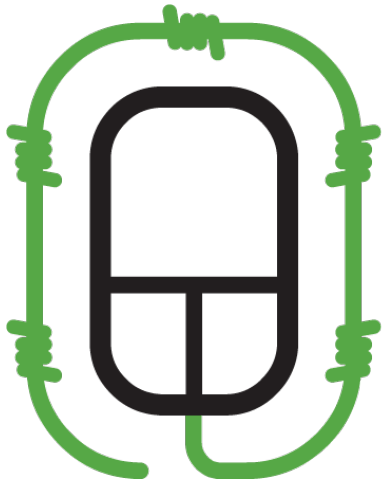




BITS OF FREEDOM

VERDEDIGT DIGITALE BURGERRECHTEN

Rejo Zenger | rejo.zenger@bof.nl | [@bitsoffreedom](https://twitter.com/bitsoffreedom) | [@rejozenger](https://twitter.com/rejozenger)





Reform of “Dutch Intelligence & Security Act of 2002”



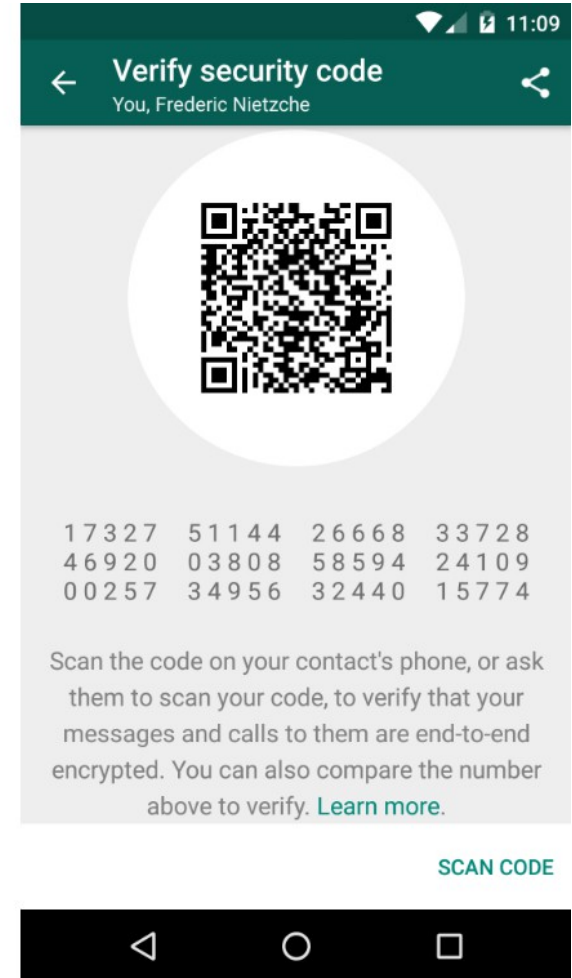
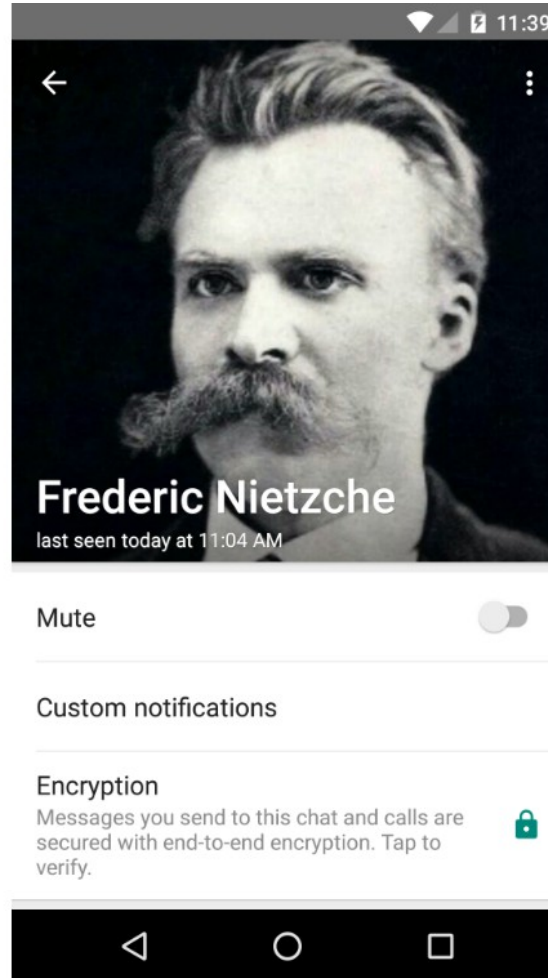
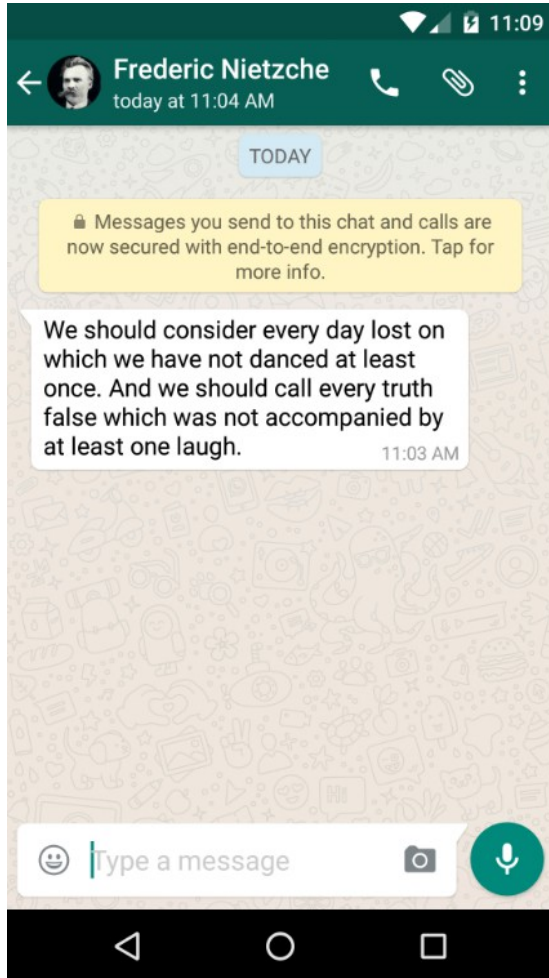
**Dragnet surveillance:
untargeted and large scale**

