Legal Notice
All information included in this document is subject to change without notice. The Members of the IWT SBO SPION project make no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The Members of the IWT SBO SPION project shall not be held liable for errors contained herein or direct, indirect, special, incidental or
consequential damages in connection with the furnishing, performance, or use of this material.

**The IWT SBO SPION Project**

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Participant name</th>
<th>Country</th>
<th>Department</th>
<th>Participant role</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>KU Leuven</td>
<td>BE</td>
<td>COSIC/ESAT</td>
<td>Coordinator</td>
</tr>
<tr>
<td>2</td>
<td>KU Leuven</td>
<td>BE</td>
<td>DISTRINET</td>
<td>Partner</td>
</tr>
<tr>
<td>3</td>
<td>KU Leuven</td>
<td>BE</td>
<td>DTAI</td>
<td>Partner</td>
</tr>
<tr>
<td>4</td>
<td>KU Leuven</td>
<td>BE</td>
<td>ICRI</td>
<td>Partner</td>
</tr>
<tr>
<td>5</td>
<td>Vrije Universiteit Brussel</td>
<td>BE</td>
<td>SMIT</td>
<td>Partner</td>
</tr>
<tr>
<td>6</td>
<td>University of Ghent</td>
<td>BE</td>
<td>OWK</td>
<td>Partner</td>
</tr>
<tr>
<td>7</td>
<td>Carnegie Melon University</td>
<td>USA</td>
<td>Heinz</td>
<td>Partner</td>
</tr>
</tbody>
</table>

**Contributors**

<table>
<thead>
<tr>
<th>Name</th>
<th>Organisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Brendan Van Alsenoy</td>
<td>KU Leuven, ICRI</td>
</tr>
<tr>
<td>2 Eleni Kosta</td>
<td>KU Leuven, ICRI</td>
</tr>
<tr>
<td>3 Jos Dumortier</td>
<td>KU Leuven, ICRI</td>
</tr>
</tbody>
</table>
Table of Contents

I. Introduction ........................................................................................................................................4

II. Role of privacy notices ..................................................................................................................5

  2.1 Transparency ............................................................................................................................6
  a. Fairness ......................................................................................................................................7
  b. Knowledge is power ...............................................................................................................8
  c. Damage control ....................................................................................................................8
  d. Purifying effect ......................................................................................................................9
  e. Accountability ........................................................................................................................9

  2.2 Legitimacy ..................................................................................................................................11
  a. 'Informed' consent .................................................................................................................11
  b. A preference for consent? ......................................................................................................13

III. Limitations of the current approach .........................................................................................16

  3.1 "Notice skepticism" .................................................................................................................16
  a. Rational ignorance ................................................................................................................16
  b. Cognitive limitations ............................................................................................................17
  c. Low signal-to-noise ratio .......................................................................................................17

  3.2 Overreliance on consent ..........................................................................................................18
  a. Privacy as a societal good .....................................................................................................18
  b. Responsibilization ..............................................................................................................19
  c. Rational choice fallacies ......................................................................................................19
  d. Fallacy of sufficiency ...........................................................................................................20
  e. Other legitimate interests .....................................................................................................21

IV. Going forward ..........................................................................................................................21

  4.1 Disentangling 'notice & choice' ............................................................................................21

  4.2 Side-stepping the autonomy trap .........................................................................................23
  a. Legitimacy of interest vs. informed consent .......................................................................23
  b. Reinstating fairness ..............................................................................................................24
  c. Accepted practices ...............................................................................................................26

  4.3 Minding the gap .......................................................................................................................27

  4.4 Complementary initiatives .....................................................................................................29
  a. Layering notice .....................................................................................................................29
I. Introduction

Privacy policies are important. Or so we are led to believe, given the volume of news articles and blog posts alerting us to the privacy policy updates of today's internet giants.\(^1\) Regulators think these policies are important too, judging by the amount of resources they spend reprimanding companies for failing to meet relevant requirements of transparency and/or specificity.\(^2\) But what about the individuals concerned; those that actually use the services to which these policies pertain? Literature abounds with empirical evidence suggesting mainly one thing: most of them don't care.\(^3\)

So what now? Abandon the current approach or stay the course? The goal of this paper is to clarify, from a European perspective, the current discourse regarding the (in)utility of privacy policies. But before we start, we need to touch briefly on a terminological matter. From this point on, we will refer to 'privacy notices' instead of 'privacy policies'; simply because the term 'privacy policy' can be used to refer to two very different things. On the one hand, there are those instruments which intend to inform individuals of the processing of their personal data, their rights as data subjects, as well as any other information required by data protection or privacy legislation. They can typically be found by clicking on the 'privacy policy' links displayed at the bottom of webpages; or alongside terms and conditions when registering with a service provider for the first time. On the other hand, the term 'privacy policy' is also frequently used in reference to documents which are internal to an organization. In this context, a 'privacy policy' refers to an instrument in which an organization documents the objectives, rules and/or controls it has adopted in order to satisfy data protection and privacy requirements. By referring to 'privacy notices' rather than 'privacy policies', we aim to avoid terminological confusion in this respect.

---


Two qualifications must be made regarding the scope of this paper. First, this paper mainly focuses on the use of privacy notices in an online environment. Second, our analysis of the current and future role of privacy notices is geared towards the European Data protection framework, particularly EU Directive 95/46/EC.  

The remainder of this paper is structured as follows. We start by identifying the role that privacy notices (can) play under the European data protection framework today. Next, we summarize the main critiques regarding the use of privacy notices in practice. From this analysis we then distill a number of a number of requirements and recommendations regarding the future use of privacy notices. Finally, by way of conclusion, the main findings of this paper shall be summarized, accompanied by an outline of areas of future research.

II. Role of privacy notices

Contrary to popular belief, EU data protection law does not require organizations to display a privacy notice on their websites – or at least not as such. Such notices are, however, seemingly logical by-products of this legislation. A quick glance at the provisions of Directive 95/46/EC suggests that privacy notices can serve mainly two purposes. First, they might serve to acquit the data controller of his transparency obligations under articles 10-11 of the Directive. These articles stipulate that data controllers shall provide their data subjects with certain specified items of information, as well as any further information which may be necessary to ensure fairness. Second, in cases where the data controller seeks to rely upon the ‘informed consent’ of the data subject in order to justify the processing, privacy notices could, in principle, also serve to secure the legitimacy of processing (articles 7-8 of the Directive). After all, the requirement that consent has to be ‘informed’ “starts from the assumption that it needs to be fully understandable to the data subject what will happen if he decides to consent to the processing of his data”. Both these aspects will be elaborated over following subsections.

---

6 The Directive defines a ‘controller’ as the entity who alone, or jointly with others, ‘determines the purposes and means’ of the processing (article 2(d)). Within the regulatory scheme of the Directive, the controller is the entity that carries primary responsibility for ensuring compliance with the substantive provisions of the Directive. For a critical analysis see B. Van Alsenoy, ‘Allocating responsibility among controllers, processors, and “everything in between”: the definition of actors and roles in Directive 95/46/EC’, Computer, Law & Security Review 2012, vol. 28, p. 25-43.  
2.1 Transparency

Articles 10 and 11 of the Directive specify which types of information data controllers must provide to data subjects with regards to the processing of their personal data. At the outset, these provisions make a distinction between two scenarios: one in which the information is obtained directly from the data subject (art. 10), and one in which the information is collected indirectly (i.e. from an entity other than the data subject) (art. 11). The notice obligations of the controller in each scenario are largely similar; the main differences concern (a) the moment by which notice must be provided and (b) the exemptions to the notice obligation. The combined effect of these provisions is essentially the following: as a rule, each data subject must be informed of at least the identity of the controller (and, if applicable, of his representative) and the purposes of the processing. In addition, the Directive offers Member States the option to require data controllers to provide the data subject with supplemental information ‘in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject’. Such additional information can refer to the recipients or categories of recipients of the data, information with regard to the existence of the right of access, the right to rectify inaccurate data, etc.

In order to gain a better understanding of the controller’s duty to inform as set out by articles 10-11, it is useful to explore the rationale behind these provisions. As a general matter, there can be little dispute that the general purpose of privacy notices is to render the processing of

---

8 In case of direct collection notice must in principle be provided at the moment of collection (or earlier) (art. 10). In case of indirect collection, notice must in principle be provided ‘at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed’ (art. 11, 1).

9 In case of indirect collection, art. 12 provides exemptions to the notice obligation where the processing is being carried out ‘for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law.’ See also M.-H. Boulanger, C. de Terwagne, Th. Léonard, S. Louveaux, D. Moreau and Y. Poulet, ‘La protection des données à caractère personnel en droit communautaire’, Journal des Tribunaux Droit Européen 1997, vol. 40, p. 150-151.

