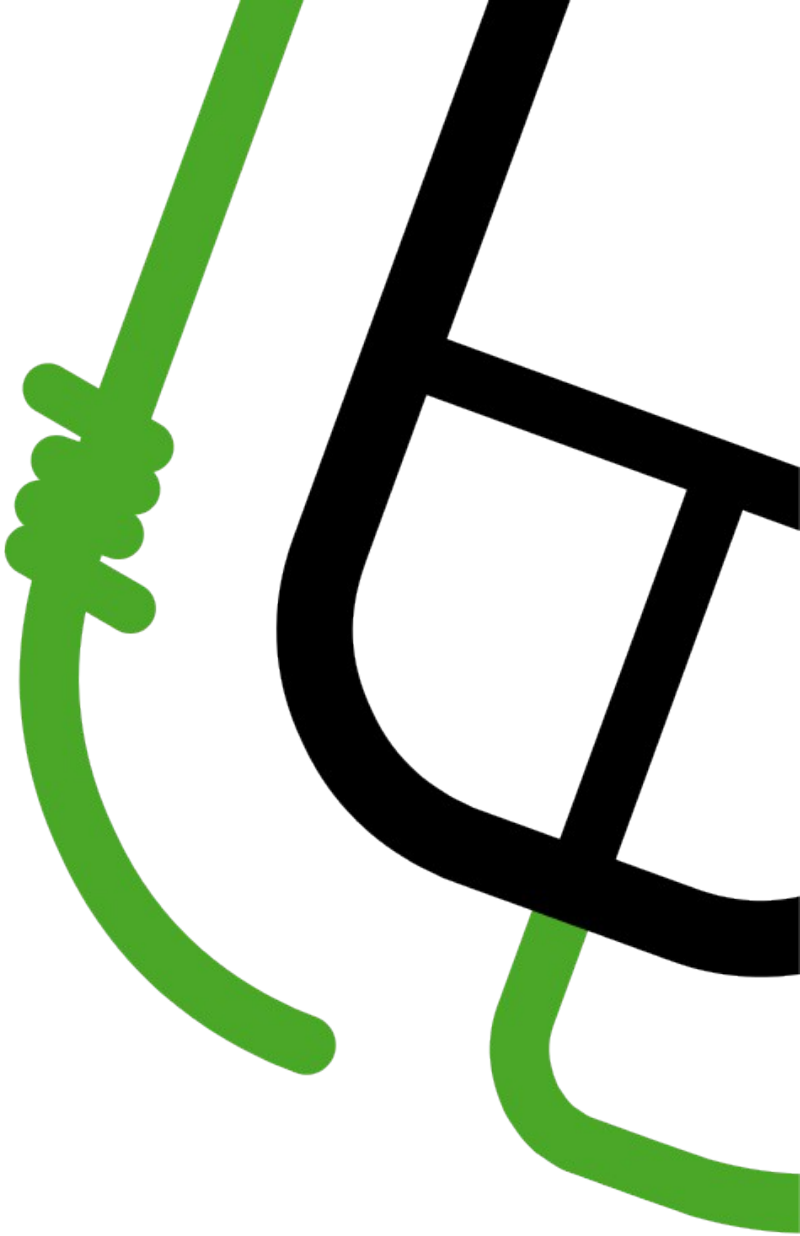
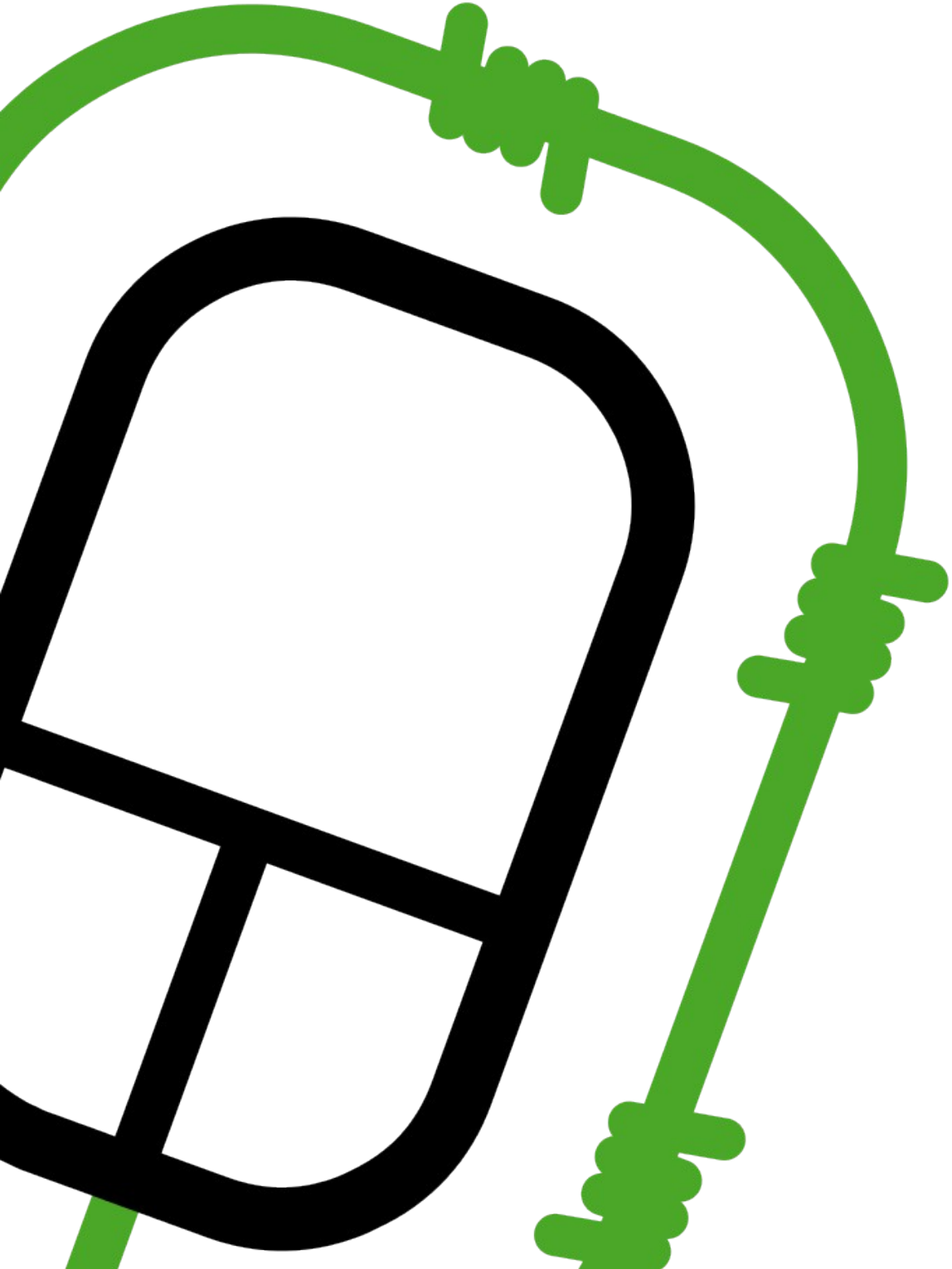
A LOOPHOLE IN DATA PROCESSING