Sharing raw data with other intelligence services



**Extends hacking to
3rd parties as proxy
to targets**





Extension of obligation to cooperate to OTT-services

Aanhangige adviezen

U BEVINDT ZICH HIER: Home ► Adviezen ► Actuele adviezen ► Aanhangige adviezen

Adviesaanvragen in behandeling bij de Afdeling advisering van de Raad van State

Sectie I

Algemene Zaken

- Geen adviesaanvragen.

Binnenlandse Zaken en Koninkrijksrelaties

- Adviesaanvraag vierde periodieke beschouwing interbestuurlijke verhoudingen.
- Voorstel van wet houdende regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele andere wetten (Wet op de inlichtingen- en veiligheidsdiensten 20.).
- Voorstel van wet van het lid Albert de Vries ter introductie van een regime om problematiek in krimpregio's tegen te gaan (Wet bestrijding krimpproblematiek).
- Voorstel van wet van het lid Van Klaveren betreffende het beëindigen van positieve discriminatie (Kst 34521 nrs. 1 t.m. 3).

Onderwijs, Cultuur en Wetenschap

- Nota van wijziging inzake het voorstel van wet tot wijziging van de Wet op hoger onderwijs en wetenschappelijk onderzoek in verband

Vorige

Print

E-mail

Reform ePrivacy directive



2. The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.

3. This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.

Article 2

Definitions

Save as otherwise provided, the definitions in Directive 95/46/EC and in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) ⁽¹⁾ shall apply.

The following definitions shall also apply:

- (a) 'user' means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service;
- (b) 'traffic data' means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;

can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

Article 3

Services concerned

1. This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community.

2. Articles 8, 10 and 11 shall apply to subscriber lines connected to digital exchanges and, where technically possible and if it does not require a disproportionate economic effort, to subscriber lines connected to analogue exchanges.

3. Cases where it would be technically impossible or require a disproportionate economic effort to fulfil the requirements of Articles 8, 10 and 11 shall be notified to the Commission by the Member States.

Article 4

Security

1. The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these

The following definitions shall also apply:

- (a) 'user' means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service;
- (b) 'traffic data' means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;
- (c) 'location data' means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;
- (d) 'communication' means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;
- (e) 'call' means a connection established by means of a publicly available telephone service allowing two-way communication in real time;
- (f) 'consent' by a user or subscriber corresponds to the data subject's consent in Directive 95/46/EC;
- (g) 'value added service' means any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof;
- (h) 'electronic mail' means any text, voice, sound or image message sent over a public communications network which

⁽¹⁾ OJ L 108, 24.4.2002, p. 33.