10 The use of plural “purposes”, in Articles 10-11, implies that the data subject has to be informed not only about the main purpose to be accomplished, but also about any secondary purposes for which the data will be used. See also D. Korff, ‘Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments: Country Study A.4 – Germany’ (2010), p. 33, available online at http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_country_report_A4_germany.pdf (last accessed on 23 March 2011), commenting on the relevant provision of the German Data Protection Act, which uses the term “purposes” as well.

11 Art. 10-11, 1, c) (emphasis add).

12 Member State laws vary considerably with regard to the kinds of information which must actually be provided in order to ensure fairness of processing. Sometimes the examples given in the are repeated, other times somewhat different examples are included, and sometimes there are no examples at all. (see Article 29 Data Protection Working Party, ‘Opinion on More Harmonised Information Provisions’, WP100, 25 November 2004, p. 3, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_en.pdf (last accessed 30 June 2012).
personal data ‘more transparent’ towards the data subject.\textsuperscript{13} As for the deeper regulatory logic underlying this obligation of transparency, various motives have been proffered. While these justifications are often closely interrelated, they each reveal interesting presumptions regarding both the goals of data protection law as a whole as well as the envisaged role of the individual towards the processing of his or her personal data. Broadly speaking, the main justifications assigned to the notice obligations of data controllers are that they:

a) promote fairness;

b) help to compensate knowledge asymmetries;

c) enable data subjects to contest abusive data practices;

d) have a ‘purifying’ effect on data controller’s actual practices; and

e) enhance the accountability of data controllers.

\subsection{a. Fairness}

Most scholars consider transparency of processing a logical extension of the requirement that personal data shall be processed ‘fairly and lawfully’ (art. 6, 1 a).\textsuperscript{14} Fairness of processing is an overarching (or ‘primary’\textsuperscript{15}) principle of data protection law; in that it is a (or perhaps even ‘the’) generic principle which has provided the foundation for other data protection requirements. In the context of transparency vis-à-vis data subjects, fairness has mainly two dimensions. First, it offers data subjects (relative) protection against surreptitious collection and further processing of their personal data.\textsuperscript{16} The basic notion here is that, even if one doesn’t have a real say in the matter, an individual should, in principle\textsuperscript{17}, at least be put ‘on notice’ when his or her personal data is being processed (e.g., “I should have the right to know when I’m being watched/profiled”). Second, fairness also shields data subjects against deception by the data controller as to the nature and purposes of the data processing.\textsuperscript{18} Specifically, it protects the data subject from ‘unfair and deceptive practices’ by the data controller regarding the processing of their personal data (e.g., misrepresentation, omission of essential information).\textsuperscript{19}

\footnotesize


\textsuperscript{15} L.A. Bygrave, \textit{o.c.}, 58.

\textsuperscript{16} \textit{Id}. The Directive itself provides for several exceptions to the notice provision in articles 10 and 11. In addition, processing operations falling outside of the scope of the Directive all together (see article 3, 2) are of course also not subject to this notice obligation.

\textsuperscript{17} Obviously derogations may be necessary (e.g., in the course of undercover operation). However, these derogations must be established pursuant to the provisions of the Directive (unless of course, the processing operation falls outside of its scope all together).

\textsuperscript{18} L.A. Bygrave, \textit{o.c.}, 58.

\textsuperscript{19} The term ‘unfair and deceptive practices’ is a term of art derived from section 5 of the Federal Trade Commission Act (5 U.S.C. §§ 41-58); thus stemming from the field of consumer protection. More and more,
b. Knowledge is power

A second justification for the controller's notice obligation is derived from the finding that Directive 95/46/EC aspires to do more than just safeguard informational privacy: it also seeks to counter the 'information asymmetries' between individuals and controllers. The central idea here is that 'knowledge is power': because data controllers stand to gain power over data subjects (through the knowledge they acquire from the processing of their personal data); data subjects should in turn be placed in a position to learn more about controller's practices. While the duty to inform data subjects is only one of several transparency obligations, it may nevertheless provide the individuals concerned with a first insight into the controller's data processing operations. In other words, prior notice can be seen as a first, albeit relatively modest, step towards 'leveling the playing field' between data subjects and controllers in terms of the knowledge acquired through processing.

c. Damage control

A third justification for the controller's notice obligation concerns the exercise of data subject rights. Articles 12 through 15 of the Directive outline a number of data subject rights, which include a right of access (art. 12, a), a right to request rectification and/or erasure (art. 12 b), and a right to object to the processing (article 14). Arguably, if a data subject is unaware of the processing of his or her personal data, he or she will not be able to scrutinize the processing and make a determination as to whether or not to object to the processing, whether to submit a request to see the data amended, etc. While it should not be excluded that data subjects may learn of the processing through other means (e.g., when served a personalized ad, when rejected for a loan on the basis of past credit history), prior notice may already provide a first opportunity to contest (and ideally prevent) abusive record holding practices. Here, as with other data subject rights, the underlying idea is that data individuals should be able to have a measure of influence over the processing of their personal information by other individuals or practitioners and scholars in the EU are looking into how this approach might inform interpretation of the fairness principle in DP law – see e.g. ; A. Kuczerawy, and F. Coudert, 'Privacy Settings in Social Networking Sites: Is It Fair?' in S. Fischer-Hübner et al. (Eds): Privacy and Identity Management for Life, 6th IFIP AICT 352, 2011, p. 231-243.


22 See T.Z. Zarsky, l.c., 998. See also A. Rouvroy and Y. Poulet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy', in S. Gutwirth, Y. Poulet, P. De Hert, C. de Terwangne and S. Nouwt (eds.), Reinventing Data Protection, 2009, Springer, p. 69 ("Data protection regimes were thus designed [...] in order to better balance informational power.")


organizations. In order for individuals to be able to take such an initiative, they first need to be aware of 'what data is being held where', for which purpose, and which data controller to contact.

d. Purifying effect

In a piece perhaps more infamous than The Right to Privacy, Brandeis lauded the regulatory effect of transparency as follows:

“Publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants; electric light the most efficient policeman.”

While this quote was part of Brandeis’ call for regulation of the financial markets in the early 1900’s, its basic tenet has been echoed in public discourse regarding freedom of information ever since. The general notion is that transparency has a ‘purifying effect’ on the actions of individuals, companies and governments alike. Once subject to the panoptic view of ‘the other’, the theory goes, behavior self-corrects to conform with expected behavior. Along the same lines, several scholars have suggested that the requirement to disclose may also help to improve privacy practices, because it may lead companies ‘to self-examine and professionalize’.

e. Accountability

A final recurring justification for the notice obligation of data controllers is accountability. Historically, data protection laws emerged as a means to help protect individuals from abuses of power resulting from the processing of their personal data. These laws instituted a variety of procedural safeguards designed to protect individuals’ privacy and to promote accountability

26 Id.
30 In the same correspondence to his fiancé Brandeis also added: “If the broad light of day could be let in upon men's actions, it would purify them as the sun disinfects.” (Id.)
31 See also M. Foucault, Discipline and Punishment, New York, Vintage Books, 1995, p. 202-203 ("He who is subjected to a field of visibility, and who knows it, assumes responsibility for the constraints of power; he makes them play spontaneously upon himself; he inscribes in himself the power relation in which he simultaneously plays both roles; he becomes the principle of his own subjection").
data controllers.\textsuperscript{35} From this perspective, it may be argued that the transparency obligations embodied by the Directive essentially mainly serve to enable or enhance accountability.\textsuperscript{36} After all: ‘what is in the dark cannot be scrutinized’.\textsuperscript{37}

Accountability is a concept with many dimensions.\textsuperscript{38} It has been characterized as being an ‘elusive’ and even ‘chameleon-like’ concept, because it can mean very different things to different people.\textsuperscript{39} In its most basic meaning, accountability refers to the existence of a relationship whereby one entity has the ability to call upon another entity and demand an explanation and/or justification for its conduct.\textsuperscript{40} Such relationships are typically found in contexts where an entity has been vested with certain powers and/or responsibilities which need to be ‘checked’ in order to mitigate risks of abuse or other undesirable outcomes.\textsuperscript{41}

So where do privacy notices fit into all this? Privacy notices do not create an accountability relationship per se, but rather have the potential of contributing to the efficacy of such relationships. By requiring controllers to openly disclose their data processing practices, these practices can be subjected to further scrutiny. If drafted properly, a privacy notice can even provide the means for assessing compliance on a post fact basis (cf. the requirement of specificity in both the purpose specification principle and the definition of consent).\textsuperscript{42} In other words, privacy notices can provide reference documentation through which a controller’s activities may be scrutinized. The duty to inform thus enhances, at least in theory, the accountability of data controllers vis-à-vis data subjects, regulators, and society at large.