Why the 'legitimate interests' test fails to protect the interests of users and the Regulation needs to be amended.

11 december 2012

BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN



Companies and governments are often processing personal data on the basis of the so-called 'legitimate interests' ground.

Research by Bits of Freedom shows that this ground has served as a basis for virtually unrestricted and unregulated forms of data processing without control of the user.

Bits of Freedom concludes that this ground should be curtailed in order to provide clarity and trust for users.

CONTENTS

BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

Bits of Freedom is a Dutch digital rights organization, focusing on privacy and communications freedom in the digital age. Bits of Freedom strives to influence legislation and self-regulation, on a national and a European level. Bits of Freedom is one of the founders and a member of European Digital Rights (EDRi).

Stichting Bits of Freedom
Postbus 10746
1001 ES Amsterdam

info@bof.nl

01. INTRODUCTION

43% of Internet users in the EU say they have been asked for more personal information than necessary when they wanted to access or use an online service, a

"70% of Europeans are concerned that their personal data held by companies may be used for a purpose other than that for which it was collected"

recent study by EuroBarometer concluded.[1] 67% of those users think that there is no alternative to disclose personal information if one wants to obtain products or services.[2] And an overwhelming 70% of Europeans are concerned that their personal data held by companies may be used for a purpose other than that for which it was collected.[3]

The perceived lack of adequate protection of personal data is the result of multiple causes, one of them being a loophole in the current data protection framework, Directive 95/46/EC ('the Directive').