Article 4

Security

1. The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

Article 5

Confidentiality of the communications

1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.

1. In implementing the provisions of this Directive, Member States shall ensure, subject to paragraphs 2 and 3, that no mandatory requirements for specific technical features are imposed on terminal or other electronic communication equipment which could impede the placing of equipment on the market and the free circulation of such equipment in and between Member States.

2. Where provisions of this Directive can be implemented only by requiring specific technical features in electronic communications networks, Member States shall inform the Commission in accordance with the procedure provided for by Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on information society services ⁽¹⁾.

3. Where required, measures may be adopted to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data, in accordance with Directive 1999/5/EC and Council Decision 87/95/EEC of 22 December 1986 on standardisation in the field of information technology and communications ⁽²⁾.

Article 15

Application of certain provisions of Directive 95/46/EC

1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this

⁽¹⁾ OJ L 204, 21.7.1998, p. 37. Directive as amended by Directive 98/48/EC (OJ L 217, 5.8.1998, p. 18).

⁽²⁾ OJ L 36, 7.2.1987, p. 31. Decision as last amended by the 1994 Act of Accession.

Article 16

Transitional arrangements

1. Article 12 shall not apply to editions of directories already produced or placed on the market in printed or off-line electronic form before the national provisions adopted pursuant to this Directive enter into force.

2. Where the personal data of subscribers to fixed or mobile public voice telephony services have been included in a public subscriber directory in conformity with the provisions of Directive 95/46/EC and of Article 11 of Directive 97/66/EC before the national provisions adopted in pursuance of this Directive enter into force, the personal data of such subscribers may remain included in this public directory in its printed or electronic versions, including versions with reverse search functions, unless subscribers indicate otherwise, after having received complete information about purposes and options in accordance with Article 12 of this Directive.

Article 17

Transposition

1. Before 31 October 2003 Member States shall bring into force the provisions necessary to comply with this Directive. They shall forthwith inform the Commission thereof.

Alles openklappen

Alles dichtklappen

Opschrift >

Aanhef >

Hoofdstuk 1 Algemene bepalingen

Hoofdstuk 2 Mededeling en registratie >
(Artikelen 2.1-2.5)

Hoofdstuk 3 Frequenties
(Artikelen 3.1-3.25)

Hoofdstuk 4 Nummerbeleid en nummerbeheer
(Artikelen 4.1-4.11)

Hoofdstuk 5 Aanleg, instandhouding
en opruiming van kabels
(Artikelen 5.1-5.17)

Hoofdstuk 6 Interoperabiliteit van diensten en vertrouwelijkheid van informatie (Artikelen 6.1-6.6)

Hoofdstuk 6a Verplichtingen voor ondernemingen die beschikken over een aanmerkelijke marktmacht
(Artikelen 6a.1-6a.22)

Hoofdstuk 6b Consultatie

Hoofdstuk 7 Eindgebruikersbelangen >
(Artikelen 7.1-7.9)

⊕ **Hoofdstuk 8** Regels met betrekking tot het verspreiden van programma's, systemen

Hoofdstuk 13. Bevoegd aftappen en toepassing van andere bevoegdheden op grond van het Wetboek van Strafvordering en de Wet op de inlichtingen- en veiligheidsdiensten 2002 in verband met telecommunicatie

Artikel 13.1

- 1** Aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten stellen hun telecommunicatienetwerken en telecommunicatiediensten uitsluitend beschikbaar aan gebruikers indien deze aftapbaar zijn.
- 2** Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot de technische aftapbaarheid van openbare telecommunicatienetwerken en openbare telecommunicatiediensten.

Artikel 13.2

- 1** Aanbieders van openbare telecommunicatienetwerken zijn verplicht medewerking te verlenen aan de uitvoering van een bevel op grond van het Wetboek van Strafvordering dan wel een toestemming op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2002 tot het aftappen of opnemen van telecommunicatie die over hun telecommunicatienetwerken wordt afgewikkeld.
- 2** Aanbieders van openbare telecommunicatiediensten zijn verplicht medewerking te verlenen aan de uitvoering van een bevel op grond van het Wetboek van Strafvordering dan wel een toestemming op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2002 tot het aftappen of opnemen van door hen verzorgde telecommunicatie.
- 3** Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot de te nemen organisatorische en personele maatregelen en te treffen voorzieningen met betrekking tot aftappen.