\textsuperscript{38} See e.g. J. Koppell, ‘Pathologies of Accountability: ICANN and the Challenge of “Multiple Accountabilities Disorder”’, \textit{Public Administration Review} 65 (2005), 94-99; R. Mulgan, ‘“Accountability”: an ever-expanding concept?’, \textit{Public Administration} 78 (2000): 555-556


\textsuperscript{40} See M. Bovens, ‘Analysing and Assessing Accountability: A conceptual Framework’, 449-450. Bovens defines accountability as a (social) ‘relationship between an actor and a forum, in which the actor has an obligation to explain and justify his or her conduct, the forum can pose questions and pass judgment, and the actor may face consequences’.


\textsuperscript{42} See also \textit{infra} section 4.1. Accountability by way of notice is perhaps clearest in the United States, where the Federal Trade Commission’s enforcement actions under section 5 of the FTCA are directly correlated to the statements made by companies (as failure to adhere to stated practices is considered an “unfair” or “deceptive” trade practice). See D. L Baumer, J. B. Earp, J.C. Poindexter, ‘Internet privacy law: a comparison between the United States and the European Union’, \textit{Computers & Security} 2004, vol. 23, p. 402.
2.2 Legitimacy

Under Directive 95/46/EC, processing of personal data may only take place to the extent that there is a ‘legitimate ground’ justifying the processing. The grounds recognized by the Directive are enumerated (exhaustively) in articles 7. Here, data subject consent is listed as the first of several bases through which the processing may be rendered legitimate.\(^\text{43}\) In order for data subject consent to provide a legitimate basis for the processing, several requirements must be met. Specifically, the consent must be\(^\text{44}\)

1. **unambiguous**: the action by the data subject can only be understood as an expression by the data subject of his agreement that personal data relating to him will be processed;\(^\text{45}\)
2. **specific**: the consent of the data subject must relate to a well-defined, concrete situation, in which the processing of his personal data is envisaged;\(^\text{46}\)
3. **freely given**: the consent must be a voluntary decision, by an individual in possession of all his faculties, taken in the absence of coercion of any kind, be it social, financial, psychological or other;\(^\text{47}\) and
4. **informed**: the consent must be based upon an appreciation and understanding of the facts and implications of this action.\(^\text{48}\)

### a. ‘Informed’ consent

\(^{43}\) Data subject consent also figures in article 8, which concerns the processing of special categories of data. This provision stipulates a general prohibition which needs to be ‘lifted’ before the processing can be justified. In practice, the distinction is not always very clear the basis for ‘lifting the prohibition’ and ‘rendering the processing legitimate’ may be by and large the same. However, the distinction is quite clear is article 8, 2, e), which lifts the general prohibition of processing special categories of data for data ‘made manifestly public by the data subject’. The public nature of such data does not exempt the controller from the obligation of securing a legitimate basis for the processing under article 7. Similar considerations apply with respect to the role of consent for cross-border transfers under article 26 (consent may serve to lift the general prohibition of transfer to jurisdictions which have not (yet) been subject of an adequacy finding, but this is in principle independent of the legitimacy of processing).

\(^{44}\) See art. 2, h juncto 7, a of the Directive.

\(^{45}\) D. De Bot, *Verwerking van Persoonsgegevens* ['Processing of Personal Data'], Kluwer, Antwerpen, 2001, p. 129. Where special categories of data are involved, article 8, 2, a of the Directive specifies that the consent of the data subject must be ‘explicit’ rather than ‘unambiguous’. Again, this is a subtle distinction which is not always perceptible in practice. The main difference is that ‘absence of ambiguity’ still allows for inference from other (affirmative) actions, whereas ‘express’ consent does not allow for inference of any kind (but rather requires an indication of wishes specifically in relation to the processing of the data in question). See Article 29 Working Party, Opinion 15/2011 on the definition of consent, WP187, 13 July 2011, p. 25 and 35. See also E. Kosta, *Unravelling consent in European data protection legislation: a prospective study on consent in electronic communications*, Doctoral Thesis, Submitted 1 June 2011, p. 203 et seq.


In cases where the data controller seeks to rely upon the consent of the data subject in order to justify the processing, use of privacy notices may in principle help secure the legitimacy of processing.\(^{49}\) However, the requirement that this consent must be 'informed' does not exhaust itself through a declaration that processing of personal data will take place.\(^{50}\) In its Opinion on the definition of consent, the Article 29 Working Party specified four requirements concerning the information which a controller must provide prior to obtaining data subject consent. These requirements concern (a) the object of the information, (b) the level of detail, (c) the quality of information and (d) the accessibility of information. While the Working Party identified these requirements as prerequisites for the validity of consent (i.e., to satisfy the requirement that consent is 'informed'), similar requirements in principle also apply in relation to the information to be provided under articles 10 and 11 of the Directive.\(^{51}\)

**Object**

According to the Article 29 Working Party, the information provided “should address the substantive aspects of the processing that consent is intended to legitimize”.\(^{52}\) As a general rule, these ‘substantive aspects’ coincide with the information listed in articles 10 and 11 (cf. supra), but the final assessment should be made on a case-by-case basis.\(^{53}\) In the end, the data subject should be provided with adequate information regarding all aspects of the processing which might reasonably be considered as having a determinative influence for the granting or withholding of consent.

**Level of detail**

The level of detail with which information should be provided is intrinsically related to the requirement of specificity of consent. Pursuant to the requirement of specificity, consent must be given in relation to clearly defined processing operations, which allow the data subject to understand the precise scope and consequences of the processing.\(^{54}\) As a result, a ‘blanket’ or ‘open-ended’ consent, whereby the data subject consents ‘to all legitimate uses’, is deemed not to be acceptable.\(^{55}\) The standard for assessing whether the requisite level of specificity has been met is, once again, one of reasonableness: could the data subject reasonably anticipate such processing to take place in light of the information provided?\(^{56}\)

**Quality**

\(^{49}\) Privacy notices provided with the view of obtaining data subject consent have also been referred to as ‘consent notices’, i.e. notices aimed at obtaining the data subject’s informed consent for certain data processing activities, e.g. by ticking a box. (N. Robinson et al., ‘Review of the European Data Protection Directive (RAND - Technical Report), prepared for the UK Information Commissioner’s Office’ (2009), p. 28-29, available online at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive.pdf (last accessed on 23 March 2011).


\(^{53}\) Id. (“This would normally cover the elements of information listed in article 10 of the Directive, but will also depend on when, and the circumstances in which, consent is requested”) *(Id.)*


\(^{55}\) Ibid, p. 17.

\(^{56}\) Ibid, p. 17-18.
The information provided by the controller should be adequate, accurate, clear and understandable. Controllers should use plain text and avoid the use of jargon as much as possible. The quality of information shall be assessed in light of the context in which it is provided; whereby the bottom line is that an average individual confronted with the notice (user, patient, citizen, ...) should be able to understand it.

**Accessibility**

The information providing the basis for consent should be given directly to the individuals concerned (i.e., it is not enough for the information to be ‘available somewhere’). Furthermore, the transmitted information must be clearly visible (in terms of type and size of fonts), prominent and comprehensive. In other words, the Article 29 Working Party expects controllers to ‘push’ the information to data subjects in a conspicuous manner before soliciting their consent.

**b. A preference for consent?**

As indicated earlier, data subject consent is just one of several grounds through which processing of personal data may be rendered legitimate under Directive 95/46. In principle, there is no prioritization among these grounds: all grounds have equal value. In practice, however, the majority of online services appear to rely on the consent of its users in order to justify the processing of personal data. Consent, as an expression of individual autonomy, is traditionally accorded great value in privacy and data protection discourses. Increasingly, however, the effectiveness and desirability of this approach is being questioned. Before delving into these criticisms, it is worth outlining some of the main factors which contribute to the preferential treatment of ‘informed consent’ as a means to justify processing in practice.

*Waivering*

Many privacy notices are written with the ‘aim of protecting the company against potential lawsuits rather than with the intention of providing clear and readable information to the data subject’. By requiring users to consent to these notices before accessing a service, the company in question hopes to shield itself against subsequent legal action for its use of data. After all, if an individual, after having been informed of all the potential uses of his or her data, decides to accept these terms and proceeds to access the service, he or she should not complain afterwards, should they?