Companies and governments may base the collection and subsequent processing of personal data on six legal grounds. One of these grounds is referred to as the 'legitimate interest'-ground. The term 'legitimate interest' is a collective term for a wide-scoped and vaguely-defined legal ground that is used for equally wide-scoped and often vaguely-defined data processing.

In order to maximize the potential of the Internet, users should be able to trust data controllers with their personal information. It is clear that such trust is currently lacking as a result of *inter alia* the broad legitimate interest ground. Our research shows powerful data controllers disregarding their users' interests and storing too much data. Bits of Freedom therefore proposes to amend the ground to improve online users' trust in data processing. These amendments are part of our work on the reform of the data protection framework ('the draft Regulation'), which started in January 2012 and is currently being debated in the European Parliament.

02. THE 'LEGITIMATE INTEREST' GROUND IS THE MOST OPEN TO INTERPRETATION

A data controller may process personal data if it has a legal ground for such processing. Most processing of personal data by online services is based on the grounds set out in in article 7(a), 7(b) or 7(f) of the Directive.

Firstly, processing is permissible when the user has unambiguously given his **consent** or when the information is necessary for the **performance of a contract**. These two grounds are relatively clear. However a remainder category for processing applies

"Users should be able to trust data controllers with their personal information. It is clear that such trust is currently lacking"

when the information is necessary for the purposes of the '**legitimate interest**' of the data controller. Only where such interests are overridden by the interests or fundamental rights and freedoms of the user, is

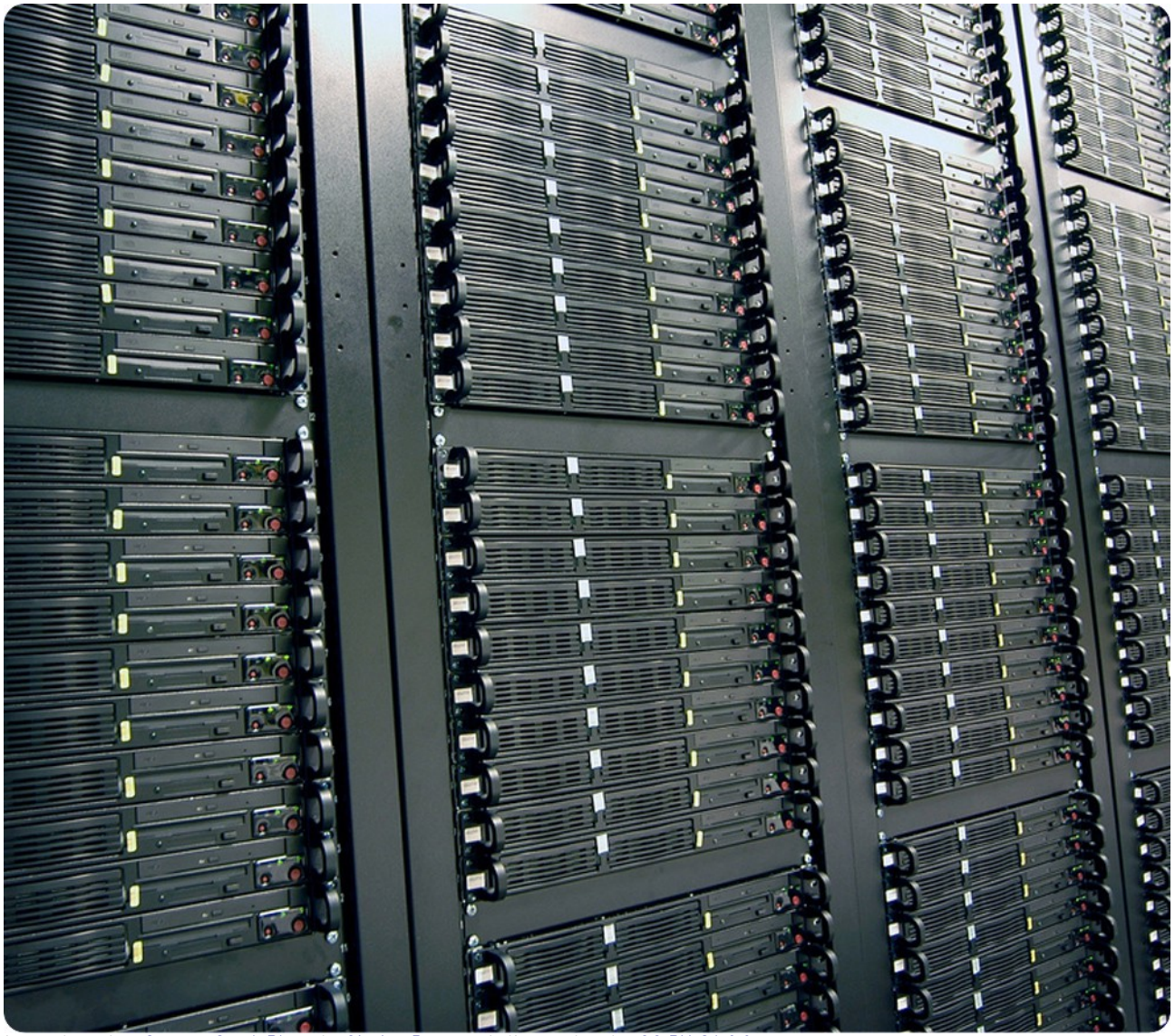
the processing not allowed. The concept of 'legitimate interest' is notably more unclear than the other two grounds. The current rules offer little guidance in determining what interests are 'legitimate' and when exactly they might be overridden by the interests of the user. This would not change under the proposed draft Regulation.

