White Paper

The Draft EU General Data Protection Regulation: Costs and Paradoxes of Explicit Consent

Omer Tene, Senior Fellow
Christopher Wolf, Founder and Co-Chair
The Future of Privacy Forum

January 2013

The Future of Privacy Forum (FPF) is a Washington, DC based think tank that seeks to advance responsible data practices. The forum is led by Internet privacy experts Jules Polonetsky and Christopher Wolf and includes an advisory board comprised of leaders from industry, academia, law and advocacy groups.

The Draft EU General Data Protection Regulation: Costs and Paradoxes of Explicit Consent

The Future of Privacy Forum (FPF) has worked hard on initiatives to provide individuals with greater transparency, choice and control over their personal data. For example, FPF has participated in initiatives geared to empower individuals with respect to targeted online advertising, smart grid and mobile apps. These initiatives have included support for privacy icons, just-in-time notification requirements, and sophisticated access and transparency tools. The lesson from our involvement with new technologies is that a "one size fits all" approach to empowering consumers is ill-advised.

FPF is concerned that the rigid and inflexible explicit consent approach of the Draft General Data Protection Regulation (GDPR)[1] as currently constructed is unlikely to enhance individual control. To the contrary, we fear it unnecessarily will restrict the scope of individuals' choices while encumbering organizations with costly formalities.

By imposing strict new restrictions on consent, the GDPR perversely will shift the paradigm from processing based on individual consent to processing based on the "legitimate interests" of the *controller* as controllers seek ways to free themselves from the difficulties of operationalizing an explicit consent requirement. This will have the paradoxical effect of reducing legal certainty and narrowing the scope for individual choice. The construct of the Rapporteur's Report further exacerbates this legal predicament, by restricting "legitimate interests" to "exceptional" circumstances while tightening consent requirements even more. This places controllers in an untenable position, inhibiting valuable economic activity in Europe.

We urge a more nuanced approach to consent-based processing. While in specific cases, explicit consent should be required; in many cases, consent may be inferred from the context of a transaction or relationship; and in certain cases, processing may not need to be

[1] References to the proposed GDPR are to the European Commission proposal of 25 January 2012: 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), COM(2012) 11 final. References to the Rapporteur's Report are to the Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7 0025/2012 – 2012/0011(COD)), Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Jan Philipp Albrecht.

legitimized by consent at all. In the absence of a more nuanced approach to consent, a new legal basis should be added to Article 6 of the GDPR to facilitate the processing of *pseudonymized data* based on the legitimate interests of the controller.

Current Law and Proposed Changes

Under European data protection law, the collection, storage, use or transfer ("processing") of personal data must be justified by a "legal basis". The existing framework enumerates several alternative legal bases, including consent, which must be "unambiguous", "specific", "freely given" and "informed" but could be explicit or implicit (Article 7(a) of the Data Protection Directive ("DPD")); compliance with a legal obligation (Article 7(c)); or fulfilling the "legitimate interest" of the data controller, which must be balanced against the privacy risk to individuals (Article 7(f)). Accordingly, Article 7 of the DPD establishes a careful balance between the interests of data controllers and the rights of individuals.

The GDPR disrupts the existing balance by eliminating the option to rely on implied consent. It defines consent as "freely given specific, informed and explicit indication of […] wishes" by an individual ("data subject") (GDPR Article 4(8)), and introduces additional restrictions, including a requirement that controllers bear the burden of proof for showing individuals' consent; that consent to data processing be separated from other agreements; that individuals shall have a right to withdraw their consent at any time; and that consent shall not be used to legitimize data processing in case of a "significant imbalance between the position of the data subject and the controller."[2] In addition, under Article 20 of the GDPR individuals have a right "not to be subject to a measure which produces legal effects… and which is based solely on automated processing…" This broad restriction on "measures based on profiling" exempts only a narrow category of cases, namely where such processing "is carried out in the course of the entering into, or performance of, a contract"; is expressly authorized by law; or is based on consent.[3]

