TO: onlineharmsconsultation@culture.gov.uk
Online Harms Team

Consultation: Online Harms White Paper

First of all, a lot of thanks to Online Harms Team for organising this important consultation.

This opinion represents an opinion of an individual citizen, not any legal entity.

This opinion does not contain:
- any business secrets
- any trade secrets
- any confidential information.

This opinion is public.

PDF file of this opinion can be added to a relevant web page.

Annex 1 holds information about disclaimers and copyright.

Best Regards,

Jukka S. Rannila
citizen of Finland

signed electronically

[Continues on the next page]
General page for my opinions

General web page for my opinions is following:
http://www.jukkarannila.fi/lausunnot.html

Consultation document is very extensive / Only some issues handled

The consultation document for this consultation is very extensive (Online Harms White Paper, April 2019). I handle only some issues mentioned on the consultation document.

About European Union / United Kingdom / Exit / European Union

We know at the moment that United Kingdom is leaving the European Union in the future. This opinion handles partially European Union issues and also issues at the national level. Therefore readers of this opinion can assess national (outside the European Union) issues.

Misinformation / What to do?

One clear problem is misinformation. Also correcting different misinformed claims should be handled efficiently. Problem of misinformation is accelerated since electronic networks can spread misinformation very efficiently.

The general aim: pursuit for the truth / truth-seeking

Copyright, licence and disclaimers: check Annex 1.
The truth is, that misinformation can spread nowadays instantly around the Internet. Therefore, the truth-seeking endeavours are facing yet another problem, i.e. distortion by the general misinformation.

There are some interesting examples of truth-seeking endeavours organised outside the European Union:

* PolitiFact
* PolitiFact Australia
* FactCheck.org
* The Fact Checker.

It can be said, that PolitiFact has a reputational brand, and the brand is now expanded to Australia. All these four examples are organised differently. (e.g. a foundation, a private company). Also, there are some (non-profit) institutions supporting investigative journalism. Naturally, there are different site for leaking different classified material to the public, e.g. WikiLeaks.

The aim is the same with different organising modes: serious truth-seeking.

**schema.org → ClaimReview standard for transferring fact-checking reviews of claims**

Here we can note ClaimReview standard for transferring fact-checking reviews of claims (http://schema.org/ClaimReview). This standard explicates several data fields which are needed for assessing truthfulness of different claims.

Naturally there are mismatches between claims and reviews of claims. One claim can be forwarded very fast. Claim reviews mean a lot of work and claim reviews can be forwarded rather slowly.

**Examples of identifiers (ID) based on scientific communication**

Following identifiers can be presented:

- DOI
- ORCID
- ResearcherID
- Scopus Author ID
- ISNI

Copyright, licence and disclaimers: check Annex 1.
DOI is identifier (ID) for scientific articles. ORCID, ResearcherID and Scopus Author ID are identifiers (ID) for scientists. ISNI is identifier (ID) for contributors to creative works generally.

What we can learn from these identifiers (DOI, ORCID, ResearcherID, Scopus Author ID, ISNI)?

Here we can note following issues:

1) specific (scientific) articles can be pinpointed clearly
2) different scientist can be pinpointed clearly
3) there can be non-profit organisations for developing different identifiers
4) there can be commercial organisations for developing different identifiers.
5) there can be different identifiers for the same issue, e.g. global and national
6) there can be some redundancy of different identifiers.

Each DOI is unique and permanent. A document keeps the same DOI for its entire lifetime and, if ever the document is deleted, the DOI will not be reused. An example of the DOI identifier can presented.

doi:10.2788/14231

The prefix (before slash) is assigned to an organisation which can register DOI names. Following the prefix (separated by a forward slash) is the suffix (unique to a given prefix) to identify the entity.

Resolving a DOI name can be done on the following web page

https://dx.doi.org

→ an example → add 10.2788/14231 to the search field.
→ this leads to actual web page of that publication (doi:10.2788/14231).

Like said before DOI means unique identifiers for scientific articles and one DOI user is Publications Office of the European Union (Publications Office).