In our research we have studied striking cases of data processing supposedly using the 'legal interests' ground.

03. EXAMPLES OF ABUSE OF THE 'LEGITIMATE INTERESTS' GROUND

Google processes practically all users' information of any service in its 'legitimate interest'

One often occurring example of abuse is where the privacy policy is very broad and hard to understand. A clear example is Google's recent merging of data privacy policies across all its services. The merging leads to large databases allowing Google "to combine almost any data from any services for any purposes", according to a recent letter by the Article 29 Data Protection Working Party (WP29).[4] The legal ground which allows Google to collect and combine all these data is 'legitimate interest'. The first part of Google's



privacy policy states broadly what is being collected about you:

"[Google] may collect information about the services that you use and how you use them, like when you visit a website that uses our advertising services or you view and interact with our ads and content. This information includes: Device information (...) Log information (...) your search queries (...) your phone number, calling-party number, forwarding numbers, time and date of calls, duration of calls, SMS routing information and types of calls. Internet protocol address (...) system activity, hardware settings, browser type, browser language, the date and time of your request and referral URL (...) cookies that may uniquely identify your browser (...) Location information (...) Local storage (...) We also use cookies and anonymous identifiers when you interact with services we offer to our partners,"[5]

In short: practically all information that is possible to process via its services, Google may allegedly collect because it serves its 'legitimate interest'. This in itself is already problematic. It is hard to believe that all these data are strictly necessary for Googles 'legitimate interests'. The services from which Google can collect the data are also very broad and combining these data covers practically all services: Google Web Search, Google Apps, Google Drive, Chrome, YouTube, Maps, iGoogle, Toolbar, Mobile, Books, Image Search, Video Search, News, Picasa, Earth, Panoramio, Docs, Calendar, Sites, Talk, Translate, Sky, Blogger, Groups, Reader, Scholar, Alerts, Goggles, Music, Google Now, Google+, Android and of course Gmail.

Next to data collected from their own services, it collects data through third-parties that use Google's advertising services such as Google Analytics, AdSense, AdWords and the most used online tracker DoubleClick.[6]

Google states the purpose for collecting all these data is "to provide, maintain, protect and improve [services], to develop new ones and to protect Google and our users. We also use this information to offer you tailored content". Google's purpose for tracking you is "to improve your user experience and the overall quality of our services."[7]

These interests which Google states are vague and include potentially all sorts of data processing. Furthermore, the purpose is broad. Without a specific purpose, it is impossible to balance its legitimate interests against the fundamental rights and freedoms of its users.

Does Facebook really need all those personal data?