The Role of Consent

Privacy scholar and pioneer Alan Westin's canonical conceptualization depicts privacy as individual control over personal information.[4] Accordingly, all existing privacy frameworks place considerable emphasis on consent. While in principle, there is no prioritization among the legitimate bases for processing set forth in Article 7 of the DPD,[5] in practice most data processing operations rely on consent for legitimacy.[6] Over the years, consent has become

[2] Additional restrictions on consent are proposed by the Rapporteur's Report; *see* proposed Article 7(6), which is discussed below.
[3] Additional restrictions on profiling are proposed by the Rapporteur's Report; *see* proposed Articles 6(1c)(d) and 20, recital 58.
[4] Alan Westin, PRIVACY AND FREEDOM 7 (Antheneum,1967).
[5] Lee Bygrave & Dag Schartum, Consent, Proportionality and Collective Power, in Serge Gutwirth, Yves Poullet, Paul De Hert, Cecile de Terwangne and Sjaak Nouwt (eds.), REINVENTING DATA PROTECTION, 2009, Springer, p. 165.
[6] Christopher Kuner, EUROPEAN DATA PROTECTION LAW: CORPORATE COMPLIANCE AND REGULATION (Oxford University Press, 2nd ed. 2007), sec. 5.28; Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, WP187, 13 July 2011, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf.

closely intertwined with the concept of privacy. Any privacy infringement presupposes *lack of consent*. By relying on consent, the legal framework has managed to remain neutral with respect to various processing activities; instead of deciding whether such practices are commendable or subject to scorn, policymakers relegate the decision to individual discretion.

The effect has been to burden individuals with difficult, complicated choices, which become a detriment to user interfaces and cause notice fatigue. As new technologies emerge, the opportunities for consent expand geometrically and eventually become meaningless, as consumers tick boxes reflexively in order to proceed with the use of the technology. Moreover, as the "Internet of Things" advances, and as the prevalence of screens on which choices may be indicated diminishes, just-in-time explicit consent may not be possible at all.

Instead of maintaining a "neutral" regulatory stance, which effectively treats all processing activities as equal, policymakers should ensure that consent requirements remain closely linked to the context, sensitivity and scope of data processing, thus requiring explicit consent in some but certainly not all cases.[7]

Explicit Consent

The discussion over the scope of consent in the privacy framework has been captured by the "opt-in vs. opt-out" debate. Proponents of opt-in consent tend to assume that explicit consent is "purer" or more meaningful than implied consent (which could be accompanied by opt-out rights).[8] Similarly, the GDPR's emphasis on explicit consent reflects an underlying assumption that opt-in consent provides more robust protection for individuals. Alas, in fact, individuals explicitly consent to agreements all the time without such consent being informed, voluntary, or meaningful. Individuals sign boilerplate contracts (*e.g.*, with banks or insurance companies), execute clickwrap agreements and end-user license agreements (EULAs), and download apps granting whatever permissions are asked of them.

As Professor Fred Cate observed: "if consent is required as a condition for opening an account or obtaining a service, a high response rate can always be obtained."[9] Professor Daniel Solove recently argued: "If the goal is not to restrict new uses of data in a formalistic manner and to distinguish beneficial from harmful uses, an opt-in system for new uses of data might impede both good and bad uses, as procuring new consent is costly."[10]

Excessive reliance on opt-ins inevitably will disrupt user interfaces and encumber individuals with repetitive prompts, which they will be eager to click through to reach their destination. This will be exacerbated by the requirement in Article 7(2) of the GDPR that consent to data processing must be unbundled from other agreements. Indeed, some would characterize the

[7] Omer Tene & Jules Polonetsky, To Track or 'Do Not Track': Advancing Transparency and Individual Control in Online Behavioral Advertising, 13 MINN. J. L. SCI. & TECH. 281 (2012).
[8] The Rapporteur's Report expressly rules out reliance on opt-out consent; recital 33.
[9] Fred Cate, The Failure of Fair Information Practice Principles, in CONSUMER PROTECTION IN THE AGE OF THE INFORMATION ECONOMY (Jane Winn ed., 2006).
[10] Daniel Solove, Privacy Self-Management and the Consent Paradox, 126 HARV. L. REV. ___(forthcoming 2013).

amended e-Privacy Directive[11] as a real-life, grand scale experiment with an opt-in model, which, far from delivering more privacy, has left the field in disarray with little benefit to users. Effectively, European regulators, not to mention websites and mobile apps, have been pressed to ignore the apparent plain meaning of the legislative text in favor of what in practice has become a notice and opt-out approach.

