INTERNET POLICY REVIEW
Journal on internet regulation

Volume 1 | Issue 4

Consent under pressure and the Right to Informational Self-Determination

Julian Staben

Internet and Media Regulation, Humboldt Institute for Internet and Society (HIIG), Germany, Berlin, julian.staben@hiig.de

Published on 17 Dec 2012 | DOI: 10.14763/2012.4.265

Abstract: The concept of consent is deeply entrenched in the German constitution's right to informational self-determination, which is itself part of the general right to personality (Art. 2 (1) in conjunction with Art. 1 (1) GG). While this concept still remains valid in law, in practice, it has taken hits that can be attributed to market developments, long contractual terms and conditions, and increasing dependence of users on online platforms. This analysis examines what is left of the notion of consent in this field, and gives an overview over several legal and practical solutions to revive it effectively.

Keywords: Data protection, Consent, EU Data Protection Regulation, Informational self-determination, General right of personality

Article information

Received: 10 Dec 2012 **Reviewed:** 12 Dec 2012 **Published:** 17 Dec 2012

Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL:
http://policyreview.info/articles/analysis/consent-under-pressure-and-right-informational-self-determination

Citation: Staben, J. (2012). Consent under pressure and the Right to Informational Self-Determination. *Internet Policy Review*, *1*(4). DOI: 10.14763/2012.4.265

NOTE

The following article has exceptionally NOT BEEN PEER REVIEWED.

Since the German constitutional court's census decision[1] the fundamental right to informational self-determination (informationelles Selbstbestimmungsrecht) is one of the most important parts of the general right of personality (Allgemeines Persönlichkeitsrecht) guaranteed by art. 2 para. 1 in conjunction with art. 1 para. 1 of the German constitution. On a statutory level, informational self-determination is especially guaranteed by federal and state data protection acts. If informational self-determination is defined as "the

> authority of each individual to determine disclosure and use of his personal data" [2] it seems inevitable to require the affected person's consent for the admissibility of personal data processing.[3] Accordingly, implementing rules can be found in § 4 para. 1, § 4a para. 1 Federal Data Protection Act (Bundesdatenschutzgesetz) and the corresponding Data Protection Acts of the States (Landesdatenschutzgesetze).

The ideal of a prior, voluntary and informed consent to the processing of personal data has gotten quite a few cracks since the spread of automated data processing and especially the age of constant data elicitation. This insight, of course, is anything but new. Nonetheless, the development has taken speed with the spread of online communication offers. It started with the use of e-mail providers (e.g. Gmail, Yahoo, Hotmail, Gmx) and forums, and is today fostered by all kinds of social networks (Facebook, Google+) and blog hosting services (Blogger, Twitter). At this point not only questions concerning the applicable law and its effective implementation have to be discussed. The ideal of a well-informed consent itself as well as our notion of voluntariness of consent are under considerable pressure.

INFORMED CONSENT

It is anything but new that parties of modern day legal relations find themselves facing contractual terms which due notice is highly unproportional to the significance of the contract. Hereby, not primarily the financial capacities of the parties are put at risk (by themselves) but the general right of personality. Additionally, the use of personal data largely eludes precise peremptory norms and while being easily reversible by cancellation in theory, this is hardly controllable in practice. These facts especially apply when it comes to accessing online communication platforms. The heart of facebook's terms of data protection, for example, is with its 9000 words about nine times as long as this blog post. Hardly any user can cope with this flood of information with regard to its content when first signing up for the service. Therefore, only the fewest users do really know what types of use of their data they have agreed to.[4] The ideal of an actual informed consent is brought down to societal facts with a bump. Legal limits for the terms of data protection are admittedly set by data protection acts as well as the laws on the admissibility of terms and conditions (Recht der Allgemeinen Geschäftsbedingungen). But while data protection acts have a rather general design and allow almost all kinds of possible data use, the laws on the admissibility of terms and conditions are not tailored to protect the right to informational self-determination. This has serious consequences: Users have poor knowledge mainly shaped by hearsay, which results in insecure online behaviour. Contrary to the constitutional and statutory ideal it remains obscure to (almost) all users for what exact purposes personal data can be used. This may be countered by arguing that every responsible user has it in his own capacity to inform himself properly about the use of his data when signing up for a service. Those too lazy to read the terms of data protection should maybe refrain from using the service. This argument, however, misses out on societal facts for several reasons: Firstly, the terms of data protection are often drafted in a very vague manner and the specific possible uses of data will possibly remain unknown to a new user, who is not familiar with the functions of a certain online communication platform. That means even if the user reads through the terms of data protection, he cannot precisely assess what will actually happen with

his personal data. Furthermore, the protection of parties in every day transactions by consumer law and the laws on the admissibility of terms and conditions have raised certain expectations of being protected by the law when it comes the use of online communication platforms. Consumers, who are used to enjoying extensive warranty and cancellation rights with almost every purchase order, will often assume that they do not have to act overcautiously online as well.

