

International privacy organisations: Don't let corporations strip citizens of their right to privacy



This report has been put together by members of European Digital Rights including Bits of Freedom, Open Rights Group and Privacy International.

The coalition of organisations supporting this initiative include Digitale Gesellschaft, Access and La Quadrature du Net.

nakedcitizens.eu

Table of Contents

1. Executive summary.....	3
2. Why does the EU need a new Data Protection Regulation?.....	4
3. Five proposals that will hurt privacy most.....	7
1. Weakening the definition of consent.....	7
2. "Profiling" citizens without their consent.....	8
3. Allowing the use of personal data for all kinds of purposes.....	8
4. Business interests vs the rights of citizens.....	9
5. Introducing false assumptions about 'pseudonymous data'.....	9
4. Recommendations and further reading.....	11
Appendix: The amendments that would do the most damage.....	12

1. Executive summary

This report features new analysis by privacy experts of proposed amendments to the draft Data Protection Regulation. It reveals how many of these amendments threaten to critically undermine the privacy of EU consumers and citizens. Together, the amendments are an effort to strip EU citizens 'naked' by making it almost impossible for them to control who sees their personal information and even how it is used.

Over 3,000 amendments to the Regulation are currently being considered by the LIBE Committee in the European Parliament. We have identified 46 of the worst. Most of these were tabled by Members of the Alliance of Liberals and Democrats in Europe (ALDE) and European People's Party (EPP) political groups (24 and 15 respectively). As these parties between them (almost) hold a majority in the European Parliament, together they threaten wholesale destruction of privacy rights of those who have elected them.

We have grouped the amendments into five themes, outlining exactly why they would be so damaging for EU citizens' privacy rights. The proposals would:

- weaken the definition of consent, making it more likely people could unwittingly agree to their data being used.
- make it easy for companies to profile people without their consent, resulting in possible discrimination particularly of the most vulnerable.
- allow businesses more readily to decide their interests outweigh people's privacy rights.
- assume that so-called "pseudonymisation of data" is an effective means of avoiding privacy harms.

These are by no means the only damaging amendments. Many more of the thousands of amendments tabled in LIBE would undermine other citizens' rights such as the right to object, to have data deleted and would weaken the sanctions that those who break the rules could face.

We urge Members of the European Parliament (MEP's) to reject these damaging amendments and help put people in control of their data. Far from being harmful to innovation and business, as some would claim, a strong and effective Data Protection Regulation would ensure EU global leadership in this field by creating harmonised rules and a more trusted, safe and predictable legal environment for an economy of 500 million people.

2. Why does the EU need a new Data Protection Regulation?

“The Internet is a surveillance state. Whether we admit it to ourselves or not, and whether we like it or not, we’re being tracked all the time.”

Security expert Bruce Schneier, March 2013¹.

Data protection law might seem technical – a niche topic for legal geeks. But it now affects us all in many important ways.

Almost everything we do creates a trail of data. Information about the websites we visit is tracked and stored. Our movements can be recorded through electronic travel cards. The mobile apps we use may demand to know where we are, or ask for information from our address books.

The people we know, the music we like, the news we read and the amount we spend – all of it is can now be tracked, stored and analysed.

The personal data we leave behind is now used by institutions and organisations to help them make many important decisions about us. These profiles affect everything from the marketing offers we receive through to the credit ratings and insurance decisions we are subject to. The information feeds those who want insights into our movements, personalities, histories, and relationships².

Too often, we do not control how and by whom our personal information will be used. Too often the data is not secure enough, with abuses and mistakes going effectively unpunished. As a result, all sorts of businesses hold personal information for reasons that have little to do with the purposes for which it was originally collected. They often use it in ways the 'data subjects' might object to.

It is not surprising that the majority of people do not trust those that collect and use their personal data. A Eurobarometer survey³ found that 70% of Europeans are concerned about companies using information for a purpose different to the one it was collected for. Recently a study by Ovum found that only 14 percent of respondents believe that Internet companies are honest about their use of consumers' personal data⁴.

1 http://www.schneier.com/blog/archives/2013/03/our_internet_su.html

2 See for example the study from Cambridge's Psychometrics Centre into Facebook 'Likes':
<http://www.cam.ac.uk/research/news/digital-records-could-expose-intimate-details-and-personality-traits-of-millions>

3 http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

4 http://ovum.com/press_releases/ovum-predicts-turbulence-for-the-internet-economy-as-more-than-two-

A lack of privacy does not just leave people feeling uncomfortable. A study by TRUSTe in the UK found that 94% of people worry about their online privacy, and that consumers engage less with companies they do not trust – leading to lower purchases (29%), app downloads (68%) and sharing of information (86%)⁵. A market study for the Executive Agency for Health and Consumers in 2011 found that 29% of people say concerns about the misuse of personal data or payment details is a key factor in them not shopping online⁶.

