A HOOVER INSTITUTION ESSAY

The Discourse of Control and Consent over Data in EU Data Protection Law and Beyond

ELETTRA BIETTI

Aegis Series Paper No. 2001

"Taking back control" seems to be the leitmotif of our time. Brexiteers invoked the slogan in their Brexit referendum rhetoric.[1] Privacy advocates and journalists such as Charlie Warzel have claimed it as part of a move to gain back control over data flows or to clarify privacy's meaning.[2] Facebook founder and CEO Mark Zuckerberg has relied on the notion of "privacy controls" to market new user-privacy options.[3] And social enterprises or start-ups such as Solid/Inrupt are relying on the notion of "individual control" to explain and justify their business models.[4] In the United States, a core pillar of the recent and much celebrated California Consumer Privacy Act,[5] an instrument that epitomizes what Daniel Solove has called "privacy self-management,"[6] is individual control over personal data.[7] The European Union's General Data Protection Regulation (GDPR), which came into force in May 2018, is also strongly anchored in notions of control and consent.[8] Much of the recent data protection case law in Europe in fact focuses on criteria for informed consent to the exclusion of questions about how to minimize data processing and how to enforce meaningful privacy guarantees by design and default.

The emphasis on individual control can hardly be explained only by the wording of the GDPR itself, let alone by how effectively consent and user control can protect consumers. In fact, these notions have a rhetorical and ideological pull that obfuscates concerns about users' privacy, instead of protecting users. When it comes to data governance, the emphasis on individual control and privacy self-management shifts the regulatory burden on users, who are often unaware and vulnerable to interface design manipulation, leaving the industry free to engage in data collection, profiling, and other processing activities that lawmakers and regulators should be scrutinizing more thoroughly. By shifting the burden of governance on users, consent and control serve the industry's interests, making systemic privacy and data governance questions appear intractable.

It is striking how prevalent individual consent, disclosure, and user control over personal data are in GDPR interpretations by data protection authorities, courts, and other actors. Across data protection, antitrust, and other areas of EU law, decisions and reports emphasize the importance and centrality of informed consent and user control, without asking whether such centrality is a fair, effective, and justified policy choice. This trend is all the

more puzzling since the GDPR is not limited to individual control–centric provisions and includes procedures for carrying out data protection impact assessments and for encoding data protection by design and by default in platform infrastructures. If effectively utilized, such tools could reduce the burden on individual users and lead to fairer data governance.

My aim in this paper is to show that some of the outwardly bold stances being taken under the GDPR are therefore not bold enough. Instead of relying on the full spectrum of provisions available, and instead of highlighting the need for data governance alternatives, focusing on the implausible rhetoric of informed consent is leading regulators in the wrong direction. It furthers the interests of the industry to the detriment of consumers. The current emphasis relies on a chimeric view of the possibilities of informed consent which is not realistic in the platform economy. Further, it obscures key interpersonal dimensions of data privacy and systemic data governance problems by making them appear irrelevant, intractable, or secondary.

After briefly providing background on the role and rhetoric of consent and control in EU data protection law and offering some objections to it, I consider three examples that illustrate how this language is reflected in GDPR case law and beyond. These are but three instances of a wider trend. They are intended to show that this language is employed in relation to a wide range of issues, from behavioral advertising and competition to misinformation and fake news. This rhetorical leakage is not always in consumers' best interests and leads to unwarranted gaps in protection. Ultimately, focusing on consent and control falls short of protecting individuals against serious privacy intrusions by private corporations both in Europe and in the United States. It undermines regulatory efforts, impoverishing EU regulators' conceptual toolbox and limiting their scope of action. I conclude with some thoughts about an alternative path.

Individual Consent, Control, and Choice

Consent and Control in European Data Protection Law

The right to have control over one's personal data[9] is implied in the right to protection of personal data under the EU Charter of Fundamental Rights.[10] Recital 7 of the GDPR provides, "Natural persons should have control of their own personal data."[11] Recital 75 emphasizes that loss of control over personal data is a harm to be prevented or deterred:

> The risk to the rights and freedoms of natural persons . . . may result from personal data processing which could lead to physical, material or non-material damage, in particular . . . where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data.[12]

Notions of control and consent are very closely related. As the Article 29 Working Party, an EU advisory body on data protection—now replaced by the European Data Protection

Board—put it: "The notion of consent is traditionally linked with the idea that the data subject should be in control of the use that is being made of his data."[13] When a company requests a person's informed consent, it purports to allow that person to exercise *control* over the data and over the company's data processing practices. Yet whether consent effectively enables meaningful control in the data economy is questionable. Merely being asked to consent to a practice does not give individuals a meaningful say over that practice and does not provide a means to choose alternative options. This is especially the case when dealing with large and monopolistic technology companies. These companies have access to very large amounts of data about individuals. They experience little, if any, competition and they take advantage of the fact that consumers opt in to whatever practices the law allows them to engage in.