Artikel 13.2a

- 1** In dit artikel wordt verstaan onder:
- a.** *gegevens*: de verkeers- en locatiegegevens, bedoeld in [artikel 11.1, onderdeel b](#) respectievelijk [onderdeel d](#), alsmede de daarmee verband

< Zoek opnieuw

Alles openklappen

Alles dichtklappen

Opschrift

Aanhef

+ Eerste Boek

Algemeene bepalingen

(Artikelen 1-138f)

+ Tweede Boek

Strafvordering in
eersten aanleg

(Artikelen 139-398)

+ Derde Boek

Rechtsmiddelen

(Artikelen 399-482i)

+ Vierde Boek

Eenige rechtsplegingen
van bijzonderen aard

(Artikelen 483-552hhh)

+ Vijfde Boek

Internationale en
Europese strafvorderlijke samenwerking

(Artikelen -5:4:17)

+ Zesde Boek

Tenuitvoerlegging en
kosten

(Artikelen 553-)

Slotformulier en ondertekening

Wetboek van Strafvordering

Geldend van 11-08-2016 t/m heden

derde lid, wordt – tenzij zulks niet mogelijk is of het belang van strafvordering zich daartegen verzet – de aanbieder in de gelegenheid gesteld medewerking te verlenen bij de tenuitvoerlegging van het bevel.

5 Het bevel, bedoeld in het eerste lid, kan slechts worden gegeven na schriftelijke machtiging, op vordering van de officier van justitie te verlenen door de rechter-commissaris. [Artikel 126l, vijfde tot en met achtste lid](#), is van overeenkomstige toepassing.

6 Voor zover het belang van het onderzoek dit bepaaldelijk vordert, kan indien toepassing is gegeven aan het eerste lid tot degene van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van versleuteling van de communicatie, de vordering worden gericht medewerking te verlenen aan het ontsleutelen van de gegevens door hetzij deze kennis ter beschikking te stellen, hetzij de versleuteling ongedaan te maken.

7 De in het zesde lid bedoelde vordering wordt niet gericht tot de verdachte.

8 Op de in het zesde lid bedoelde vordering zijn [artikel 96a, derde lid](#), en [artikel 126l, vierde, zesde en zevende lid](#), van overeenkomstige toepassing.

9 Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld over de wijze waarop het in het eerste lid bedoelde bevel en de in het derde en zesde lid bedoelde vorderingen kunnen worden gegeven en over de wijze waarop daaraan wordt voldaan.

Artikel 126ma

1 Indien bij de afgifte van een bevel als bedoeld in [artikel 126m, derde lid](#), bekend is dat de gebruiker van het nummer, bedoeld in [artikel 126m, tweede lid, onderdeel c](#), zich op het grondgebied van een andere staat bevindt, wordt, voor zover een verdrag dit voorschrijft en met toepassing van dat verdrag, die andere staat van het voornemen tot het opnemen van telecommunicatie in kennis gesteld en de instemming van die staat verworven voordat het bevel ten uitvoer wordt gelegd.