Facebook is notorious for collecting personal information of more than a billion of its users. The data includes all chats, comments, every invited event, location, likes, removed tags, deleted friends, messages, connections, devices users logged in with, other users who have logged in with that same device and profiles specific users are most interested in. Even after deletion of the user's account personal data is kept. Printing the information Facebook collects may result in 1,200 pages per user, as one researcher found out when he requested access to his data.[8] In November 2012 Facebook proposed to furthermore share data with all its affiliates as well.[9] Simultaneously Facebook proposed to change its Statement of Rights and Responsibilities to abolish the influence of users on Facebook's policy.[10]

Data processing in the interest of harvesting massive amounts of personal data for advertising interests can hardly be considered a 'legitimate interest' outweighing data protection rights of users, especially

without providing information on balancing these interests. According to the WP29, systems that process personal data with far-reaching consequences are not allowed; "even if the processing of personal data is based on the consent of the user, this would not legitimise the collection of data which is excessive in relation to a particular purpose."[11] Consent for this extensive gathering of data, generated by Facebook, is absent and this data is out of the user's control. Users cannot trust Facebook to make an adequate assessment of the necessity and purpose of processing of their personal data.

LinkedIn and Path; apps without trust

Apps also collect information or require permissions unnecessary for the described functionality of the apps.[12] There thus have been incidents of popular apps collecting irrelevant information.[13]

In fact, several times data controllers have been confronted with public outrage after collecting personal data. The most prominent cases were those of Path and LinkedIn.

Path sent full contact information of the contacts of its users to their servers without the users' knowledge or consent.[14] And when LinkedIn users installed its mobile app to connect LinkedIn profiles to meetings they would have, instead of just using the calendar entries of the user, the LinkedIn app harvested everything, including contact information, confidential notes and passwords. LinkedIn sent all this information to its servers.[15]

LinkedIn and Path collected these data without a clearly described purpose. Only when the issue was raised by investigative individuals, uproar followed and the apps discontinued their practices. Clearly a genuine 'legitimate interest' was absent and performing the balance test against the user's data protection rights failed. These apps kept collecting personal data from their users until they found the limits of public uproar and ran into trouble.

The bigger issue, of course, is that most data controllers which collect personal data without a 'legitimate interest' do not get caught. Illegitimate data processing stays unnoticed and the user is left in the dark.

These examples show that the 'legitimate interests' ground is often used as a pretext to escape the adequate and relevant safeguards for data collecting. When no other justification for the processing of

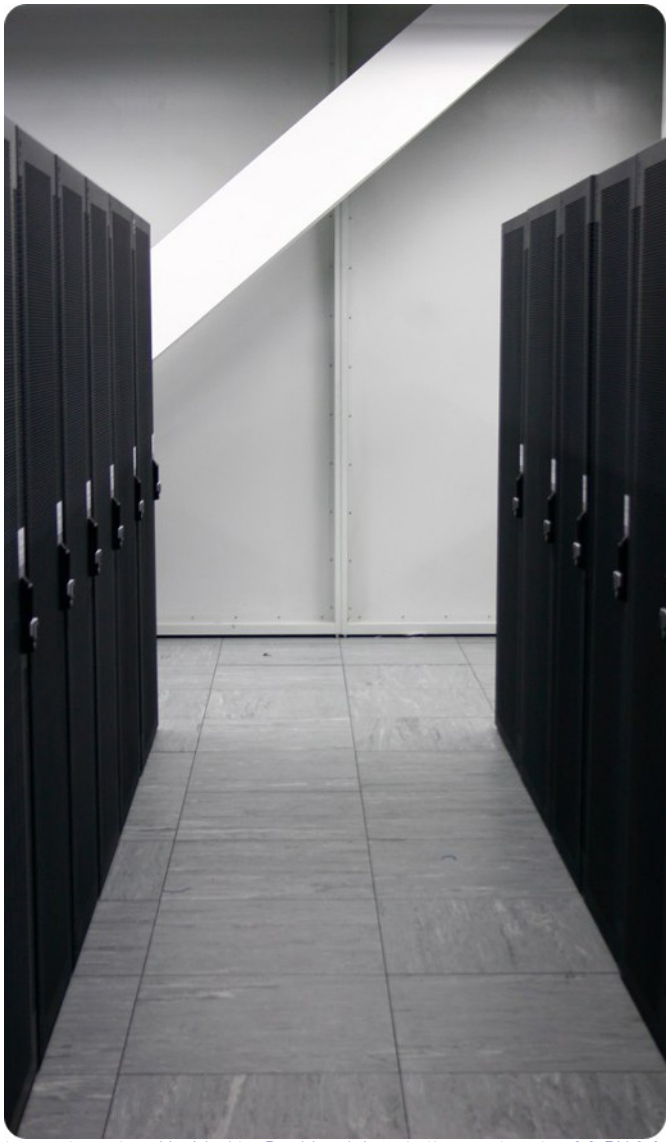
personal data remains, data controllers can currently rely too easily on their 'legitimate interest'. The specific purpose often remains unclear, which is in direct contrast with the principle of a specific and explicit purpose for data collecting. As a consequence, this ground enables the disregard of the principle of data minimisation.