Proposal for identifiers (ID) for media solutions

Based on the previous ideas of identifiers (ID) there could be following issues when creating different identifiers (ID) for media solutions:

• identifiers (ID) for media organisations (e.g. newspaper or television channel)
• identifiers (ID) for journalists
• identifiers (ID) for stories provided by media organisations
• identifiers (ID) for corrections of different stories.

Proposal: A serious assessment of different identifiers (ID) for media solutions could be

Copyright, licence and disclaimers: check Annex 1.
done carefully.

Naturally following identifiers (ID) could be assessed:

- global identifiers (ID)
- EU-wide identifiers (ID)
- general member state (EU) identifiers (ID)
- several identifiers (ID) in members states (EU)
- identifiers outside the European Union.

Based on examples of identifiers (ID) of scientific publications there could be similar efforts.

**National level?**

It can be concluded, that a specific story in the national in a member state is actually distributed in several systems in a member state. Different member state systems (MSS) are then integrated in different layers. In other words, the original is distributed totally and partially to several systems.

Like said before, one (or more) of the systems can be a special system for correcting the misinformation distributed in different stories.

At the national level (member state) there is a need at least for the following information:

- clear identifier for an original story
- original story without modifications
- modification(s) added later to the original story
- originator(s) of a story
- factual references of a story
- original distributor of a story
- members (persons / communities) in a story
- references to previous story / stories

On the other hand, the misinformation can spread also, and there could be the following information:

- clear identifier for the found misinformation
- original (misinformation) story without modifications
- modification(s) added later to the original (misinformation) story
- originator(s) of a (misinformation) story
- factual references of a (misinformation) story
- non-factual references of a (misinformation) story
- original distributor of a (misinformation) story
- members (persons / communities) in a (misinformation)story.

Naturally, there has to be identifier for person / community, who / which has made a evaluation of a
story and the amount of misinformation in a story. Therefore some more additions:

- person / community responsible for evaluating the amount of misinformation in a story.

It can be said, that depending on the situation in a specific member state, misinformation distributing efforts are covered rather fast. E.g. in Finland different media actors are quite eager to point mistakes in stories provided by other media actors.

**Media pluralism – possible problems?**

One issue is naturally “new” media which is not like “traditional” media. “New” media can be internet-only solutions and possibly not following guidelines for journalist; e.g. in Finland we have guidelines\(^1\) for journalists and an annex (Material generated by the public on a media website).

Naturally there should be journalistic freedom when publishing news based on different viewpoints.

**One centre (European centre?) for informing different information technology problems**

I have advocated one center for informing different information technology problems. At the moment there are several possibilities for informing different information technology problems.

Examples for informing information technology problems are following:

- Spamhouse Project\(^2\) for tracking email spammers and spam-related activity
- SpamCop\(^3\) service for reporting spam
- Common Vulnerabilities and Exposures (CVE)\(^4\) for informing information-security vulnerabilities and exposures
- Forum of Incident Response and Security Teams\(^5\)
- computer emergency response team (CERT) – also national CERT teams
- CSIRT Virus Watch\(^6\)
- Scamdex\(^7\)
- providers of different technology solutions have their own reporting services.

There is one note on inception impact assessment document about fragmentation of the effort, lack of a dynamic EU-wide ecosystem.

**Proposal: There could be some work for creating just one service for informing different information technology problems.**

\(^2\) [https://www.spamhaus.org](https://www.spamhaus.org)
\(^3\) [https://www.spamcop.net](https://www.spamcop.net)
\(^4\) [http://cve.mitre.org](http://cve.mitre.org)
\(^5\) [https://www.first.org](https://www.first.org)
\(^6\) [http://www.csirt.org](http://www.csirt.org)
\(^7\) [http://www.scamdex.com](http://www.scamdex.com)

Copyright, licence and disclaimers: check Annex 1.
Proposal: Possibly there could be just one service for informing different information technology problems.

Like said before (also based on previous opinions) there can be several solutions for informing different information technology problems. Possibly different services are not connected to other systems.

More and more identifiers (ID)

In the previous consultations there has been discussion about different identifiers (ID) in different systems. It can be noted from the previous opinions, that there will be several and different identifiers (ID) for different levels. At the European Union level there can be several identifiers (ID), e.g. following:

* global identifiers (ID)
* EU-wide identifiers (ID)
* general member state identifiers (ID)
* several identifiers (ID) in member states.

