague qualifiers cannot resolve issues with overbroad definitions

The draft bill appears to attempt to qualify its overbroad definitions, but the vague qualifiers used for this purpose do not appreciably narrow the broad scope of entities and actions that would newly be defined as criminal.

For example, Section 7, on “unlawful interference with data”, potentially criminalizes everyone who uses any digital device, from a smartphone to a microwave, simply because they are using a computer, which will inherently “interfere with” - a term which, according to 7.3 (a) includes “altering” - data. All computers alter data. Other provisions, such as “interception” of data in section 5, have similarly overbroad coverage.

These and many other sections in this bill put great reliance on the phrase “unlawfully and intentionally” to try and distinguish everyday activities using a computer from wrongdoing. However, the bill’s intent is itself to define what is unlawful. Defining it as “that done unlawfully” is circular and therefore meaningless.

The net result is that these qualifiers offer no surety to Internet users, and cannot help address the breadth of scope, or the practical or chilling effects imposed by it.

3. Computer usage and even possession seem presumptively wrong

Several clauses of the legislation take an existing act which is already a crime, and create additional offences simply because a computer is used in committing that crime. A computer, or the Internet, is merely a tool, and attaching heightened criminality to its use is unwarranted. Should there be areas of existing criminal law that somehow are not applicable if the crime is committed using a computer, these laws should be modified, rather than including a provision that specifically targets computer usage for heightened attention and penalty. As the consultation document rightly notes:

> *“it is hard to imagine a cybercrime or perhaps any crime, that does not involve electronic evidence linked with internet protocol connectivity."*

Identifying computer usage in this way will further heighten the practical and chilling effects this draft bill imposes on ordinary use of technology by South African Internet users, even if their actions are not in any way harmful.

In other provisions, this draft bill goes so far as to penalize the mere possession of software or data. Sections 3 (personal information and financial information), 6 (software and hardware tools), 9 (malware), and 10 (passwords) criminalize the possession of certain software or data if the possessor is “unable to give a satisfactory exculpatory account of such possession.” Among other problems with this approach and harmful chilling effects it will lead to, it also does not reflect normal user awareness of technology. Computers are

complex objects whose ways of operation are not understood by many users. They can be compromised or invaded by remote attackers and the contents of the system changed without the knowledge of the owner. Possession of a particular item of data or software on a user's computer cannot be taken as incontrovertible evidence that they placed it there.

4. Careful policy balances are overturned

In addition to hampering ordinary use of computers and the Internet, some provisions of this bill would seem to overturn, or at least drastically modify, existing policy balances. For example, Section 17, "Prohibition on dissemination of data message which advocates, promotes or incites hate, discrimination or violence" is in tension, at minimum, with Section 16 of the Constitution of the Republic of South Africa grants the right to freedom of expression, including the "freedom to receive or impart information or ideas." This draft bill takes the approach of addressing hate speech where it occurs using technology and the Internet separately (including using a significantly broader definition of hate speech), rather than approaching it through the existing policy and Constitutional frameworks.

As another example, Section 20, "Infringement of copyright", seems to effectively redefine copyright infringement. Copyright law has developed over many years to include a number of exceptions and limitations which are vital for free speech and normal social discourse - for example, allowance of use for parody or quotation. Rather than preserving these necessary exceptions, the bill says that any action which "will be prejudicial to the owner of the copyright" is an offence under section 20, even if that act would not be copyright infringement under South Africa's existing copyright law.