04. THE 'LEGITIMATE INTEREST' CLAUSE CAUSES DISTRUST OF DATA CONTROLLERS

The 'legitimate interests' balance in article 6(1)(f) of the draft Regulation is not only a continuation of the uncertainty regarding the scope and lawfulness of certain forms of processing, but the 'legitimate interest' test also results in a serious distrust by the general public of data controllers.

The balance test favours the Data Controller

Currently 'legitimate interests' grant a basis for virtually unrestricted and unregulated forms of data processing. Data controllers are expected to perform their own balancing test and are consequently able to give more weight to their own interests than to those of their users. It is furthermore impossible to verify if the balancing test in fact took place, as few users have yet been able or willing to test reliance on this vague



criterion in court. The right to objection does not apply, with the exception of direct marketing and certain very narrowly described situations. This gives data controllers the freedom to let their interests prevail over the theoretical interests of users, causing a serious imbalance. Furthermore the test undermines the intention of the law to prescribe clear goals for data processing, since there is no incentive for providing a specific purpose for processing by the data controller.

The 'legitimate interests' clause impairs the control of users

In the context of massive data collection, almost any instance of data processing occurs in conditions of power imbalance. Such data processing is executed by data controllers that have advantages in expertise and resources. Effectively, the Proposal in its current form withholds information from the user; the balancing act happens out of sight, and this results in an unclear situation for users. This leads to a much lesser degree of individual control by the user.

The review of the balancing test is only done after processing

The 'legitimate interests' test is reviewed by courts, data protection authorities (DPAs) or as a result of public uproar only after the fact. Moreover, only rarely are any 'legitimate interests' reviewed in practice. And even when issues become known, they're hardly ever reviewed by DPAs. This is even more problematic, as these reviews are the only way to determine whether the balance tests have been rightly performed. It is unrealistic to expect the 'legitimate interests' test to be a tool for the protection of users' personal data, when the actual test is rarely checked.

The vague definition of 'legitimate interests' causes problems in the internationalised environment

The draft Regulation should ensure that a consistent approach is taken by DPAs. However, the various Member States may conduct the balance of 'legitimate interests' differently. This could lead to an inconsistent interpretation of the 'legal interest' clause and with a growing amount of companies relying on the clause, legal uncertainty will grow as well.

Using the 'legitimate interest' clause will only become more appealing

Letting data controllers weigh out their own interests against users data protection rights without public oversight is not a balanced system. Not surprisingly, data controllers would like to uphold their powerful position in this imbalanced situation. The strict safeguards in the other grounds for processing suggest that this loophole will be used by even more data controllers in the future, since the consent ground will become stricter, while the other grounds will stay the same.

In order to trust data controllers using the 'legitimate interests' clause, the clause needs to be improved. This means (i) restricting the use of 'legitimate interests' ground, (ii) accepting objection, when collecting on that basis (opt-out) and (iii) specifying the purposes of processing data.

05. SOLUTIONS TO IMPROVE TRUST IN DATA PROCESSING

The upcoming Regulation gives us a unique chance to restore trust in data processing; to keep data controllers from gathering too much personal data in the next decades. If the upcoming Regulation is not

amended, the lack of trust in data processing will persist and the situation will only deteriorate.

'Legitimate interests' ground

Article 6(1)(f), in its current form, offers data controllers a way to avoid many processing restrictions altogether.