**Intrinsic force?**

---


59 *Id.*

60 *Id.*

61 *Id.*


A second factor contributing to the widespread use of consent is its ‘aura’ of intrinsic force. Contrary to the other grounds for processing, reliance upon data subject consent does not, by itself, involve a substantive justification of the processing. Specifically, it does not involve any reference to external criteria or factors (such as ‘legal obligation’, ‘contract’, or ‘vital interests’) against which the necessity or adequacy of the processing must be measured. As Brownsword puts it:

“The attraction of consent as a justifying reason is not hard to understand. Quite simply, not only does consent provide the recipient […] with a complete answer against the consenting agent […] it does so without having to engage contestable substantive justifications – or at any rate, such ‘on the merits’ justifications do not have to be offered to the consenting party (even if such substantive justifications cannot be altogether avoided in relation to third parties).

As such, consent functions as a procedural rather than substantive justification. The legitimacy of processing is not derived from its ‘rightness’ or ‘appropriateness’, but rather from the authorization granted by the data subject. In doing so, the task of ensuring legitimacy is seemingly reduced from a substantive evaluation to a mere box-ticking exercise.

### Jurisdictional preferences

Even though Directive 95/46 does not prioritize among the grounds of legitimacy, data subject consent is perceived as a preferred ground in certain jurisdictions. For example, the Czech Republic, France, Greece and Portugal, have established consent as the primary ground based on which the processing of personal data is legitimate; whereby all other grounds are seen as exceptions to consent. Germany, Austria and Spain also give consent primary status, alongside processing based on a law processing to fulfill a legal obligation. This approach does not necessarily mean that the other grounds for processing do not enjoy full legal force; it merely signifies that the aforementioned grounds are seen as ‘first among equals’. In practice, it may also imply that data controllers are encouraged by their national regulators to justify the processing on one of the primary grounds, before opting for a ‘secondary’ one.

### Extra-EU influence

When seeking to understand the prevalence of consent as a means to ensure legitimacy in the online context, one should also consider the impact of regulatory influences outside of the EU. In this respect, it is worth noting that the U.S. Federal Trade Commission (FTC) has since long

---

65 Ibid, 88.
66 Id.
67 As we will demonstrate later, however, data subject consent does not absolve the controller from his obligation to specify a legitimate purpose and to limit the processing to that which is necessary to achieve that purpose. Cf. infra; 4.2.
70 Id.
encouraged private companies to develop notices describing their information collection and use practices. Furthermore, even though there is no generally applicable legislation which requires U.S. companies to adopt privacy notices, several pieces sector-specific legislation (such as HIPAA, GLB or COPPA) do require such notices.\textsuperscript{71}

III. Limitations of the current approach

In the previous section we established, at a high level, the theoretical underpinnings of the controller’s duty to inform. We also identified the role that the provision of such information might play in ensuring the legitimacy of processing, as well as the main drivers for data controllers to rely upon informed consent as a means to justify the processing. The resulting online practice, whereby users are required to agree to lengthy privacy notices before accessing a service, is subject to increasing criticism. In this section, we will outline the main arguments advanced against the use of privacy notices, specifically under a ‘notice and choice’ model. The aim of this section is not to refute or subscribe to any of these arguments in particular, but rather to draw up an inventory of the prevalent rhetoric in scholarly and public discourse on this topic.

3.1 “Notice skepticism”

Despite the theoretical value of privacy notices, the efficacy of existing notice obligations is increasingly questioned. Three vulnerabilities in particular are often cited:

a) most individuals choose not to read, or merely gloss over privacy notices;

b) privacy notices are often drafted in a way that make them difficult to understand and/or evaluate; and

c) the degree of abstraction in privacy notices is such that it makes them relatively meaningless.

a. Rational ignorance

It is no secret that many people choose not to read privacy notices. But why? A first explanation is that they simply have better things to do. In our online experience, we are creatures with limited resources, who must decide how to best allocate our time. In making this decision, we

---

72 The criticisms presented here have in first instance been directed towards the ‘notice & choice’ approach to data protection, which has historically been advocated for by the U.S. Federal Trade Commission (see also supra; section 2.2). However, similar considerations also apply within the EU, at least to the extent that the practical reality is such that most online service providers appear to rely upon data subject consent.

73 The term “notice skepticism” was coined by R. Calo, ‘Against Notice Skepticism in privacy (and elsewhere)’, l.c., p1027 et seq.


arguably apply a ‘welfare-maximizing’ rationality, much like the one we apply in so many other aspects of life. For many of us, the cost of reading privacy notices is simply perceived as being too high. For others, the perceived benefit of reading notices is simply too low. As a result, one can argue that the majority of internet users choose to maintain a ‘rational’ ignorance about how their personal data will be processed.

b. Cognitive limitations

A second set of observations which challenge the efficacy of notice requirements pertain to our shared cognitive limitations. As a document with potential legal implications, notices are often drafted in a very ‘legalistic’ fashion, containing formal and technical wording. In addition to being difficult to comprehend (especially for lay persons), individuals are often pressed to understand the actual consequences of the information practices described in these notices, particularly in the long term. Furthermore, as individuals are repeatedly exposed to privacy notices, it seems inevitable that, over a time, a certain degree of ‘notice fatigue’ kicks in, as a result of which individuals may stop paying attention to privacy notices. Other examples of cognitive limitations include information overload, optimism bias (i.e., a tendency to discount the probability of a negative event occurring) and susceptibility to framing (i.e., the manner in which the information is presented impacts the decision that is made regarding this information).

c. Low signal-to-noise ratio

A third set of criticisms focuses not on the target audience of privacy notices (i.e. data subjects), but rather on the way in which notice requirements are satisfied in practice. In addition to the complexity of language (cf. supra), privacy notices are often characterized by vagueness, obscurity and boilerplate language. As Grimmelman puts it:

76 R. Calo, ‘Against Notice Skepticism in privacy (and elsewhere)’, l.c., p.1052.
77 See also A. McDonald and L.P. Cranor, ‘The Cost of Reading Privacy Policies’ (2008) 4 (Privacy Year in Review issue) I/S: A Journal of Law and Policy for the Information Society, available online at http://www.aleecia.com/authors-drafts/readingPolicyCost-AV.pdf (arguing that the time that website visitor have to invest in reading privacy policies is in itself a form of payment, which can serve as a justification why people are not reading long privacy policies).
78 J.H. Beales and T.J. Muris, ‘Choice or Consequences: Protecting Privacy in Commercial Information’, l.c., p. 114-115 ("It simply does not pay for most consumers to think and make decisions about policies on the use of their information, given that the issue is of such little practical consequence to them").
79 P. Van Eecke and M. Truyens (eds.), ‘The future of online privacy and data protection’, l.c., p. 42.
80 P. Van Eecke and M. Truyens (eds.), ‘The future of online privacy and data protection’, l.c., p. 42.
'Between the lawyerly caution, the weasel words, the commingling of many standard terms with the occasional surprising one, the legally mandated warnings and disclaimers, and the legalese, most privacy policies have a painfully low signal-to-noise ratio.'

This poor ratio can be attributed to a variety of reasons. The first is the desire to protect the controller as much as possible: by giving prior notice, the author hopes to shield the organization against subsequent legal action with respect to its data practices (cf. supra). A second reason is laziness: it is no secret that lawyers avidly engage in ‘copying & pasting’ when drafting public-facing documents such as privacy notices or terms and conditions. A third reason is that it is “better to be safe than sorry”: failure to provide sufficient information typically attracts greater regulatory scrutiny than providing too much information.

Fourth, there is the fear that detailed privacy notices will actually constrain the organization in its future uses of data: knowledge of fluctuations, over time, in actors and processes, pushes drafters of such notices towards abstraction. Finally, organizations arguably have, at least from a marketing and PR perspective, an incentive to obfuscate and/or embellish potentially unpopular data practices as much as possible.

### 3.2 Overreliance on consent

In the previous section, we highlighted a number of criticisms regarding the efficacy of privacy notices. Alongside these criticisms there is also a second strand of critique, which focuses less on the efficacy of notice per se, but more on the issue of whether it is appropriate to rely on data subject consent as a means to legitimize data processing. The following lines of argument can typically be discerned:

a) privacy is a societal good, and should therefore not be treated as a negotiable commodity;
b) requiring individuals’ to ‘police their own privacy’ is a burden unfit for most;
c) the efficacy of ‘notice & choice’ as a regulatory technique depends too heavily on rational choice fallacies;
d) data subject consent should not serve as a waiver for privacy-intrusive practices; and
e) requiring data subject consent inhibits socially beneficial re-use of information.

