

October 2018

# The Ethiopian Cybercrime Law and Human Rights



Dawit Bekele  
Director, African Regional Bureau  
[bekele@isoc.org](mailto:bekele@isoc.org)

# Background

- In 1991, TPLF/EPRDF toppled the DERG regime and took power
- In 1994: new Constitution
- For the last 27 years, EPRDF controls the legislature and executive
- Today, 100% of all members of parliament are from EPRDF and affiliates
- In 2005, an almost democratic election, until ...
- The then PM stopped the counting of ballots and declared victory
- After that, the parliament enacted a number of repressive laws:
  - The Media law (2008)
  - The Anti-Terrorism proclamation (2009)
  - The Charities and Societies proclamation (2009)
  - The Computer Crime proclamation (2016)



Meles Zenawi – Ethiopian PM 1991-2012

# Background ...

- By 2015, thousands of people are in prison using those laws
- The country revolted, triggering two consecutive state of emergencies
- Realizing that the country is hanging on a cliff PM resigned in Feb 2018
- Dr Abiy Ahmed was selected as PM by EPRDF
- The New PM
  - Acknowledged that the government has been using the law against its own people
  - Released thousands of political prisoners
  - Promised to reform repressive laws
  - This presentation is on the aspect of the cybercrime law that we believe need to be amended



Dr. Abiy Ahmed – Ethiopian PM since April 2018

# Problematic issues of the cybercrime law

- The law has many clauses that can help protect citizens against cybercrime
- However, it also has many provision that are in contravention of:
  - The constitution of FDRE
  - The Universal Declaration of Human Rights
  - The International Covenant on Civil and Political Rights
  - The African Declaration on Internet Rights and Freedoms
  - The African Charter on Human and Peoples Rights
  - Declaration of Principles of Freedom of Expression

**የኢትዮጵያ ፌዴራላዊ ዲሞክራሲያዊ ሪፐብሊክ**  
**ፌዴራል ነጋሪት ጋዜጣ**  
**FEDERAL NEGARIT GAZETTE**  
**OF THE FEDERAL DEMOCRATIC REPUBLIC OF ETHIOPIA**

|   |  |   |
|---|--|---|
| <p>ገጽ ፱፻፶፰ ቁጥር ፱፻፶፰<br/>                 አዲስ አበባ ሰኔ ፳፯ ቀን ፪፻፳፮ ዓ.ም</p>            | <p>በኢትዮጵያ ፌዴራላዊ ዲሞክራሲያዊ ሪፐብሊክ<br/>                 የሕዝብ ተወካዮች ምክር ቤት ጠባቂነት የወጣ</p>   | <p>22<sup>nd</sup> Year No. 83<br/>                 ADDIS ABABA 7<sup>th</sup> July, 2016</p> |
| <p><b>አዋጅ ቁጥር ፱፻፶፰/ ፪፻፳፮</b><br/> <b>የኮምፒዩተር ወንጀል አዋጅ.....ገጽ ፱፻፶፰</b></p>         | <p>PROCLAMATION No. 958/2016<br/>                 Computer Crime Proclamation .....Page 9104</p>   |   |
| <b>ግዑጫ</b>  |  |   |
| <p><b>አዋጅ ቁጥር ፱፻፶፰/ ፪፻፳፮</b><br/> <b>የኮምፒዩተር ወንጀልን ለመደንገግ የወጣ አዋጅ</b></p>         | <p><b>CONTENTS</b><br/>                 PROCLAMATION No.958/2016<br/> <b>A PROCLAMATION TO PROVIDE FOR THE<br/>                 COMPUTER CRIME</b></p> |   |
| <p>የኢንፎርሜሽንና የኮሙኒኬሽን ቴክኖሎጂ ለሃገሪቱ ኢኮኖሚያዊ፣ ማህበራዊና ፖለቲካዊ እድገት ቁልፍ ሚና የሚጫወት በመሆኑ፤</p> | <p>WHEREAS, information and communication technology plays a vital role in the economic, social and political development of the country;</p>          |   |
| <p>የኢንፎርሜሽንና የኮሙኒኬሽን ቴክኖሎጂ አጠቃቀም ተገቢ ጥንቃቄና ጥበቃ ካልተደረገለት</p>                       | <p>WHEREAS, unless appropriate protection and security measures are taken, the utilization of</p>  |   |



# Some problematic provisions

- Liability of Intermediaries
  - The 'duty to report' obligation (Art 27) requires communication service providers to report to Information Network Security Agency (INSA) and the Police when they become aware of the commission of cybercrimes or circulation of illegal content on their computer systems.
- Problem
  - The term "knowledge" is unclear in legal terms
  - This might push service providers to
    - Monitor content to avoid penalties
    - Over-block content to avoid risks
- Best practice
  - No monitoring required
  - Clear provision on removing content when informed



# Some problematic provisions ...

- Access to computer by investigators
  - Article 32 requires a warrant for investigators to access a computer
- Problem
  - The Article extends the warrant to all computers connected to that computer
  - This erodes individual rights of people whose computer systems would be accessed without specific warrant

## Best practice

- Warrant should be specific and targeted at a single computer system





## Some problematic provisions ...

- Interception and surveillance of communication
  - Article 25 says the the Attorney General may give permission to the investigatory organ to conduct interception or surveillance without court warrant where there are reasonable grounds and urgent cases ...
  - The Attorney General shall present the reasons for interception or surveillance without court warrant ...to the President of the Federal High Court within 48 hours,
- Problem
  - Why not get a post-facto authorization from the court to insure independence of the judiciary

### Best practice

- The court to provide the post-facto authorization



## Some problematic provisions ...

- Retention of communication data
  - Article 24:
    - In English: One year retention
    - In Amharic: ቢያንስ ለአንድ ዓመት ይዞ ማቆየት ይኖርበታል
- Problem
  - Service provider can keep any data for indefinite amount of time

### Best practice

- The provision should more focused, requiring a relationship between the data and a threat to public safety
- Include sufficient limitations and safeguards





# Conclusion

- Cybercrime laws should be enacted by respecting the fundamental human rights of citizens
- The Ethiopian experience shows that using laws to criminalize law abiding citizens for political purpose is counter effective in the long term
- Cybercrime laws should not be used to curtail freedom of speech
- Cybercrime laws should be drafted in a truly multistakeholder manner by creating consensus between the various stakeholders



**Fitsum Arega**   
@fitsumaregaa

Following 

Freedom of expression is a foundational right that other rights depend on. #Ethiopia has opened access to 264 blocked websites/bloggers/ ESAT and OMN. A free flow of information is essential for engaged & responsible citizenry. Only a free market of ideas will lead to the truth.

2:40 AM - 22 Jun 2018



# Thank you.

Firstname Lastname

Job Title

[surname@isoc.org](mailto:surname@isoc.org)

Visit us at  
[www.internetsociety.org](http://www.internetsociety.org)  
Follow us  
[@internetsociety](https://twitter.com/internetsociety)

Galerie Jean-Malbuisson 15,  
CH-1204 Geneva,  
Switzerland.  
+41 22 807 1444

1775 Wiehle Avenue,  
Suite 201, Reston, VA  
20190-5108 USA.  
+1 703 439 2120



# Get involved.

There are many ways to support the Internet. Find out today how you can make an impact.

Visit us at  
[www.internetsociety.org](http://www.internetsociety.org)  
Follow us  
@internetsociety

Galerie Jean-Malbuisson 15,  
CH-1204 Geneva,  
Switzerland.  
+41 22 807 1444

1775 Wiehle Avenue,  
Suite 201, Reston, VA  
20190-5108 USA.  
+1 703 439 2120