Why the new Data Protection Regulation will help

The European Commission published a draft Data Protection Regulation on 25 January 2012. It is a proposed update to the Data Protection Directive from 1995. The Regulation as it stands is designed to address the problems mentioned above. It is a stronger and more enforceable assertion of existing data protection principles.

The Regulation outlines a number of measures that would give people more control over their data and make sure businesses that use it play by the rules, ensuring they are held to account for their data practices. It would give people a stronger definition of consent, stronger rights to have data erased, enable people to find out about and challenge profiling, and make sure those using data are held accountable for mistakes and abuses.

This sort of strong Regulation would put citizens and consumers at the heart of the digital economy. It would harmonise the rules across the EU, creating a more trusted, safe and predictable legal environment.

Why is there a problem now?

The Regulation is currently being discussed by the LIBE Committee in the European Parliament.

Among the thousands of amendments tabled in the Committee are a large number that threaten to severely weaken privacy rights. These damaging amendments are largely the result of an unprecedented lobbying storm by big US tech companies, the US Government and the advertising industry.

[thirds-of-consumers-say-no-to-internet-tracking/](#)

5 http://www.truste.com/about-TRUSTe/press-room/news_truste_transparency_choice_needed_to_address_uk_privacy

6 Consumer market study on the functioning of e-commerce and Internet marketing and selling techniques in the retail of goods, Executive Agency for Health and Consumers, 2011
http://ec.europa.eu/consumers/consumer_research/market_studies/docs/study_ecommerce_goods_en.pdf (Page 32)

Instead of a Regulation that gives people more of a stake in how their personal information is used, these amendments would take these decisions out of people's hands. Instead of empowering users to take control of their information, the amendments would allow businesses, institutions or organisations to collect and share personal information in opaque, unaccountable ways.

The proposed changes to the Data Protection Regulation analysed in this report will strip citizens of the control of their personal data and leave them 'naked' to the prying eyes of big business. We urge MEP's to vote against these amendments and help finally give citizens control over their personal data.

3. Five proposals that will hurt privacy most

Below are the five worst changes to data protection law proposed by members of the LIBE Committee. Each section provides a short analysis of the problem and why the amendments would have a detrimental effect on privacy. A list of specific relevant amendments can be found in the Appendix.

1. Weakening the definition of consent

Why is this an issue?

Consent is one of the legal bases of processing. It is frequently abused, especially online, where collection is often based on vague or confusing language. Sometimes businesses say it is enough that someone's behaviour – for example signing up to a website – implies that they consent to the use of their data.

The Regulation says that consent must be 'informed, specific and explicit'. That would mean somebody has to make an active choice, ensuring people really know what data processing they are agreeing to.

People want more control over how their data is used. For example, participants in a 2010 study by the UK think-tank Demos ("A People's Inquiry into Personal Information"), made a number of demands for more control, for example through greater transparency and more meaningful consent.⁷

What would these amendments do?

Many amendments we have analysed for this report would weaken this definition, for example by removing the word 'explicit' or by replacing the definition with more vague language. This would allow companies to assume consent has been given or to include consent language in hard to understand terms and conditions.

⁷ http://www.demos.co.uk/files/Private_Lives_-_web.pdf (see for example page 94)

2. "Profiling" citizens without their consent

Why is this an issue?

Profiling is the automated processing of information relating to a person in order to derive information about some of their characteristics or traits. That could include their creditworthiness, their location or another type of personal behaviour. This information is often used to make decisions about people or to affect them in a number of significant ways, from the offers they receive online through to their credit ratings.

The Regulation could help make sure that profiling only takes place when people clearly agree to it, or when profiling is necessary to conclude a contract (for instance for a personal loan). In other cases, profiling should remain prohibited to make sure that people have a say in the assumptions and judgments made about them.

What would these amendments do?

A great number of the amendments put forward by MEPs do not recognize the dangers associated with profiling and propose allowing profiling even *without* consent of citizens. This means that citizens run a real risk of being assessed by automated means, for instance online, without their consent or knowledge.

3. Allowing the use of personal data for all kinds of purposes

Why is this an issue?

Data protection law is based on the principle of "purpose limitation". Data collected for one reason cannot simply be re-used for any other purpose. This prevents a business from collecting data for one seemingly reasonable purpose and then simply using it in further, unspecified ways that the data subjects may object to.

What would the amendments do?