#### a. Privacy as a societal good

If privacy is, as many have suggested, primarily an issue of informational self-determination, why shouldn’t every individual decide for herself what uses shall be made of her data? The answer most often proffered is this: privacy is not merely a private interest, but also a

---

86 See also O. Ben-Shahar and C.E. Schneider, 'The failure of mandated disclosure', University of Michigan Law School, Program in Law and Economics, 2010, Paper 9 at p. 30 (“When a [disclosure] mandate is stated broadly, disclosers might think that duty requires – or prudence demands – disclosing everything.”)
87 See also A. Meijer, 'Understanding modern transparency', International Review of Administrative Sciences 2009, vol. 75, no. 2, p. 262, regarding transparency provided through government websites (“In a radical perspective this could mean that the representation itself becomes more important than the practice it is representing.”)
precondition for informed citizenship. From this perspective, privacy is above all a precondition for maintaining meaningful democracy: privacy is necessary to guarantee free self-expression, enable diversity and prevent undue societal control. As a result, privacy should also be considered a public good which cannot be traded at will.

b. Responsibilization

"Responsibilization" has been defined as a process ‘whereby subjects are rendered individually responsible for a task which previously would have been the duty of another – usually a state agency – or would not have been recognized as a responsibility at all’. By emphasizing individual choice over societal acceptance, data subjects are effectively pushed into a situation where they must ‘police their own privacy’, for want of communally agreed restrictions upon intrusive data practices. As the complexity of data processing increases, both in terms of the actors involved and operations they perform, this task quickly evolves into an unrealistic burden.

c. Rational choice fallacies

One of the main critiques against notice, as we already highlighted above, is that it relies on a false model of human capacity (‘the perfectly rational consumer with limitless attention’). As a result, reliance upon the informed consent of data subjects, as a means to justify data processing practices, is often subject to similar criticisms. These authors highlight both the cognitive limitations of data subjects, as well as the illusory nature of the premise that they will actually ‘vote with their mouse’ in the face of intrusive data practices. As Beales and Muris put it:

"The reality that decisions about information sharing are not worth thinking about for the vast majority of consumers contradicts the fundamental premise of the notice approach to privacy. To be an effective approach, some significant number of consumers must not only read privacy notices for the businesses with whom they currently deal, they must also consider the privacy practices of alternative service providers and choose the provider

---


92 See e.g. O. Tene and J. Polonetsky, ‘To Track or “Do Not Track”: Advancing Transparency and Individual Control in Online Behavioral Advertising’, Minnesota Journal of Law, Science & Technology 2012, vol. 13, no. 1, p. 335-338 (‘While the privacy-as-choice model is perceived as empowering individuals, it in fact often leaves them helpless and confused [...] Policymakers and businesses, not individual users, should shoulder the burden of setting privacy safeguards’).

93 R. Calo, ‘Against Notice Skepticism in privacy (and elsewhere)’, l.c., p. 1054.

94 As elaborated earlier, the requirement that consent be ‘informed’ also requires effective provisioning of information. Cf. supra; section 2.2.a.
whose practices best match their privacy preferences. There is no reason to think this is currently happening, or will ever happen."\(^95\)

Several scholars supplement this argument by citing a range of additional factors undermining the efficacy of ‘notice and choice’ regulation. In the context of social networks for instance, Grimmelmann has argued that the informed-choice model is completely unrealistic, because it fails to account for the social dynamics of how people make privacy-affecting decisions.\(^96\) Others argue that very often the degree of choice presupposed by this model is often absent, particularly for those products and services offered by data controllers in a monopoly (or near-monopoly) position.\(^97\) And then there are those who extend further upon the cognitive limitations identified above, emphasizing inter alia risks of ‘routinization’\(^98\) and/or ‘consensual exhaustion’\(^99\).

d. Fallacy of sufficiency

Overreliance on consent can also be denounced by pointing to what Brownsword has coined ‘the fallacy of sufficiency’.\(^100\) Briefly put, the argument mainly goes as follows. First, it is wrong to think of consent as a free-standing justification: the significance of granting or withholding consent should always be construed with regard to broader context in which it takes place. Second, it is incorrect to assume that in the absence of a ‘private wrong’ (because of consent given by the parties), there can be no public interest justification for intervention.\(^101\) The fallacy committed here ‘is not so much that an absence of consent makes things wrong, but that it’s presence makes things right’.\(^102\) As a result,

‘[…] we must discourage lazy or casual appeals to consent. Where substantive justification is called for, we should settle for nothing less; in particular, we should not be satisfied with artificial procedural justifications that are tendered in their place.’\(^103\)

---

\(^95\) J.H. Beales and T.J. Muris, ‘Choice or Consequences: Protecting Privacy in Commercial Information’, \(l.c., p. 114\).


\(^97\) See e.g. L. A. Bygrave and D.W. Schartum, ‘Consent, Proportionality and Collective Power’, \(l.c., p. 160\).

\(^98\) See R. Brownsword, ‘Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality’, \(l.c., p. 90\).


\(^102\) \(Ibid\), p. 240.

\(^103\) R. Brownsword, ‘Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality’, \(l.c., p. 90\).
e. Other legitimate interests

A fifth recurring argument against reliance on consent is that it can pose undue obstacles towards the pursuit of objectives beneficial to society. By requiring individuals to express their informed consent before a processing operation can take place, the argument goes, society as a whole is effectively prevented from (re)using their data in the pursuit of other legitimate interests. Such legitimate interests might include disease management, road traffic optimization, prevention of crime, service innovation, etc.

IV. Going forward

In the previous two sections, we have sketched both the justifications for and criticisms against the use of privacy notices in practice. In our view, each of these argumentations brings a valuable perspective to the debate. However, when taken to the extreme, each of these argumentations can also easily be torn apart. Rather than exposing the limitations of each argumentation individually, we will outline a number of recommendations and requirements regarding the use of privacy notices, in the hope of informing future discourses regarding their desired role.

4.1 Disentangling ‘notice & choice’

The first recommendation is to apply a clear distinction, both conceptually and in practice, between ‘notice’ and ‘choice’. Debates regarding the (in)utility of privacy notices often confound two very distinct issues, namely transparency on the one hand, and legitimacy on the other. We perceive mainly two reasons for this. First, there is the widespread practice among online service providers of requiring individuals to consent to privacy notices during registration. As a result, to many individuals, ‘notice’ and ‘choice’ appear as inseparable.\(^{104}\) Second, in certain contexts, the phrase “notice & choice” has effectively become a shorthand reference for privacy regulation based on the Fair Information Practices (FIPs). By systematically referring to these concepts in tandem, the function of notice is often, either implicitly or explicitly, reduced to a means of securing ‘informed’ consent.\(^ {105}\) Given that the majority of privacy notices have proven themselves to be inept at this task, the use of notice in general has become more vulnerable to criticism than perhaps it should be.

\(^{104}\) This is true, even if even if in practice the actual notice is only incorporated by reference, and thus logically still removed from the exercise of ‘choice’.

\(^{105}\) See also R. Brownsword, ‘Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality’, \textit{Lc}, p. 100-101 (observing that there is a tendency ‘to run the two questions together under the general rubric of informed consent’).
Having a duty to inform is distinct from having a duty to ensure that consent is informed.\textsuperscript{106} However, divorcing these two concepts entirely appears to be difficult. As noted by the Article 29 Working Party:

\begin{quote}
"The obligation to inform is [...] distinct but in many cases [...] obviously linked to consent. While consent does not always follow the provision of information (another ground in article 7 can be used), there must always be information before there can be consent."\textsuperscript{107}
\end{quote}