An explicit consent model based on a rigid, formalistic understanding of individual control is ill suited for current technological and business realities. Today, information is gathered via multiple channels, including always-on sensors such as mobile devices and social media where individuals are active participants, and is processed by layers upon layers of service providers who often reside in the cloud. Imposing explicit consent requirements at multiple junctions of information flows would frustrate individuals' user experience while at the same time unduly restricting innovation and economic progress. European policymakers should avoid reducing the legitimacy of data processing to a bureaucratic box-ticking exercise.

The requirement for explicit consent, particularly when coupled with burden of proof obligations under Article 7(1) of the GDPR, will incentivize organizations that currently process strictly de-identified data to increasingly rely on an architecture of authenticated identities. For such organizations, the imposition of an explicit consent requirement creates perverse results which run counter to the gist of other provisions of the GDPR, such as Article 10. Although the Rapporteur's Report implies that provable explicit consent could be secured without relying on authenticated identities,[12] such a conclusion, while perhaps not technologically impossible,[13] is impractical in a business setting.

The GDPR's explicit consent requirement is not interoperable with other branches of European law dealing with consent. European contract law has long distinguished between three different situations:

Category 1 consists of cases where consent can never be given for any reason. For example, French law states that an author cannot agree to sell his or her moral rights. Similarly, the GDPR could provide that an individual cannot voluntarily transfer all of his or her rights with regard to personal data for all uses, now and in the future.

Category 2 consists of cases where consent is possible, but special precautions are needed to protect individuals. There are many examples for this in contract and consumer protection law. For example, Italian law requires separate signature for clauses relating to jurisdiction or arbitration. French law requires persons granting personal guarantees to write out their obligations in hand. The draft European Regulation on a Common European Sales Law

[11] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), 2002 O.J. (L 201) 37 (July 31, 2002) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0037:EN:PDF.

[12] *See, e.g.*, Rapporteur's Report proposed recital 32, stating: "Where processing is based on the data subject's consent, the controller should have the burden of proving that the data subject has given the consent to the processing operation (…) To comply with the principle of data minimization, the burden of proof should not be understood as requiring the positive identification of data subjects unless necessary."

[13] *See, e.g.*, OAuth Community Site, http://oauth.net.

(RCESL),[14] which was proposed two months before the GDPR, provides that consumers must separately consent to the choice of Common European Sales Law as governing law of the contract. The GDPR could provide in this vein that for certain sensitive uses of personal data, enhanced precautions are required to ensure that consent is validly given.

Category 3 consists of cases where consent should be covered by general rules on contracting, including rules on mistake, misrepresentation, proof, imbalances in bargaining positions, withdrawal of consent, and when conduct constitutes acceptance.[15] The rules of the RCESL or equivalent national contract laws would apply to this category. In the context of data protection, this third category would include routine uses of personal data in the context of contracts for digital products and services, uses that do not create special risks triggering the use of category 1 or 2.

The GDPR, in contrast, treats all instances of consent to the processing of personal data as category 2 cases. The impact of this approach, particularly on the development and security of contracting for digital products and services, appears disproportionate and inconsistent with the Digital Agenda for Europe.

An Alternative Approach

In many cases, consent that is implied from the *context* of a transaction or relationship is more meaningful than explicit consent. This is particularly true where such contextual, implied consent is accompanied by transparency and opt-out rights. In its guidance on the rules on use of cookies and similar technologies, the UK Information Commissioner (ICO) recognized that "[i]mplied consent has always been a reasonable proposition in the context of data protection law and privacy regulation" and that "[i]mplied consent is certainly a valid form of consent".[16] The ICO introduced the concept of "feature led consent," explaining that "[p]rovided you make it clear to the user that by choosing to take a particular action then certain things will happen you may interpret this as their consent."[17]

Explicit consent should be reserved for cases where an organization uses individuals' data in a manner materially different than claimed when the data were collected; or collects sensitive data for certain purposes. For example, explicit consent should be used to legitimize the processing of genetic or sensitive biometric data. Similarly, continuous monitoring of location should require opt-in consent. Conversely, in cases where data

[14] Proposal for a Regulation of the European Parliament and of the Council on a Common European Sales Law, 11 October 2011, COM(2011) 635 final

[15] The RCESL has ten articles dealing with "defects in consent," some of which potentially conflict the provisions on consent in the GDPR.

