29 September 2021

Deputy Prime Minister and Minister of Public Administration, Public Enterprises, Telecommunication and the Postal Services Mrs. Petra De Sutter

Deputy Prime Minister and Minister of Justice and the North Sea Mr. Vincent Van Quickenborne,

Minister of Defense, Mrs. Ludivine Dedonder

Dear Ministers De Sutter, Van Quickenborne and Dedonder,

End-to-end encryption keeps Belgium safe.

Encryption protects everyday activities, like handling bank accounts online, securing confidential data like salary slips or tax information, and communicating with your friends and family. End-to-end encryption also protects vulnerable communities and professions where private communications are essential, such as for journalists, lawyers, and medical professionals.

The Belgian government is considering new legislation, the most dangerous being considered among European Union Member States, that would undermine the security and privacy provided by end-to-end encryption.

The *Draft law on the collection and storage of identification, traffic and location data in the electronic communications sector and their access by the authorities*,[1] or "the Data Retention Legislation," would require operators of encrypted systems to enable law enforcement to be able to access on request content produced by specific users after a specified date in the future. That is, they would have to be able to "turn off" encryption for specific users. There is no way to simply "turn off" encryption; providers would need to create a new delivery system and send targeted users into that separate delivery system. Not only would this require significant technical changes, but it would thereby break the promises of confidentiality and privacy of end-to-end encrypted communications services.

Far from making Belgians safer, these requirements would undermine the use of end-to-end encryption in Belgium and, as the Belgian Data Protection Authority wrote in its opinion against the Data Retention Legislation, would force companies to create a "de facto backdoor."[2] The consensus among cybersecurity experts is clear: there is no way to provide third party access to end-to-end encrypted communications without also creating encryption backdoors and vulnerabilities that can be exploited by anyone that finds them.[3] In other words, there is no way for only law enforcement to have access to backdoors, without risking bad actors from gaining access to the same. Creating encryption backdoors weakens the

[1] https://ibpt.be/index.php/operateurs/publication/annexe-1-dispositif
[2] https://www.autoriteprotectiondonnees.be/publications/avis-n-108-2021.pdf
[3] https://academic.oup.com/cybersecurity/article/1/1/69/2367066

security of the whole system and puts all its users at risk.[4] Undermining encryption by introducing backdoors to encrypted communications would leave Belgium exposed to attacks, including its journalists, doctors, lawyers, public sector employees, and other citizens, as well as businesses and institutions, including governments.

Beyond introducing backdoors into existing end-to-end encrypted systems, the Data Retention Legislation would also discourage companies from offering new end-to-end encrypted products. As seen in other countries that have passed similar legislation,[5] the legislation will have a negative impact on trust in Belgian technology companies and damage their ability to compete in the international and European markets. Further, the legislation also threatens to have a wider impact on the European Digital Single Market, as companies in other Member States may be forced to consider these new requirements if they want to offer their products in the Belgian market.

If the Data Retention Legislation is supposed to make Belgians safer, it cannot do so by undermining the strong protections we all rely on to live our lives; end-to-end encryption should not be threatened or undermined by this legislation.

Signatories*

Access Now
Adriaan Peeters
Africa Media and Information Technology Initiative (AfriMITI)
Alexandre Dulaunoy, Security Researcher and Lead of an Incident Response Team, CIRCL.lu
An Van Wesemael
AP2SI - Associação Portuguesa para a Promoção da Segurança da Informação
Bart Coppens, Professor, Ghent University
Bart Preneel, Prod. dr. ir., University of Leuven
Big Brother Watch
Blacknight Internet Solutions Ltd
Cédric Peeters, Vrije Universiteit Brussel (VUB)
Centre for Democracy and Technology
Citizen D/Državljan D
Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
ContactOffice
Cranium
Cybersecurity Advisors Network (CyAN)
Dieter Houthooft, IT Generators BV
Digital Infrastructure Association NL

[4] https://www.globalencryption.org/2020/11/breaking-encryption-myths/
[5] https://www.internetsociety.org/news/press-releases/2021/new-study-finds-australias-tola-law-poses-long-term-risks-to-australian-economy/

Dr Dries Van Dyck, CISO, SCK CEN
Eddy Willems, G DATA CyberDefense AG
Encryption Europe
European Digital Rights (EDRi)
Filip Lenaerts, CEO, Filip Lenaerts Corporation
Filip Schepers
Frans Gerbosch, Rack 66
Geert Antheunis
Global Partners Digital
Global Voices
Guido De smet
Hannes De Bondt
Homo Digitalis
Immo Deprez
Instituto Beta: Internet & Democracia (Brasil)
Internet Freedom Foundation (IFF)
Internet Society
Internet Society Belgium Chapter
Internet Society Brazil Chapter
Internet Society Catalunya Chapter
Internet Society Democratic Republic of Congo Chapter
Internet Society Ghana Chapter
Internet Society Netherlands Chapter
Internet Society Portugal Chapter
Internet Society India Delhi Chapter
Internet Society India Hyderabad Chapter
IP.rec - Law and Technology Research Institute of Recife
IT-Pol Denmark
Dr. Jan Tobias Muehlberg, KU Leuven, Dept. Computer Science
JCA-NET
Jenne Tondeleir
Jens Finkhäuser, Interpeer Project
Jeroen Lambrichts, University of Hasselt
Jochen Timmerman
Joran Leenders
José Legatheaux Martins, Professor, Faculty of Sciences of NOVA University of Lisbon
Kedero.com BV
Kijiji Yeetu
Koen Rutten, Managing Partner, Sensin
Koen Van Impe, cudeso.be Comm.V.

Kristof Dujardin
Kristof Provost, FreeBSD
LAYLO
Liga voor Mensenrechten
Mailfence
Mário Gaspar da Silva, Professor, Instituto Superior Técnico, Universidade de Lisboa, Portugal
Maarten De Bal
Mathias Bynens
Mega Limited
Merijn De Mil
Milton Mueller, Professor, Internet Governance Project, Georgia Institute of Technology
Netwerk Democratie
Onckelinx & Onckelinx BV
Open Governance Network for Europe
OpenMedia
OSCC BV Organization
OSIX s.r.l.
Peter Vandenabeele, All Things Data BV
Peter Van den Broeck, CyberAware Belgium
Peter Vanderborght
Philippe Dreesen, Vrije Universiteit Brussel (VUB)
Privacy & Access Council of Canada
Quantum Leap Development
Rack66 - EUSIP bvba
Raf Jespers, Lawyer, Justis Lawyers Group Antwerp Belgium
Ranking Digital Rights
RESPONSUM
Riana Pfefferkorn, Research Scholar, Stanford Internet Observatory
Rutger Bevers, CEO, ConversationStarter.net
Sammi Fux
SFLC.in
Statewatch
Steven Wittens, Software Engineer, Hacko
Stijn Volckaert, Professor of Computer Science, KU Leuven
Suomen Internet-yhdistys - Internet Society Finland Chapter
Tensr NV
The Electronic Privacy Information Center (EPIC)
Tresorit
Tutanota

Wim Remes, CEO, Wire Security BV
Youth Forum for Social Justice

*Affiliations listed for identification purposes only