A number of amendments undermine or even delete this principle by suggesting that data collected for purpose "A" could be re-used for a completely different and unrelated purpose by the same or in some cases another company. This would rob citizens of any control over their own data, creating a lawless environment for personal data for the benefit of companies or governments. This would leave people with almost no knowledge of or control over how their data is used.

4. Business interests vs the rights of citizens

Why is this an issue?

Companies often use a legal basis for processing personal data called the 'legitimate interests' ground. This allows companies to determine whether their legitimate 'business interests' can prevail over the rights and interests of citizens.

Research has shown that companies often misuse this ground – for example, it permitted Google to merge data privacy policies across all its services, allowing Google to combine data from their services for any purposes⁸. People often do not have access to information about when this ground is used and which interests are served by it.

What would the amendments do?

Instead of fixing this often misused ground, members of the European Parliament propose extending it by including the interests of third parties as a 'legitimate interest' and extending the scope to purposes that are incompatible with the original purpose for which the data was collected. This will allow companies unknown to citizens to process personal data relating to these citizens if the companies believe it is in their 'best interest' to do so. That would make an already big loop hole even more broad and permit all sorts of processing without the consent of the individual.

5. Introducing false assumptions about 'pseudonymous data'

Why is this an issue?

There are ways to try to 'anonymise' data sets, so that it seems the subjects of a study or dataset are not identifiable. The term 'pseudonymisation' is a way of describing a broad range of techniques for trying to make data identifiable only when combined with other data.

However, even if a company 'pseudonymises' information about a specific person (meaning "Mr. Smith's" name is separated from other information about him and this information is then saved in a separate database as record number "ABC123") the information can still be used to make decisions targeted at Mr. Smith.

Furthermore, data that is supposedly 'anonymous' or 'anonymised' can, in fact, be re-identified⁹. For example, researchers were able to identify people who participated in a large

⁸ https://www.bof.nl/live/wp-content/uploads/20121211_onderzoek_legitimate-interests-def.pdf

⁹ See, for example, "The Re-Identification of Anonymous Data and the Processing of Personal Data for Further Purposes: Challenges to Privacy" http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1740383

genomic study based on some of the participants' genomes and other publicly accessible information.¹⁰ As technology and techniques develop, re-identification from supposedly anonymised or pseudonymized datasets will become easier.

What would the amendments do?

Many amendments introduce a definition of 'pseudonymous data'. They are based on the false assumption that the processing of pseudonymous data will not impact the privacy of citizens. Simply removing names from data does not mean data will not be used to target individuals or subsequently re-identify them.

Parliamentarians must to recognize that pseudonymous data are personal data and deserve full protection under the law. Pseudonymisation might serve as a useful additional security measure, but should not be regarded as a separate category of data over which people have fewer rights.

¹⁰ <http://www.wired.com/wiredscience/2013/01/your-genome-could-reveal-your-identity/>

4. Recommendations and further reading

We urge MEP's to reject the amendments analysed in this report. Instead, we urge MEPs to support a Regulation which empowers people to take control of their data through enforceable data subject rights, narrower exemptions and exceptions to those rights and stronger sanctions. European Digital Rights has published recommendations and an analysis of the key issues (see below)¹¹.

Further information and material

- Privacy International : Analysis of the Data Protection Regulation: <https://www.privacyinternational.org/blog/our-analysis-of-the-european-commissions-proposal-for-a-general-data-protection-regulation>
- EDRI's online information centre for the Data Protection Regulation: <http://protectmydata.eu/>
- Key issues of the Data Protection Regulation: <http://www.privacypolicy.eu/wp-content/uploads/2013/02/Keyissues-EUDataP.pdf>
- EDRI's "myth busting" briefings, booklet and flyers on the Data Protection Regulation: <http://www.privacypolicy.eu/2013/01/material/>
- Bits of Freedom : A loophole in data processing - Why the 'legitimate interests' test fails to protect the interests of users and the Regulation needs to be amended https://www.bof.nl/live/wp-content/uploads/20121211_onderzoek_legitimate-interests-def.pdf
- Open Rights Group brief guide to the issues: <http://www.openrightsgroup.org/ourwork/reports/data-protection-regulation:-a-brief-guide-to-the-issues>

Contact information

Joe McNamee, Executive Director, European Digital Rights via +32 (0)2 2742570 or press@edri.org

¹¹ EDRI: Key issues and what we need in the Regulation <http://www.privacypolicy.eu/wp-content/uploads/2013/02/Keyissues-EUDataP.pdf>