[16] Information Commissioner's Office, GUIDANCE ON THE RULES ON USE OF COOKIES AND SIMILAR TECHNOLOGIES (v.3, May 2012), 6-7. http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide/cookies.aspx; also pointing out that "it might be useful to unpack what we actually mean by the term 'implied consent' remembering throughout that consent (whether it is implied or express) has to be a freely given, specific and informed indication of the individual's wishes".

[17] *Ibid*, at p 22.

processing is an inevitable consequence of a relationship or transaction, requesting individuals' consent would be pointless.

The emphasis on context is based on work by Professor Helen Nissenbaum, who introduced a notion of privacy that is "a function of several variables, including the nature of the situation or context; the nature of information in relation to that context; the roles of agents receiving information, their relationships to information subjects; on what terms the information is shared by the subject and the terms of further dissemination."[18] As Professor Nissenbaum recognizes, relationships can change over time. This is particularly true with respect to business models that are young and in flux together with users' perceptions and expectations. For example, if Facebook had not proactively launched its News Feed feature in 2006, we might not have benefitted from Facebook (or similar services) as we know it today. It is only when data started flowing that users saw the benefit, which is viewed today as an indispensible service by more than one billion users worldwide.

Some argue that soliciting express consent should be a prerequisite to *any* shift in existing boundaries.[19] In reality, however, shifting contexts are not always readily negotiated. Rather, organizations should assess the effects of any prospective change on data subject expectations; convey their policies clearly and conspicuously; and in certain cases provide data subjects with an opportunity to opt out. When a change in context is radical and transparency measures inadequate to support it, express consent can be relied upon to ensure that data subjects are willing to accept a new data use. Finding the precise balance between evolving social norms and individual rights is never easy; yet in order to permit innovation and growth in the European economy, policymakers should avoid overly restrictive formalistic standards.

The boundaries of context are not subject to hard and fast rules. Data practices and context must be assessed according to case-specific data subject expectations. Amazon, for example, may pursue a high degree of customization in line with consumer expectations, with or without explicit choices, given its clear messaging about customization and friendly user interface; whereas travel site Orbitz will surprise users when tailoring specific kinds of travel offers to their browser type.[20] As Professor Nissenbaum put it: "Although the online bookseller Amazon.com maintains and analyzes customer records electronically, using this information as a basis for marketing to those same customers seems not to be a significant departure from entrenched norms of appropriateness and flow. By contrast, the grocer who bombards shoppers with questions about other lifestyle choices—*e.g.*, where they

[18] Helen Nissenbaum, Privacy as Contextual Integrity, 79 WASH. L. REV. 119 (2004). *Also see* Helen Nissenbaum, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (Stanford Law Books 2009). The Federal Trade Commission adopted this approach in its Report on Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, March 2012, http://ftc.gov/os/2012/03/120326privacyreport.pdf.

[19] This is the upshot of the narrowing of the "legitimate interests" basis for processing under the Rapporteur's Report; proposed Article 6(1c)(c).

[20] Dana Mattioli, On Orbitz, Mac Users Steered to Pricier Hotels, WSJ, Aug. 23, 2012, http://online.wsj.com/article/SB10001424052702304458604577488822667325882.html.

vacationed, what movies they recently viewed, what books they read, where their children attend school or college, and so on—does breach norms of appropriateness."[21]

Under the contextual approach, data use practices are not evaluated in a vacuum. Criteria such as the size of an organization, the number of data subjects or the breadth of data under its control are not dispositive. Rather it is the context of a transaction or relationship, as shaped by data subject expectations that legitimizes data practices. For example, an individual using a device marketed by a social networking service reasonably expects such a device to be embedded with data sharing features. And while an individual's sneakers are not ordinarily expected to communicate with the individual's phone; if Nike sold a Nike branded smartphone, individuals would likely expect that it communicated seamlessly with their bluetooth-enabled Nike shoes.