Given that, in many cases, the information that is necessary to secure ‘informed’ consent corresponds, by and large, with the elements of information listed under the controller’s duty to inform\textsuperscript{108}, it is quite easy to understand why these two requirements get mixed together. It is worth reiterating, however, that notice (and transparency in general) holds within it the potential to fulfil an array of other functions, including the promotion of fairness, the reduction of knowledge asymmetries and the increase of accountability of data controllers.\textsuperscript{109} While several of the theoretical justifications for transparency can easily be caricatured and criticized, we believe that the principles of transparency and openness\textsuperscript{110} are (and should remain) essential to the regulatory scheme of Directive 95/46/EC. For example: it may be easy to question the function of notice as a means to help ‘level the playing field’ between controllers and data subjects.\textsuperscript{111} In an era where personal data processing occurs ubiquitously and seamlessly, reliance on notice alone would not only imply an unrealistic need for sequential oversight by individuals, but also fail to take into account the additional knowledge asymmetries that exist between controllers and data subjects (e.g., in terms of technical expertise).\textsuperscript{112} This finding does not however, exclude notice from being instrumental in the evaluation of compliance an organisation’s data practices on a post fact basis (i.e., since the provisioning of notice), in ensuring basic fairness of processing (by putting data subjects ‘on notice’ that their personal data is being processed), or in promoting general awareness of data subject rights. At the same time, we must of course caution ourselves not to overstate the potential functions of notice: different information problems generally demand different information solutions.\textsuperscript{113}

\begin{flushright}
\textsuperscript{106} See also O. Tene and J. Polonetsky, ‘To Track or “Do Not Track”: Advancing Transparency and Individual Control in Online Behavioral Advertising’, l.c., p. 343; R. Brownsword, ‘Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality’, l.c., p. 100.
\textsuperscript{107} Article 29 Working Party, Opinion 15/2011 on the definition of consent, l.c., p. 19.
\textsuperscript{108} Cf. supra; section 2.2.a.
\textsuperscript{109} Cf. supra; section 2.1.
\textsuperscript{110} The ‘principle of openness’ is not explicitly listed in Directive 95/46/EC (it is enshrined in the OECD Privacy Guidelines), but it may be considered a variation on the same theme.
\textsuperscript{111} Cf. supra; section 2.1.b.
\textsuperscript{112} See also J. Alhadeff and B. Van Alsenoy, ‘Legal and Policy handbook for TAS$^3$ Implementations’, TAS$^3$ Deliverable D6.1-2, 2011, p. 28. See also the argument that most individuals are unfit ‘to police their own privacy’ (supra; section 3.2.b).
\textsuperscript{113} See also R. Calo, ‘Against Notice Skepticism in privacy (and elsewhere)’, l.c., at p. 1063-1064 (‘Indeed, notice scholarship generally could benefit from the recognition that merely because one form of notice – say privacy policies – happens not to work, it does not follow that no mandatory information strategy could. Different problems can demand different solutions.’). See also C. Hood, ‘What happens transparency meets blame-avoidance’, Public Management Review 2007, vol. 9, no. 2, p. 194 et seq. (highlighting the trade-offs involved in different forms of transparency) and S. Dawes, ‘Stewardship and usefulness: Policy principles for information-based transparency’, Government Information Quarterly, 2010, vol. 27, p. 377-378 (highlighting tensions between comprehensiveness and understandability).
\end{flushright}
4.2 Side-stepping the autonomy trap\textsuperscript{114}

The second set of recommendations concerns the use of consent as a 'wildcard'\textsuperscript{115} justification for intrusive data practices (cf. the 'fallacy of sufficiency'). Our argumentation is essentially twofold: (1) the relationship between legitimacy and informed consent should be revisited, and (2) common sense should be applied in determining whether a certain practice requires the informed consent of the individual concerned as \textit{a conditio sine qua non} for its legality.

a. Legitimacy of interest vs. informed consent

As indicated earlier, one factor contributing to the widespread reliance on consent is its 'aura' of intrinsic force. Consent seemingly allows data controllers to forego, at least initially, the task of providing a substantive justification for the processing (i.e., as being, all things considered, a reasonable activity to undertake).\textsuperscript{116} Several arguments can be advanced against this approach. The first argument is that, as a matter of principle, consent should not be employed as a 'lazy' justification.\textsuperscript{117} As Brownsword convincingly argues:

\begin{quote}
'We must discourage lazy or casual appeals to consent. Where substantive justification is called for, we should settle for nothing less; in particular, we should not be satisfied with artificial procedural justifications that are tendered in their place.'\textsuperscript{118}
\end{quote}

Second, while the lawfulness of an act can depend, at least in part, on whether or not the individual consents to the act, consent by itself does not automatically prevent an illegality from occurring.\textsuperscript{119} Something more may be required. This is also the case under Directive 95/46/EC: even if a controller is able to avail himself of one of the grounds for processing enumerated in article 7, it does not absolve him from compliance with the fundamental principles of data protection as contained article 6.\textsuperscript{120} Consequently, consent should not be perceived as securing legitimacy in and of itself: in order for processing to truly be 'legitimate', it must also be undertaken in the pursuit of an interest worthy of recognition, with appropriate respect (and safeguards) for the various interests at stake.\textsuperscript{121} Sadly, the language employed by the drafters of the Directive suggests the contrary: by listing consent as one of the 'criteria for making data

\footnotesize{\textsuperscript{114}The 'autonomy trap' is a term coined by Paul Schwartz, referring to 'a cluster of related consequences flowing from the reliance on the paradigm of control of personal data in cyberspace: (1) the strong limitations existing on informational self-determination as it is construed at present; (2) the fashion in which individual autonomy itself is shaped by the processing of personal data; and (3) the extent to which the State and private entities remove certain uses or certain types of personal data entirely from the domain of two-party negotiations.' (P. M. Schwartz, 'Internet Privacy and the State', \textit{Connecticut Law Review} 2000, p. 821.)

\textsuperscript{115}See O. Tene and J. Polonetsky, 'To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising', \textit{I.C.}, p. 338.

\textsuperscript{116}Cf. supra; section 2.2.b.

\textsuperscript{117}R. Brownsword, 'The cult of consent: fixation and fallacy', \textit{I.C.}, p. 224.

\textsuperscript{118}R. Brownsword, 'Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality', \textit{I.C.}, p. 90. See also supra; section 3.2.d (fallacy of sufficiency).

\textsuperscript{119}R. Brownsword, 'The cult of consent: fixation and fallacy', \textit{I.C.}, p. 240 et seq. See also supra; section 3.2.d.

\textsuperscript{120}See for example Article 29 Working Party, Opinion 15/2011 on the definition of consent, \textit{I.C.}, p. 9 ('Obtaining consent does not negate the controller’s obligations under Article 6 with regard to fairness, necessity and proportionality, as well as data quality. For instance, even if the processing of personal data is based on the consent of the user, this would not legitimize the collection of data which is excessive to a particular purpose').

\textsuperscript{121}See also A. Rouvroy and Y. Poulet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy', \textit{I.C.}, p. 73.}
processing legitimate', the Directive itself has given rise to the misconception that consent alone can legitimize the processing of personal data. The practical result has been that 'ensuring the legitimacy of processing' has largely been reduced to a bureaucratic ('box-ticking') exercise: the controller, who has already decided upon the desirability of the processing, reviews the grounds listed in article 7 and picks the one which suits him best. When the more substantive justifications included in the Directive (articles 7, b, c, d and e) are unavailable, the controller is essentially left with two options: either rely upon the (easily contestable) article 7, f), or go for the option which seemingly empowers the data subject: reliance upon consent. This outcome undermines the regulatory scheme of Directive 95/46/EC. Even worse: it opens the door for abusive data practices guised by a cloak of legitimacy.

b. Reinstating fairness

While operating a principled distinction between informed consent and legitimacy may bring greater conceptual clarity, it still begs a number of questions: first, if informed consent and legitimacy are in fact two different things, what should be the relationship between the two? Second, if consent is not ipso facto a requirement for legitimacy, what standard should we use to determine whether it is necessary or not? To answer these questions, it is informative to start by reviewing one of the foundational documents of the current data protection framework, namely the OECD Privacy Guidelines.

The OECD Privacy Guidelines make reference to consent in two of its basic principles, namely the 'collection limitation principle' and the 'use limitation principle':

'Collection Limitation Principle
7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject. […]

Use Limitation Principle
10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:
   a) with the consent of the data subject; or
   b) by the authority of law.'

---

122 One might also submit that the drafters of the Directive in fact used the same term ('legitimate') in three subtly distinct ways, namely: (1) 'legitimacy of purpose' (art. 6, 1, b) (i.e., the aim pursued may be considered as reasonable and respectable); (2) 'legitimacy of processing' (art. 7) (i.e., the processing enjoys sufficient authority, an authority which can derive either from consent of the individuals concerned or from endorsement/acceptance by the majority) and (3) 'legitimacy of interest' (art. 7, (f)) (i.e., an interest 'being worthy of recognition').


124 Paragraph 9 of the OECD Privacy Guidelines specifies that 'The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.' (Purpose Specification Principle)

125 OECD Privacy Guidelines, i.e., paragraphs 7 and 10 (emphasis added).
The quoted principles give rise to a number of observations. The first is that, under the framework of the OECD Privacy Guidelines, consent is not required for every type of data collection (as is also the case with the EU Directive\textsuperscript{126}). There may be scenarios in which obtaining consent is deemed appropriate, but there may also be instances in which it is not. Second, paragraph 10 stipulates that consent is necessary in case of disclosure or use beyond the initially specified purposes (unless this disclosure or use benefits from ‘the authority of law’). This suggests that consent has an important role to play in case of re-purposing of data. The Explanatory Memorandum to the OECD Privacy Guidelines further elaborates upon the role of consent as follows:

‘52. The second part of Paragraph 7 (data collection methods) is directed against practices which involve, for instance, the use of hidden data registration devices such as tape recorders, or deceiving data subjects to make them supply information. The knowledge or consent of the data subject is as a rule essential, knowledge being the minimum requirement. On the other hand, consent cannot always be imposed, for practical reasons. In addition, Paragraph 7 contains a reminder (“where appropriate”) that there are situations where for practical or policy reasons the data subject’s knowledge or consent cannot be considered necessary. Criminal investigation activities and the routine up-dating of mailing lists may be mentioned as examples.’