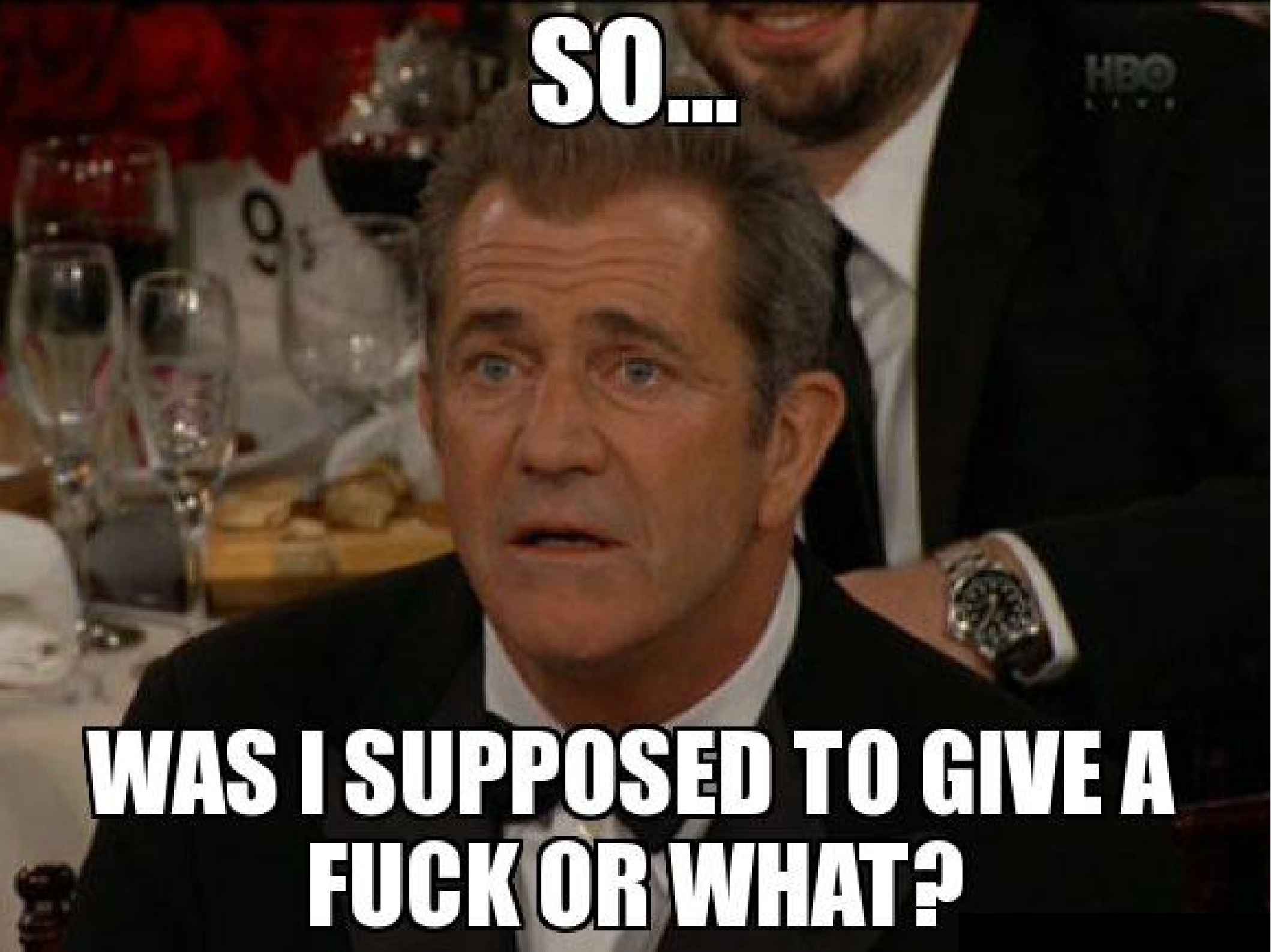
Should a new instrument cover new communication services (instant messaging, VoIP)?

Is there a need to allocate enforcement to one single authority? Which one?

Close to 70% of the combined total responses from industry, citizens and civil society say that one single national authority should be entrusted to enforce the rules, while half of the public bodies who responded to the consultation are not convinced that this is needed. For respondents who



“Truly arm our democracies on the issue of encryption”



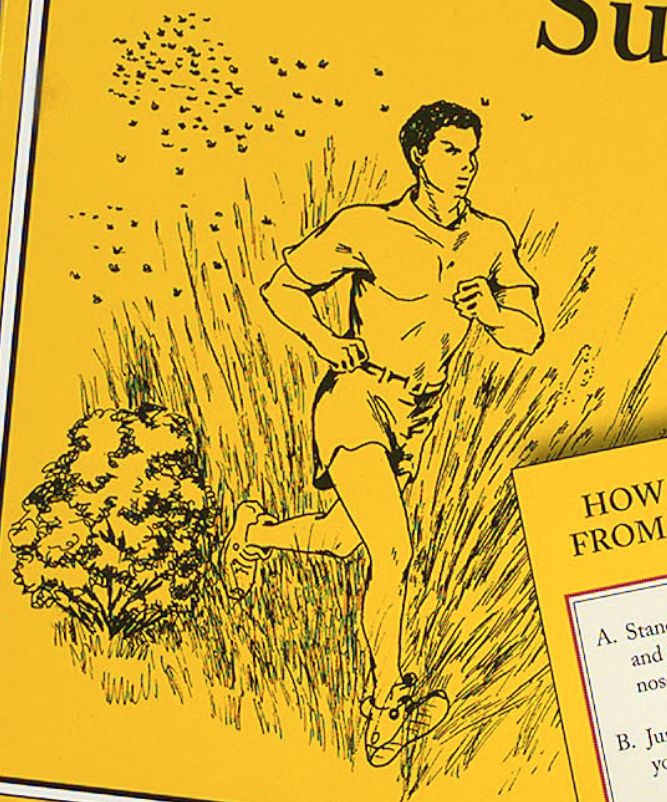
SO...