Legitimate Interests

In order to maintain a zone of individual empowerment while not stifling innovation and highly beneficial data uses, the role of consent should be demarcated according to normative choices made by policymakers. Instead of repeatedly prompting individuals to make difficult choices, policymakers should assess which activities are socially desirable and spell out default norms accordingly. In some cases, consent should not be required;[22] in others, consent should be assumed subject to a right of refusal; in specific cases, explicit consent should be necessary to legitimize data use. The classification of data uses into the appropriate categories should be based on a context-specific analysis weighing the risk of a given data use to individuals' privacy against its expected value; assessing the sensitivity of the information; and distinguishing between uses that benefit individuals, organizations, and society at large.

In fact, the EU framework already accommodates such collective and contextual determinations through the "legitimate interests" clause. However, the legitimate interests test is not fully developed and fails to provide organizations with the legal certainty and predictability required to support a viable business model. This, in turn, drives organizations to revert to individuals' consent.

The legitimate interest test is rife with ambiguity and delicate balancing acts. Under the test, organizations must decide what is a "legitimate" interest; balance such interest against "the interests or fundamental rights and freedoms of the data subject" ("in particular where the data subject is a child"); be prepared to withstand an "objection" by the data subject under Article 19 of the GDPR; in which case they would need to prove "compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject." Reliance on "legitimate interests" is always contestable and requires

[21] Nissenbaum, *supra* note 18, at p. 152-53.

[22] Under the OECD Privacy Guidelines, for example, consent is not required for every type of data collection. The "Collection Limitation" principles states: "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." OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA, Sep. 23, 1980, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html (*emphasis added)*.

organizations to justify their actions on a case-by-case basis. In other words, the "legitimate interests" test does not scale. Clearly, in order to operationalize "legitimate interests," organizations must be provided with clear and concrete guidance from regulators.

The Rapporteur's Report attempts to limit "legitimate interests" into a finite set of acceptable criteria.[23] Alas, in doing so, it eviscerates the ability of controllers to rely on legitimate interests in their processing, narrowing the test to "exceptional" circumstances; ruling it out for cases of profiling; and requiring controllers to inform data subjects and to "publish the reasons" as to why their legitimate interests override data subjects' "interests or fundamental rights and freedoms."[24] Under proposed Article 6(1c)(c), legitimate interests may not be used to justify re-purposing of data, thus eliminating one of the primary reasons to rely on the test, *i.e.*, to expand the scope of consent-based processing. In addition, the Rapporteur's Report severely constrains the processing of data for "historical, statistical and scientific research purposes" purposes, to only "research that serves an exceptionally high public interests, if that research cannot possibly be carried out otherwise."[25] These excessive restrictions may prove highly detrimental for important public policy goals of the European economy.

Furthermore, the legitimate interest test has been difficult to apply given vast differences in its implementation among EU Member States. Spain, for example, completely failed to transpose Article 7(f) of the DPD and has recently been ordered to do so by the European Court of Justice.[26] If the legitimate interest test is to become useful, increased harmonization will be required not only at the level of Member State legislation but also with respect to implementation on the ground. As explained in our white paper on jurisdiction and applicable law, even with a consistency mechanism, the approaches of national data protection authorities, each with its own enforcement and investigatory powers, are likely to vary, meaning that companies will remain subject to conflicting interpretations or applications of the law.[27]

Given the stiff requirements for consent and in the absence of additional clarity with respect to the legitimate interest clause, a new legal basis should be added to the GDPR to authorize the processing of pseudonymized data without data subject consent. This would incentivize organizations to implement pseudonymization and prevent the usage of authenticated identities strictly in order to prove compliance with the consent provisions of the GDPR. Such use of authenticated identities by organizations that currently use pseudonymized data could be detrimental to data subjects' privacy. It would violate the spirit, if not the letter, of Article 10 of the GDPR, which provides that "[a] controller shall not be obliged to acquire