The OECD Privacy Guidelines, unlike the EU Data Protection Directive, did not include ‘legitimacy’ among its basic principles of data protection as such. Nevertheless, the examples listed in paragraph 52 are still informative. They teach us that whether or not consent should be considered necessary (or “appropriate”) should be assessed on a case-by-case basis, using common sense. So which standard should be made in making this determination? We submit that an appropriate standard for assessing the necessity of obtaining data subject consent is fairness. Under this approach, processing of personal data can be

- unfair if the data subject has not consented to the processing;
- unfair even if the data subject has consented to the processing; or
- fair, all things considered, without consent of the data subject;
- fair without consent of the data subject provided he or she has the right to object or opt out.

Whether or not data subject consent is necessary in order to ensure fairness of processing is inevitably context-dependent. Not all processing of personal data requires consent of the individual concerned, simply because not all processing operations implicate the fundamental rights and freedoms of individuals in the same way. In addition, there may be compelling overriding interests which legitimize the processing of personal data even in the absence of data subject consent.\textsuperscript{127} Or the processing might simply be an inevitable consequence of a certain transaction or event, in which case requesting data subject consent is rather pointless. But there are also operations which, despite a recognition that the aim or interest pursued by the controller might be ‘legitimate’, still require prior consent by the individual concerned in order to be considered ‘fair’. Such fairness should be assessed, not only by reference to the individual’s ‘reasonable expectations of privacy’, but also by reference to human dignity, which requires a

\textsuperscript{126} Cf. supra; section 2.2.

\textsuperscript{127} See also, ‘Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality’, \textit{i.e.}, p. 90 (exposing ‘the fallacy of necessity’).
baseline of freedom in the construction of one's own identity and development of societal relations.

c. Accepted practices

If we accept fairness as a standard for determining when data subject consent is necessary, the next question is: who shall determine what's fair and what's not? The answer to this question is relatively straightforward. In the absence of specific legal requirements, it shall in first instance be the controller who makes this determination. This is a logical consequence of the 'stewardship' model embodied by Directive 95/46/EC: public and private actors are in principle vested with the authority to engage in personal data processing, provided they observe all the relevant legal requirements. It is also a logical consequence of article 7, f, of the Directive, which provides that processing of personal data shall be considered 'legitimate' if it

'[...] is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).'

This is an open-ended provision, pursuant to which essentially any form of processing can be 'legitimated' - provided that the balance of interests between the controller(s) and data subject(s) is appropriately observed. Of course, the assessment made by controllers may be made subject of regulatory and/or judicial review at a later stage. So while data controllers, in first instance, make their own determination of what is 'fair' and what is not, this decision may later be challenged and subjected to independent scrutiny.128

It has been pointed out that general legal standards, such as 'fairness', 'proportionality', or 'reasonableness', hold within them certain weaknesses.129 While offering greater flexibility, the practical efficacy of these standards is dependent on a number of factors, inter alia:

(1) whether or not the standard is applied conscientiously; and

(2) the degree to which regulators and courts are willing to substitute their assessment for the initial assessment undertaken by private or public actors.130

Courts and regulators may be reluctant, to some extent, to supersede the value judgment made by data controllers - particularly where the individuals concerned have allegedly consented to the processing.131 The standard of fairness is therefore by no means a 'silver bullet'. Others might challenge this approach by pointing to risks of (quasi-)judicial activism; insisting that the restrictions upon personal data processing should be decided by a democratically elected

128 In certain instances, the initial assessment made by the controller may be the subject of regulatory scrutiny even before the processing is initiated. Under the current framework, this may be the result of a 'prior checking' mechanism adopted pursuant to article 20 of the Directive. In the proposed regulation, it is similarly foreseen that certain forms of processing require prior consultation with and/or authorization by a supervisory authority. See in particular article 34 of the 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)', Brussels, 25 January 2012, COM(2012) 11 final 2012/0011 (COD).


131 Id.
majority, not by judges or regulators. However, to a certain extent, this is the natural state of things: the law is filled with open-ended norms which must be made concrete by those applying them. That being said, it is also essential that the general requirement of ‘fairness’ be made more concrete, so that those who apply the standard are given sufficient direction. 132 Such concretization may take the form of legislation, but may also take a variety of other forms: collective labor agreements, regulatory guidance, self-regulatory standards, identification of best practices, etc.133

In this context, it is worth signaling the recent proposal by the U.S. Federal Trade Commission to delineate certain ‘commonly accepted practices’. The FTC has identified 5 categories of practices which companies can (in principle) engage in without offering consumer choice, ‘because they involve data collection and use that is either obvious from the context of the transaction or sufficiently accepted or necessary for public policy reasons.’134 The proposed categories include: (1) product and service fulfillment; (2) internal operations; (3) fraud prevention; (4) legal compliance and public purpose; and (5) first-party marketing.135 While the FTC has revised its original approach somewhat in light of the comments received (placing greater emphasis on ‘the context of interaction’136), it continues to believe that the highlighted practices ‘provide illustrative guidance regarding the types of practices that would meet the revised standard and thus would not typically require consumer choice’.137

### 4.3 Minding the gap

The previous section identified ‘fairness’ as a standard for determining whether or not data subject consent is necessary to secure legitimacy. By not treating consent as a free-standing justification for the processing of personal data, this approach may help minimize some of the issues associated with ‘overreliance’ on consent. However, this by no means implies that consent shall no longer be important: a logical extension of the outlined approach is that obtaining data subject consent will in some instances be a necessity, as a condition for fairness. In these

---

132 See also O. Tene and J. Polonetsky, ‘To Track or “Do Not Track”: Advancing Transparency and Individual Control in Online Behavioral Advertising’, l.c., p. 341 (calling upon policymakers to ‘actively cordon-off the limits of consent’).

133 See also L. Edwards and I. Brown, ‘Data control and Social Networking: Irreconcilable Ideas?’ , l.c., p. 19 (citing ‘model contracts’ and ‘industry or co-regulatory codes of conduct’ as a means for preventing retrospective litigation). Note that Member States may in fact have an obligation to impose certain restrictions, pursuant to their ‘positive obligations’ under article 8 ECHR.


135 Id. See also O. Tene and J. Polonetsky, ‘To Track or “Do Not Track”: Advancing Transparency and Individual Control in Online Behavioral Advertising’, l.c., p. 339 et seq. (comparing the FTC’s approach of identifying ‘commonly accepted practices’ to enumeration of the ‘criteria for making data processing legitimate’ under article 7 of Directive 95/46/EC).


instances, vigilance is required in order to ensure that the consent which is given is truly meaningful.138

In its Opinion on the definition of consent, the Article 29 Working Party has elaborated extensively upon the requirements for valid data subject consent.139 One way to help ensure that the given consent is truly meaningful, is by applying these standards strictly.140 Taking this approach even further, one might also increase the stringency of the requirements for valid consent themselves. In the recently proposed Data Protection Regulation141, the European Commission appears to have taken a further step in this direction. First, in the definition of consent, it is proposed to replace the criterion ‘unambiguous’ with ‘explicit’ for all types of data processing, in order to ensure that the data subject is fully aware that, and to what, he or she gives consent.142 The recitals of the proposed Regulation similarly emphasize the need for explicit consent, as well as the requirement of ‘free and genuine choice’.143 The proposed Regulation even goes so far as dedicating a full article to further specify the conditions for valid consent.144 While at times repetitive, this greater emphasis on the requirements for valid consent signals the Commission’s desire to ensure that the granting or withholding of consent is a truly autonomous act (or at least approaches this ideal as much as possible).