**WAS I SUPPOSED TO GIVE A
FUCK OR WHAT?**

UNIVERSITY
GAMES
01880

The WORST-CASE SCENARIO Survival Game™

Ages 8 &
2 or More



HOW TO ESCAPE FROM KILLER BEES

- A. Stand very still and quiet, and breathe through your nose.
- B. Jump into a body of water if you are near one.
- C. Run away as fast as you can.

HOW TO FEND OFF A SHARK

- A. Make quick, sharp, repeated jabs in the eyes or gills.
- B. Repeatedly punch or kick it in the nose, until it swims away.
- C. Grab and hold one or both pectoral fins.

The
WORST-CASE
SCENARIO
Survival Game™

TO LAND
OR LIFE RAFT
ON THE SHORE

The
ST-CASE
NARIO
val Game

UNIVERSITY
GAMES
01880

The
WORST-CASE
SCENARIO
Survival Game™

WhatsApp Messenger
Versione 2.11.169



© 2010-2014 WhatsApp Inc.
All rights reserved.

**Scope is broadened to cover
over-the-top players.**





- (1) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ⁽³⁾ requires Member States to protect the rights and freedoms of natural persons with regard to the processing of personal data, and in particular their right to privacy, in order to ensure the free flow of personal data in the Community.
- (2) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) ⁽⁴⁾ translates the principles set out in Directive 95/46/EC into specific rules for the electronic communications sector.
- (3) Articles 5, 6 and 9 of Directive 2002/58/EC lay down the rules applicable to the processing by network and service providers of traffic and location data generated by using electronic communications services. Such data must be

(1) Opinion delivered on 19 January 2006 (not yet published in the Official Journal).

(2) Opinion of the European Parliament of 14 December 2005 (not yet published in the Official Journal) and Council Decision of 21 February 2006.

(3) OJ L 281, 23.11.1995, p. 31. Directive as amended by Regulation (EC) No 1882/2003 (OJ L 284, 31.10.2003, p. 1).

(4) OJ L 201, 31.7.2002, p. 37.

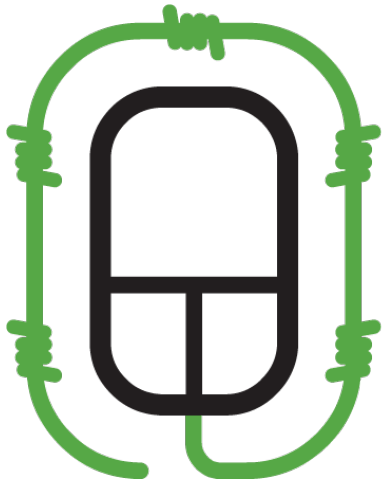
- (5) Several Member States have adopted legislation providing for the retention of data by service providers for the prevention, investigation, detection, and prosecution of criminal offences. Those national provisions vary considerably.
- (6) The legal and technical differences between national provisions concerning the retention of data for the purpose of prevention, investigation, detection and prosecution of criminal offences present obstacles to the internal market for electronic communications, since service providers are faced with different requirements regarding the types of traffic and location data to be retained and the conditions and periods of retention.
- (7) The Conclusions of the Justice and Home Affairs Council of 19 December 2002 underline that, because of the significant growth in the possibilities afforded by electronic communications, data relating to the use of electronic communications are particularly important and therefore a valuable tool in the prevention, investigation, detection and prosecution of criminal offences, in particular organised crime.
- (8) The Declaration on Combating Terrorism adopted by the European Council on 25 March 2004 instructed the Council to examine measures for establishing rules on the retention of communications traffic data by service providers.







**Question
everything.**



BITS OF FREEDOM

VERDEDIGT DIGITALE BURGERRECHTEN

Rejo Zenger | rejo.zenger@bof.nl | [@bitsoffreedom](https://twitter.com/bitsoffreedom) | [@rejozenger](https://twitter.com/rejozenger)

Photo credits: Ronald Plasterk by Comité des Régions, Share by Albert Sunyer, An old fishing net by Sam Cox, HHMM by Kerri Lee Smith, WhatsApp encryption by Engadget, Mr Jean-Claude Juncker by Comité des Régions, Bernard Cazeneuve by Toms Norde, Worst Case Scenario Game by University Games, European Parliament by Ash Cow, Man with the Megaphone by Rob Chandanaïs, Whatsapp su smartphone Nexus 5 by Desiree Catani.