Proposal: There could be a systematic review of different identifiers (ID).

It can be noted, that some member states (EU) are federations, and different federal states can have their own identifiers (ID).

Examples of these identifiers are following:

1) Facebook ID for an individual person
2) Facebook ID for the individual up-dates of individuals
3) Data Universal Numbering System (D-U-N-S)
4) Reuters instruments codes (RICs)
5) Social security code for individual citizens in the European Union member states
6) Business identity code for a company in an European Union member state
7) Value added tax code for a company in an European Union member state.

The examples of private IDs (Facebook IDs, Data Universal Numbering System (D-U-N-S), Reuters Instrumens Codes (RICs)) show, that persons and/or communities can use or even demand of using IDs from privately owned information systems.

More new identifiers (ID)?

The current reality is, that there will be more and more IDs, since digitalisation of different areas will result new IDs and/or combination of new and old IDs.

The creation YET another public ID is not always organised by the European Union, and in some

Copyright, licence and disclaimers: check Annex 1.
cases the European Union (and member states) just have to accept the reality of some of those public IDs – in some cases even private IDs are the norm. The Reuters Instrument Codes (RICs) is an example of a near monopoly situation, and some of current private IDs might constitute (near) monopoly situations. Naturally, (near) monopolies can be assessed by the Competition Directorate-General, and it will be interesting to see possible new cases related to private IDs.

Note: Digitalisation of everything means more identifiers (ID).

Note: All new identifiers (ID) mean more work for developing existing and new informations systems.

Note: There can be new stakeholder groups in the near/distant future which mean more identifiers (ID).

Proposal: The could be some assessment(s) based on different versions of different identifiers (ID).

Open horizontal standards

There are differences between horizontal and vertical standards. A simple example is naturally email solutions. There are several vertical standards when creating technically email solutions. Then there are horizontal standards which enable sending messages between technically different email solutions. Horizontal standards enables technological solutions which can work together. Horizontal standards hides different complexities in information systems.

Proposal: There could be assessment of vertical and horizontal standards.

Proposal: Using horizontal standards could be favoured when creating different information systems.
Opinion: The number of redundant standardisation efforts should be minimal.

Proposal: There could be separation of horizontal standards and vertical standards.

Proposal: There could be different standardisation efforts to horizontal standards and vertical standards.

Personally I have advocated using different horizontal standards. For example email standards (horizontal) are implemented with very different technologies (vertical).

Proposal: Governments should especially concentrate on horizontal standards.

Proposal: Some government agencies could apply for memberships of different standard setting organisations which develop especially horizontal standards.

Here we can note some problems:

- some systems are based on de-facto standards
- some systems are based on de-jure standards
- there can be confrontations between de-facto and de-jure standards
- there can be a monopoly situation in some domain
- some standards may inhibit possible actions of some stakeholders
- there can be a standard war on some domains
- standards have different life-cycles
- systems have different life-cycles

Copyright, licence and disclaimers: check Annex 1.
there can be mismatches between different life-cycles
there can be failed standards
there can be deprecated standards.

It is quite normal situation in the information technology field that there are competing standards for some application field. Therefore there are all the time ongoing “standards wars” or “format wars”. The information technology standards tend to be interrelated and one “standards war” or “format war” can lead to another similar situation.

I have advocated open standards even though in some cases open standards are not de facto standards. In practice public sector has very important role, when some standards are competing in the market place. Because public sector has a considerable power when buying/developing information systems and therefore public sector can sometimes direct markets to certain standards. Therefore there should be serious vigilance when assessing different standards and “standards” in some application fields.

An example for cooperation: Web feeds (RSS and Atom)

I have advocated usage of web feeds on several previous opinion documents. Actually there are two standards for web feeds: RSS and Atom.

Proposal: Web feeds (RSS and/or Atom) could be advocated when developing different informations systems (EU / Member states).

Proposal: Web feeds (RSS and/or Atom) should be used extensively for providing (real-time) information for different stakeholder(s) (communities).

Proposal: There can be different web feeds (RSS and/or Atom) for different stakeholder(s) – having just one web feed (RSS and/or Atom) may not be a feasible solution.