VOLUNTARY CONSENT

Yet the biggest problems emerge when the alternatives are taken into consideration: The individual citizen is increasingly deprived of a free[5] decision in favour of or against online communication platforms, because these are more and more indispensable for a modern execution of fundamental rights.

Today, almost all fundamental rights are lived out online, especially those concerned with communication (Kommunikationsgrundrechte).[6] Online communication sometimes substitutes offline communication; in most cases, nevertheless, the former complements the latter. Calls for demonstration and assembly, for example, are prepared, spread and discussed online. However, in recent years certain communication platforms prevailed over others and gained a position with a market dominating character.[7] The citizens exercising their fundamental rights by using online communication are confronted with growing monopolistic or oligopolistic structures favouring corporations, which are naturally – in contrast to the state – not bound by fundamental rights.[8] One could argue that citizens are free to execute their fundamental rights outside prevalent communication platforms. But fundamental rights concerned with communication are by nature dependent on each citizen's realistic chance to make his concerns heard by potential supporters. The prospects of being perceived seem considerably smaller outside of established communication platforms. If the chance of being heard by others diminishes to a very low level, the use of certain online platforms for communication becomes inevitable for the individual citizen. There is not much left of our notion of voluntariness of consent, when citizens have the choice between surrendering their data to dubious use or effectively waiving their fundamental rights.

Consent is generally not voluntary and therefore void when it is granted under the influence of duress or deception.[9] In this strict legal sense consent is indeed a voluntary act and consequently stays valid in the near future. It would however constitute a misconception of societal and constitutional developments, if one believed that consent in its present shape could secure informational self-determination online and thus the general right of personality permanently.

IS A REVITALISATION OF CONSENT IN PERSONAL DATA PROCESSING POSSIBLE?

The question has to be asked, which significance can be assigned to the consent in data protection law especially online. As demonstrated, the fundamental idea of an informed voluntary consent is under pressure: by long, confusing terms of data protection on the one side and through market domination inevitable becoming online communication platforms on the other side. Does the factual idle of consent lead to a violation of the state's duty to protect

resulting from fundamental rights? Can there be alternatives to consent or can the concept of consent be revived? Solutions are sought to decrease the information deficit and to prevent the outlined predicament.

REMEDIES FOR THE INFORMATION DEFICIT

Regarding the flood of information the user faces when accepting the terms of data protection it is more than questionable that (further) peremptory norms can provide a solution. Specific instructional duties often drown in the bulk of terms concerning data protection. A structured and consistent presentation could provide relief here. The projects Terms of Service; Didn't Read and Wikimarx count on the contribution of internet users. While Wikimarx tries to highlight important and critical terms, Terms of Service; Didn't Read attempts to inform the user about important terms at a glance by using colour coding. A general colour coded ranking of online communication is planned to directly show when visiting a website by employing a browser add-on. It remains to be observed if these attempts to channel the flood of legal information will succeed and if the entanglement of broad contractual terms and national laws can be coped with. It is at least a possibility worth considering in order to restore the users' responsibility when it comes to the protection of their data.

WAYS BACK TO A VOLUNTARY DECISION?

However, in spite of potentially increasing transparency there are few possibilities to evade the growing power of online communication platforms for the effective execution of fundamental rights. In order to be heard one has to step into the space where one's potential supporters can be found. Therefore the question arises how reasonable access terms can be established and which role the legislator can or must play in this matter.

THE STATE'S CONSTITUTIONAL DUTY TO PROTECT

Initially it is to be examined if certain legislative actions are potentially predetermined by fundamental rights. Due to the fact that the aforementioned online communication platforms are operated by private corporations, the fundamental rights are not directly applicable between operators and users. It principally rests upon the citizens to govern their contractual relations – including the use of personal data – themselves by choosing the appropriate contractual terms. By providing the law and instruments of law enforcement the state offers the parties the means for achieving an equilibrium of interests and adhering to it. But the state principally refrains from strictly designing the legal relationships in the interest of the freedom of the citizens. However, if it comes to such a domination of one party over another that one of them can unilaterally set the contractual terms, it is the duty of the State to "save the fundamental rights of the parties involved in order to prevent the inversion of self-determination into external determination"[10][1]. The state has to comply with this constitutional duty to protect also when it comes to the right to informational self-determination.[11][n.2]

The future point in time when an external determination and therefore an infringement of the duty to protect is to be assumed, cannot quite be answered here. The alternative actions for each citizen and the amount and quality of data necessary to be disclosed for the effective execution

of fundamental rights remain to be examined.[12][3]

Yet if a constitutionally relevant lowering of the level of protection could be found here, still as always a broad margin of possible actions remain in order to achieve compliance with the constitutional duty to protect. Some possibilities of protection and their effectiveness shall be considered now.