---

[23] The Rapporteur's Report, proposed Articles 6(1a) – 6(1)(c).
[24] The Rapporteur's Report, proposed Article 14(1)(bb).
[25] The Rapporteur's Report, proposed Article 81(2a).
[26] Joined cases C-468/10 & C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) v. Administración del Estado, Judgment of the Court (Third Chamber) of 24 November 2011, http://curia.europa.eu/juris/document/document.jsf?text=&docid=115205&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=44742.
[27] Future of Privacy Forum, White paper, OVEREXTENDED: JURISDICTION AND APPLICABLE LAW UNDER THE DRAFT REGULATION (January 2013).

additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation."

Additional Concerns

Burden of proof. Imposing the burden of proof on organizations to show and document individuals' consent will require them to redesign systems and processes in a manner which could be detrimental to individuals' privacy. As discussed above, in order to evidence individuals' consent, organizations will have to authenticate users' identities and retain information in identified form for extended periods of time (*e.g.*, as long as a user is active plus the statute of limitations period). This unintended consequence, which is inconsistent with the thrust of Article 10 of the GDPR, should give policymakers cause for concern when assessing the costs of Article 7(1) of the GDPR.

Right to withdraw. Article 7(3) of the GDPR requires that individuals have a right to withdraw their consent at any time. The business model whereby individuals receive services for "free" in return for use of their personal data has become an increasingly attractive value-proposition for consumers in online and mobile markets.[28] In this context, individuals' decisions to retrench on their promise and withdraw their consent may disrupt binding transactions and innovative pricing models (*e.g.*, where a tablet is sold at a discount in an "ad-supported" mode and a user then decides to cut off data flows for ads). Accordingly, the requirement in Recital 33 that individuals can "withdraw consent without detriment" must be qualified; since individuals cannot expect to reap the benefit of the bargain once they have rescinded their part of the deal. In addition, the legal effect of such withdrawal must be strictly prospective. Organizations should not be expected to delete information that is maintained for purposes such as compliance with legal obligations or protection from potential legal claims.

Imbalance of power. Article 7(4) of the GDPR preempts the use of consent "where there is a significant imbalance between the position of the data subject and the controller." The introduction of such cryptic language into the consent provision would be counterproductive. Arguably, almost every interaction between controller and data subject features an imbalance of power. Such is the case in the relationships between state and citizen, employer and employee, and vendor and customer. Indeed, data protection law was devised to mitigate imbalances of power.[29] Predicating the validity of consent on the absence of such an imbalance is tantamount to putting the cart before the horse.

Contract conditional on consent. The Rapporteur's Report would prohibit reliance on consent for processing where "execution of a contract or the provision of a service [is] made conditional on the consent to the processing or use of data that is not necessary for the execution of the contract or the provision of the service."[30] Such a restriction would obstruct the dominant business model of the digital economy whereby (for-profit) businesses provide

[28] Chris Anderson, FREE: THE FUTURE OF A RADICAL PRICE (2009).
[29] Daniel Solove, Privacy and Power: Computer Databases and Metaphors for Information Privacy, 53 STAN. L. REV. 1393 (2001).
[30] The Rapporteur's Report, proposed Article 7(6).

consumers with valuable services for free in return for use of personal data.[31]

Conclusion

The Future of Privacy Forum supports measures to provide individuals with greater transparency, choice and control over their personal data. However, by restricting organizations' ability to rely on implied consent without at the same time simplifying the "legitimate interest" test, the GDPR elevates form over substance. Much like the amended cookie provisions in the e-Privacy Directive, this will result in formalistic compliance without delivering individuals meaningful transparency and control. Consent should not be treated as a one-size-fits-all model; it should be tailored to the context of a relationship or transaction and tied to the sensitivity of the data as well as the societal value of its use. In light of the restrictive approach to consent and unpredictable nature of "legitimate interests", a new legal basis should be added to the GDPR to authorize the processing of pseudonymized data without consent.

[31] Chris Anderson, FREE: THE FUTURE OF A RADICAL PRICE (Hyperion Books, 2009).