Vigilance is also required in order to ensure the practical utility and relevance of privacy notices. Many of the arguments against notice are fuelled not by its theoretical justifications, but rather by how notice requirements are implemented in practice. Cognitive limitations of data subjects are only part of the equation. As elaborated earlier, there are a number of additional factors which undermine the efficacy of notice – factors which relate not to the data subject, but rather to the way in which notices are drafted.145 Especially in cases where notice is intended to serve as a basis for consent, or as a basis for subsequent scrutiny, there is a real risk that such notices fail to deliver the intended level of transparency.146

In summary, we must remain mindful of the gap between, on the one hand, the ‘ideal’ of data subject consent (as a well-informed and truly autonomous act), and the consent that is obtained in practice on the other. The same applies with respect to privacy notices more generally: if

---

138 See also R. Brownsword, ‘The cult of consent: fixation and fallacy’, l.c, p. 224 (‘As an anti-dote, we should repeat once a day that consent is easy to claim and much more difficult to attain’) (regarding ‘casual’ or ‘lazy’ appeals to consent).

139 Cf. supra; section 2.2.a.

140 For instance, on the basis of the requirement regarding accessibility, one might argue that the information provided to the data subject may not be incorporated by reference, but should rather be presented prominently at the very moment that consent is to be either granted or withheld.


142 Ibid, p. 8. See article 4(8) of the proposed Regulation. Regarding the difference between ‘unambiguous’ and ‘express’ consent see also supra; at note 47.

143 See in particular recitals (25) and (33) of the proposed Regulation.

144 See article 7 of the proposed Regulation.

145 Cf. supra; section 3.1.c.


To be clear: we are not arguing that the accountability of function of notice should be removed: given that the proposed regulation seeks to quash the general notification obligation to supervisory authorities, privacy notices may in fact be one of the last sources of reference documentation for later scrutiny.
implemented properly, privacy notices can be a source of valuable information, serving an array of functions. However, if implemented poorly, their added value can be negligible.

4.4 Complementary initiatives

Meaningful transparency and informed decision-making doesn’t come easily. Over time, policymakers and academics have proposed a number of measures to bring us one step closer. The purpose of this section is to briefly highlight two initiatives which may play an auxiliary role towards augmenting the transparency of data practices and informed decision-making by data subjects.

a. Layering notice

In 2004, the Article 29 Working Party adopted an Opinion on the development of more harmonized information provisions. This Opinion outlined a ‘layered approach’ towards fulfilling notice obligations to help mitigate risk of complexity. Layer 1, the ‘short notice’, comprises

the core information required under Article 10 of the Directive namely, the identity of the controller and the purposes of processing – except when individuals are already aware-and any additional information which in view of the particular circumstances of the case must be provided beforehand to ensure a fair processing. In addition, a clear indication must be given as to how the individual can access additional information.

Layer 2, the ‘condensed notice’, includes all relevant information required under the Directive, as well as a point of contact, and should be accessible to the data subject at all times. Layer 3, the full notice, must include all the legal requirements provided for in the national legislation.

The approach of the Article 29 Working Party has been criticized by some as being naïve. It has been argued that ‘some national laws require full descriptions of data processing activities, and it is very difficult to describe them in a form the consumer can understand’. Albeit not perfect, the suggestion of the Article 29 Working Party can function as a good starting point for the simplification of information notices that serve as the basis for the provision of informed consent in environments. Additionally, it can be suggested that the proper information of the data subject will be enhanced when the information relating to the processing of personal data is highlighted in some way – printed in bold or in a distinguishable frame – so that the data subject

148 Under such an approach not all information is provided in a single document, but rather spread out of over a number of layers of information (short – condensed – full).
150 Id.
151 Id.
can spot it easily. Other proposed ways of improving or simplifying notice include ‘visceral’ notice\textsuperscript{153}, and use of the use of ‘privacy icons’ or ‘nutrition labels’.\textsuperscript{154}

\textbf{b. Feedback & awareness tools}

A second way of enhancing transparency and informed decision-making by individuals is through so-called ‘privacy feedback and awareness tools’ (PFA). The idea underlying PFA is to show individuals the consequences of potentially privacy-relevant activities that they and others may perform within a particular system.\textsuperscript{155} These tools essentially aim to foster greater understanding and reflection, so that individuals, through the feedback they receive, can gain greater knowledge and understanding of the privacy implications of their system use.\textsuperscript{156}

A variety of PFA are already available today. Many are ‘historical viewers’, which may for example provide users with greater insight into the consequences of one’s settings.\textsuperscript{157} Other tools may take the form of ‘ongoing monitors’, which may reveal to the individual how he or she is being tracked when navigating among websites, or the amount of cookies stored on one’s PC.\textsuperscript{158}

An important caveat regarding the use of PFA is that there can be a very fine line between being informative, entertaining or normative/controlling.\textsuperscript{159} The reference value employed by the designers of these systems (e.g., ‘sharing is good’ vs. ‘sharing is risky’) is bound to impact the actual design of these tools. Just as with more traditional forms of notice, we must remain mindful of the susceptibility to framing.\textsuperscript{160} However, this finding does not ipso facto prevent these tools from improving decision-making by individuals online. Furthermore, these tools can enhance the accountability of data controllers, by providing automated means for establishing, at least partially (and provisionally), whether a company in fact abides by its own stated data practices.

\textbf{V. Conclusion and outlook}

\textsuperscript{153}See R. Calo, ‘Against Notice Skepticism in privacy (and elsewhere)’, \textit{l.c.}, in particular p. 1034 et seq.
\textsuperscript{154}See O. Tene and J. Polonetsky, ‘To Track or “Do Not Track”: Advancing Transparency and Individual Control in Online Behavioral Advertising’, \textit{l.c.} p. 342 et seq.
\textsuperscript{156}Id.
\textsuperscript{157}Id. For example, ‘Privacy mirror’ seeks to demonstrate how much profile information third party applications can access on Facebook (\url{http://apps.facebook.com/privacy_mirror}).
\textsuperscript{158}For example, ‘Collusion’ visualizes how seemingly separate companies are tracking users together See \url{http://www.toolness.com/wp/2011/07/collusion}
\textsuperscript{159}B. Berendt and B. Gao, ‘Feedback and awareness aspects’, \textit{l.c.}, p. 70
\textsuperscript{160}Cf. supra; section 3.1.b. See also O. Tene and J. Polonetsky, ‘To Track or ”Do Not Track”: Advancing Transparency and Individual Control in Online Behavioral Advertising’, \textit{l.c.}, p. 346 (describing the value judgment implicit in mechanisms such as visceral notice as compared to historical viewers such as ‘dashboards’).
With the rise of the information society, certain notions of privacy, such as the right to control the exchange information about oneself, are increasingly challenged. In practice, only a fraction of internet users read the privacy notices that precede the collection of their ‘informed’ consent. Regardless of whether privacy notices are read or completely ignored, it is worth re-evaluating the extent to which data subject consent should formally serve as a justification for the processing of personal data. The result has been a wide-spread practice whereby "‘consenting’ is reduced to a bureaucratic process, where the collection of informed consent is carried out in a casual way, and where we succumb to the temptation to make use of consent as a lazy justification." Overreliance on the consent of the data subject for the processing of his personal data definitely does not enhance the data protection of individuals, quite on the contrary.

The European Data Protection Directive has foreseen a number of criteria for making the processing of personal data legitimate. Consent of the data subject is only one of them. The Directive accommodates instances where the processing may be justified by virtue of legitimate interests which were not explicitly anticipated by the European legislator. This should in principle allow for sufficient flexibility. In order to determine whether or not data subject consent is needed, recourse may be had to other principles of data protection, such as fairness. Determining whether or not data subject consent is necessary to ensure fairness is by definition a context-specific exercise. It is impossible to draw up an exhaustive list of instances in which consent is either necessary or illusory. However, legislators, regulators, civil society and industry can work together to define specific instances in which use of consent is deemed necessary, desirable, superfluous, or fictitious. These specifications may then serve as ‘guide posts’ for regulators and data controllers alike when evaluating the legitimacy of processing in a specific instance.

In any event, the function of privacy notices should not be reduced to a means of securing ‘informed’ consent. Openness and transparency are fundamental principles of data protection law, which are essential to the regulatory scheme of Directive 95/46/EC. Mandated disclosure through notice can fulfill an array of functions, provided those functions are properly understood by all stakeholders involved, and reflected in the corresponding legal provisions.

Finally, when trying to navigate the limitations of notice and consent, we do well to heed the problems arising from cognitive limitations and responsibilization. However, we must also remain mindful of the motivations and mindset of those who have a duty to inform, regardless of whether such information precedes the elicitation of consent. In order for data privacy notices to fulfill a meaningful role, vigilance is required both from regulators, data controllers and society at large. Complementary mechanisms should be promoted to ensure that, where consent is needed, it is appropriately granted. Layering of notice may be a step in the right direction, but in principle there is no limit to the ways in which transparency and autonomous decision-making can be stimulated. Future research efforts should continue to seek out additional mechanisms to enhance transparency, both on an ex ante and post fact basis.

---