Proposal: Several web feeds (RSS and/or Atom) can be based on different viewpoints.

It can be easier to create web feeds in different information systems since web feeds enable connections without direct system-to-system connections.

18 https://en.wikipedia.org/wiki/Web_feed
19 http://www.rssboard.org/rss-specification, RSS 2.0 Specification
21 https://en.wikipedia.org/wiki/Atom_(standard), Wikipedia / Atom (standard)

Copyright, licence and disclaimers: check Annex 1.
It can be noted, that different back-office systems (with a wide variety of different technologies) can implement RSS standards, and these RSS feeds can be used in the front-office systems. With this kind solutions front-office systems don’t need direct system-to-system communications with back-office systems.

Answers to some specific questions

Question 3:
In what other ways should users be able to tell the regulator about harmful information or activity online?

Answer:
Previously I have advocated just one place and one service for informing different information technology problems like online harm.

United Kingdom could organise just one place and one service for informing different information.

Naturally global cooperation should be assessed carefully.

Question 4:
What role should parliament play in checking the work of the regulator? Should parliament be part of writing the codes of practice?

Answer:
European Union has published Code of Practice on Disinformation


That approach could be assessed by different stakeholders in the United Kingdom.

Answer:
There could be a specific Code of Practice on Disinformation in the United Kingdom.

Question 7a:
What do you think we should ask private channels for communicating to do, so that we can deal with online harm?

Answer:
Cooperation with private stakeholders can be organised in different ways.

Private stakeholders can be part of the solution for assessing online harm.

Question 15:
How should the government be a part of dealing with these barriers and opportunities?

Answer:
(1) Government could organise different application programming interfaces (API) for different stakeholders.
(2) Different stakeholders can provide own interfaces.
(3) Cooperation between different stakeholders (APIs) can be organised.

Note: there can several application programming interfaces (API) and different versions of application programming interfaces (API).
Note: In practical reality different information systems are layered in different ways.
Note: There can be several standards (formats) for transmitting data

(4) United Kingdom could organise one central system (CS) for reporting online harm.
(5) Different standard (formats) for reporting online harm could be assessed carefully.
ANNEX 1

DISCLAIMERS

Legal disclaimer:
All opinions in this opinion paper are personal opinions and they do not represent opinions of any legal entity I am
member either by law or voluntarily. This opinion paper is only intended to trigger thinking and it is not legal advice.
This opinion paper does not apply to any past, current or future legal entity. This opinion paper will not cover any of the
future changes in this fast-developing area. Any actions made based on this opinion is solely responsibility of respective
actor making those actions.

Political disclaimer:
These opinions do not represent opinions of any political party. These opinions are not advices to certain policy and
they are only intended to trigger thinking. Any law proposal based on these opinions are sole responsibility of that legal
entity making law proposals.

These opinions are not meant to be extreme-right, moderate-right, extreme-centre, moderate-centre, extreme-left or
moderate-left. They are only opinions of an individual whose overall thinking might or might not contain elements of
different sources. These opinions do not reflect past, current or future political situation in the Finnish, European or
worldwide politics.

These opinions are not meant to rally for a candidacy in any public election at any level.

Content of web pages:
This text may or may not refer to web pages. The content of those web pages is not responsibility of author of this
document. They are referenced on the date of this document. If referenced web pages are not found after the date when
this document is dated, that situation is not responsibility of the author. All changes done in the web pages this
document refers are sole responsibility of those organisations and individuals maintaining those web pages. All illegal
content found on the referred web pages is not on the responsibility of the author of this document, and producing that
kind content is not endorsed by the author of this document.

Use of broken English
This text is in English, but from a person, whose is not a native English-speaking person. Therefore the text may or may
not contain bad, odd and broken English, and can contain awkward linguistic solutions.

COPYRIGHT

This opinion paper is distributed under Creative Commons licence, to be specific the licence is “Attribution-
NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0)”. The text of the licence can be obtained from
the following web page:
http://creativecommons.org/licenses/by-nc-nd/4.0/
The English explanation is on the following web page:
http://creativecommons.org/licenses/by-nc-nd/4.0/legalcode

Copyright, licence and disclaimers: check Annex 1.