Appendix: The amendments that would do the most damage

1. Weakening the definition of consent (7)

AM757 (Jens Rohde, Adina-loana Vălean, ALDE);
AM758 (Louis Michel, ALDE);
AM760 (Lidia Joanna Geringer de Oedenberg S&D);
AM762 (Sarah Ludford, Charles Tannock, ALDE);
AM764 (Timothy Kirkhope, ECR);
AM765 (Axel Voss, Seán Kelly, Wim van de Camp, Hubert Pirker, Monika Hohlmeier, Georgios Papanikolaou, Véronique Mathieu Houillon, Anna Maria Corazza Bildt, EPP)
AM766 (Agustín Díaz de Mera García Consuegra, Teresa Jiménez-Becerril Barrio, EPP);

2. “Profiling” citizens without their consent (12)

AM1545 ((Alexander Alvaro, ALDE)
AM1547 (Jens Rohde, Adina-loana Vălean, ALDE);
AM1549 (Axel Voss, Seán Kelly, Wim van de Camp, Véronique Mathieu Houillon, EPP)
AM1551 (Lidia Joanna Geringer de Oedenberg S&D);
AM1553 (Timothy Kirkhope, ECR);
AM1554 (Ewald Stadler)
AM1555 (Louis Michel, ALDE)
AM1556 (Jens Rohde, Adina-loana Vălean, ALDE);
AM1557 (Jens Rohde, Adina-loana Vălean, ALDE);
AM1560 ((Alexander Alvaro, ALDE)
AM1568 (Jens Rohde, Adina-loana Vălean, ALDE);
AM1572 (Axel Voss, EPP);

3. Using personal data of citizens for all kinds of purposes / 'purpose limitation principle' (6)

AM818 (Jens Rohde, Adina-loana Vălean, ALDE)
AM819 (Louis Michel, ALDE)
AM944 (Alexander Alvaro, Nadja Hirsch, ALDE)
AM945 (Axel Voss, Seán Kelly, Wim van de Camp, Véronique Mathieu Houillon, Monika Hohlmeier, Lara Comi, Renate Sommer, EPP)
AM947 (Ewald Stadler)
AM948 (Jens Rohde, Adina-loana Vălean, ALDE)

4. Business interests vs the rights of citizens (4)

AM880 (Louis Michel, ALDE);

AM882 (Agustín Díaz de Mera García Consuegra, Teresa Jiménez-Becerril Barrio, EPP);

AM883 (Salvatore Iacolino, EPP);

AM884 (Ewald Stadler)

5. The introduction and use of pseudonymous data (17)

AM726 (Alexander Alvaro, ALDE);

AM729 (Sarah Ludford, ALDE);

AM730 (Axel Voss, Seán Kelly, Wim van de Camp, Véronique Mathieu Houillon, Renate Sommer, Monika Hohlmeier, Georgios Papanikolaou, Anna Maria Corazza Bildt, EPP).

AM732 (Adina-Ioana Vălean, Jens Rohde, ALDE);

AM851 (Alexander Alvaro, ALDE);

AM887 (Adina-Ioana Vălean, Jens Rohde, ALDE);

AM897 (Adina-Ioana Vălean, Jens Rohde, ALDE);

AM898 (Axel Voss, Seán Kelly, Wim van de Camp, Véronique Mathieu Houillon, Renate Sommer, Monika Hohlmeier, EPP);

AM900 (Axel Voss, Seán Kelly, Wim van de Camp, Véronique Mathieu Houillon, Renate Sommer, Monika Hohlmeier (EPP);

AM904 (Alexander Alvaro, Nadja Hirsch, ALDE);

AM921 (Axel Voss, Seán Kelly, Wim van de Camp, Véronique Mathieu Houillon, Renate Sommer, Monika Hohlmeier, EPP);

AM922 (Sabine Verheyen, Axel Voss, Anna Maria Corazza Bildt, Monika Hohlmeier, EPP)

AM1542 (Jens Rohde, Adina-Ioana Vălean, ALDE);

AM1543 (Axel Voss, Seán Kelly, Wim van de Camp, Véronique Mathieu Houillon, Renate Sommer, Monika Hohlmeier, EPP);

AM1568 (Jens Rohde, Adina-Ioana Vălean, ALDE);

AM1585 (Axel Voss, Seán Kelly, Wim van de Camp, Véronique Mathieu Houillon, Renate Sommer, Monika Hohlmeier, EPP);

AM1630 (Monika Hohlmeier, Axel Voss, EPP).

By group:

15 proposed by members of the EPP group.

24 amendments proposed by members of the ALDE group.

2 amendments from a member of the ECR group.

2 amendments from a member of the S&D group.

3 from an unattached member (Ewald Stadler).