ALTERNATIVES TO CONSENT OR CONSENT LIGHT?

First it can be discussed if there are other solutions for securing personality rights than the concept of consent. The underlying idea is that citizens cannot be coerced into consenting if the ground for consent is taken by compelling law.

But is data protection and from a constitutional perspective the right to informational self-determination even imaginable without consent or consistent with constitutional doctrine? The right to informational self-determination has yet the *literal* condition that the right holder must and can decide upon disclosure of information himself. Not being able to further follow this chain of thought here, it is at least to be noted that consent into disclosure of certain information is currently forbidden by law. An employee, for instance, cannot validly consent into a genetic test by his employer according to § 18 GenDG (Genetic Diagnostics Act).[13][4] This is a distinct exception to the principle of private autonomy. It could be discussed to design data protection law – at least between consumer and entrepreneur – as in large parts compelling special private law (Sonderprivatrecht) comparable to the law of employment or tenancy.

However, it should not be taken hold of this supposedly rescuing hand too hastily. Surely, it would not only end the domination by contractual parties in some areas, but also in many cases limit private autonomy und therefore the freedom of the users themselves.

More important appears the following: A set of “one size fits all” provisions cannot do justice to the diversity of personal data and different purposes of data processing. In some cases data elicitation that constitutes a deep interference with the private sphere and therefore seems fit for prohibition, can yet in other cases be desirable and in the best interest of the user. For example, the disclosure of a user’s age or sexual orientation to an e-mail provider or an ordinary social network in contrast to a dating platform are to be viewed differently. Possible communication services seem too diverse especially online to be governed by a set of strict universally applicable provisions. Such provisions would always pose the threat of either providing a protection level too low or of preventing legitimate business models. This troublesome and regulatory difficult path should remain as a last resort.

Additionally, problems may emerge concerning the respectively applicable law and its effective implementation in transnational cases. When it comes to pure online services it is often too easy for corporations to escape from unpleasant national, even compulsory, law or at least from its effective implementation. [14][5]

Which means do remain to guarantee an effective execution of fundamental rights in the future? It is to be noted, that some sort of consent to data processing must remain the underlying legal principle of data protection in the future. Existing approaches of simplified presentation of information may help to restore the informational basis of consent. Additionally, it can be tried to set minimum standards in certain areas by the complementary effect of precise, compelling law. In this process an eye should be kept on implementation deficits. A universal European

solution can help to provide an acceptable standard of protection in the long run and enable people to make use of their fundamental rights through communication in the 21st century.

FOOTNOTES

1. BVerfGE 65, pp. 1.

2. BVerfGE 65, p. 43.

3. About consent and the new European General Data Protection Regulation confer the blog post from 22 Oct. 2012.

4. Cf. Buchner, DuD 2010, p. 42.

5. About voluntariness offline Menzel, DuD 2008, p. 406, Schapper/Dauer, RDV 1987, p. 170; Schmidt, JZ 1974, p. 247; thoughts on voluntariness with regards to participation in social networks Buchner, DuD 2010, p. 41.

6. Of course, besides that the general right of personality is realised online especially by digital natives. This blog entry is however focused on the fundamental rights concerned with communication in the narrower sense.

7. On the one hand the prevalence of fewer communication platforms makes the due notice of each set of the data protection terms more appropriate or proportional (see above), on the other hand this as a result increasingly undermines the voluntariness of consent.

8. This causes separate issues, which cannot be addressed here.

9. Gola/Schomerus, Bundesdatenschutzgesetz Kommentar, 11. edition 2012, § 4a, marginal no. 19 et seqq.

10. E.g. BVerfGE 114, 1, 34.

11. Cf. concerning this BVerfG, 1 BvR 2027/02, decision from 23th Oct. 2006, para. no. 33.

12. The constitutional court, for example, decided on insurance terms which allowed a deep interference with the insured's right to self-determination. The abandonment of an occupational capacity insurance by the individual as the only possibility to save one's right to self-determination was not deemed acceptable by the constitutional court, BVerfG, 1 BvR 2027/02, decision from 23th Oct. 2006, para. no. 39.

13. Also cf. Thüsing, Arbeitnehmerdatenschutz und Compliance, 1. edition 2010, margin no. 389, 396 et seqq.

14. What it means for the state's duty to protect, when areas like this evade from state authority, must remain uncovered here.