Therefore, the Regulation needs a clear meaning of the 'legitimate interest' ground in the preamble.[16] Recitals should clarify what will be considered legitimate interests, define the notion of data subjects' interests in more detail and clarify how these interests should be weighed or verified.

If a data controller wishes to use 'legitimate interest' as a basis for processing, this must be separately and explicitly flagged to the data subject and the data processor should publish its grounds for believing that its interests override those of the data subject. Our proposed amendments introduce obligations on controllers to this effect.

Data subjects should be able to object (opt-out) from any form of processing based on 'legitimate interest'. Opting out must be directly effective and free of charge. Objection must be possible at any moment, including the moment of collection of personal data, via the same channel as the data are being collected or the direct marketing is being sent.[17]

Purpose limitation and necessity principles

Bits of Freedom plays an active role in the development of the new Data Protection Regulation. We have proposed a set of amendments that aim to protect citizens rights and to restore the balance between data controllers and internet users. This balance is essential to safeguard the fundamental right to privacy and to establish trust in online services that process users' personal data.

Next to our proposals related to the 'legitimate interests' ground, which are set out in this paper, we propose to strengthen the definitions of personal data and consent, prevent incompatible further use of personal data, guarantee transparency and control for data subjects and prohibit furtive profiling of internet users. In addition, we aim to strengthen the rules for privacy by design and default, improve data breach notifications and properly define the boundaries between data protection rules and other rights, such as the right to freedom of expression.

If you want to receive more information about Bits of Freedoms work on the data protection reform, please visit our website www.bof.nl, or contact Janneke Slöetjes: +31 6 17953655, janneke.sloetjes@bof.nl

1. Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union, REPORT, Fieldwork: November – December 2010, Publication: June 2011, p. 54: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf
2. Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union, REPORT, Fieldwork: November – December 2010, Publication: June 2011, p. 28: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf
3. Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union, REPORT, Fieldwork: November – December 2010, Publication: June 2011, p. 146: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf
4. Letter to Google by ARTICLE 29 Data Protection Working Party, 16 October 2012, p. 2: http://www.cnil.fr/fileadmin/documents/en/20121016-letter_google-article_29-FINAL.pdf
5. Google's Privacy Policy, last modified 27 July, 2012: https://www.google.nl/intl/en/policies/privacy/
6. C.J. Hoofnagle & N. Good, The Web Privacy Census, October 2012: http://law.berkeley.edu/privacycensus.htm
7. Google's Privacy Policy, last modified 27 July, 2012: https://www.google.nl/intl/en/policies/privacy/
8. Europe-v-facebook.org: http://www.europe-v-facebook.org/EN/Data_Pool/data_pool.html
9. Facebook's Redline of Proposed Data Use Policy, November 2012: https://fbcdn-dragon-a.akamaihd.net/cfs-ak-ash3/676592/128/460431350669077_1584612884.pdf
10. Facebook's Redline of Proposed SRR, November 2012: https://fbcdn-dragon-a.akamaihd.net/cfs-ak-prn1/676641/517/256230001169573_786305489.pdf
11. Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, Adopted on 13 July 2011, p. 7: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf
12. Permissions to actual app functionality, Juniper Networks, 30 October 2012: http://forums.juniper.net/t5/Security-Mobility-Now/Exposing-Your-Personal-Information-There-s-An-App-for-That/ba-p/166058
13. Your Apps Are Watching You, Wall Street Journal, 17 December 2010: http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html
14. Ars Technica, Path addresses privacy controversy, but social apps remain a risk to users, 12 February 2012: http://arstechnica.com/gadgets/2012/02/path-addresses-privacy-controversy-but-social-apps-remain-a-risk-to-users/
15. NY Times Bits, LinkedIn's Leaky Mobile App Has Access to Your Meeting Notes, 5 June 2012: http://bits.blogs.nytimes.com/2012/06/05/linkedins-leaky-mobile-app-has-access-to-your-meeting-notes/
16. Article 29 Data Protection Working Party, Opinion 01/2012 on the data protection reform proposals, Adopted on 23 March 2012, p. 7: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf
17. European Digital Rights, Protect My Data: EDRi's comments on the Data Protection Reform: http://protectmydata.eu/topics/limitations/ and http://protectmydata.eu/articles/articles-1-10/article-6/