When the GDPR came into force in May 2018, it repealed the previous data protection regime and introduced a radical reconfiguration of privacy protection worldwide.[14] It reinforced the requirements for informed consent and introduced new inalienable data subject rights that cannot be waived by consent.[15] Those rights include expanded rights to access information about the personal data being processed, the right to be forgotten, the right to data portability, and the right to human intervention in AI-based decision making. The GDPR also introduced innovative means of facilitating compliance, such as the establishment of internal codes of conduct[16] and the carrying out of data protection impact assessments (DPIAs), a process whereby companies must describe and evaluate aspects of the firm's data processing practices likely to result in high risk under the GDPR.[17] These can include the profiling and scoring of individuals, the use of AI systems that do not include a human in the loop, the processing of sensitive data, or processing on a large scale.[18] Certification mechanisms were also envisaged as a way to facilitate small and medium businesses' compliance with the GDPR and consist in the creation of data-protection seals and marks overseen by certification bodies.[19] Perhaps most important, Article 25 on data protection by design and by default demands that companies set up appropriate internal technical measures such as data-minimization standards and means of ensuring that only data necessary to carry out a given purpose are used for that purpose.

While all of these procedures and rights bring about a needed transformation for privacy compliance and have the potential to generate greater transparency and auditing, the criteria of informed consent under Articles 6 and 7 have attracted a disproportionate amount of regulators' attention. There has been no litigation around aspects such as privacy-minimization standards and DPIAs.

Informed consent under the GDPR is only one of seven possible bases for legitimating data processing.[20] Yet it is the widest basis that businesses can rely on to justify their activities. The GDPR defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him

or her."[21] To be valid under the GDPR, an expression of consent must be informed, specific, and unambiguous, meaning that presenting individuals with pre-ticked boxes or bundling consent with other actions would not be sufficient.[22] Consent must also be freely given, meaning that it must provide individuals with real choice and control without coercion.[23]

Article 7 of the GDPR, which specifies additional conditions for the validity of consent, adds that in assessing whether consent is freely given, it is important to consider whether the processing was necessary to offer the service in question. The more peripheral the data a company seeks to acquire is to the services it provides, the more burdensome the disclosure it must provide. Article 7 also specifies that there is a right to withdraw consent at any time[24] and that personal data-related information must be disclosed in a manner that is clear, intelligible, easily accessible, and distinguishable from other matters.[25]

The requirements for valid consent under the GDPR appear very robust. But these robust and idealized criteria—which assume that free, autonomous digital consent is possible—obfuscate how toothless the requirement is in fact. EU data protection law as it exists today, characterized by a strong emphasis on informed consent on the one hand and data subject rights on the other, is grounded in the normative intersection of control, consent, and choice. Both consent and data subject rights signal an emphasis on—and a belief in—individual autonomy and individual rights to the detriment of collective forms of data and privacy governance. The lack of interpretation and focus on questions such as data protection by design and by default illustrates the general trend. As the GDPR's scope and mode of application are progressively clarified through the intervention of courts, regulators, and civil society, among others, the strong ideological and rhetorical pull of consent and control is becoming increasingly evident. In the long run, this will benefit companies more than consumers.

Normative Underpinnings of Control, Consent, and Choice

The rhetoric of individual control, consent, and choice in relation to privacy is ubiquitous. Charlie Warzel defines privacy as being "about how data is used to take away our control."[26] Last year, Zuckerberg, among other tech CEOs, announced that Facebook would be offering "privacy controls" in response to the GDPR.[27] A number of scholars have provided normative justifications for the claim that privacy is a right to individually control personal information.[28] For Charles Fried, for example, privacy is "the control we have over information about ourselves."[29] But there is more to data privacy than individual control over how one's information is shared. Helen Nissenbaum and Julie Cohen have highlighted that there are important interpersonal dimensions to how data is experienced and accessed. Focusing on individual control obscures and ultimately neglects those dimensions, to the detriment of individuals and society as a whole.[30]

The emphasis on control and consent seems to be premised on a faith in individuals as the ultimate and best decision makers. When the law requires consent to data processing in order to allow that data processing, it assumes that the matter is such that a consumer can adequately deliberate alone and that the individual is free and uncoerced from external factors pertaining to the design and infrastructure of the platform economy. The trouble is that individuals are hardly fully autonomous and data is hardly always of that renounceable kind, for two reasons. First, technological devices and systems can collect and process data about a variety of individuals at once and the consent of some may result in consequences that affect others. This is what Maggie Koerth-Baker called the "privacy of the commons" problem, defining it as:

> what happens when one person's voluntary disclosure of personal information exposes the personal information of others who had no say in the matter. Your choices didn't cause the breach. Your choices can't prevent it, either. Welcome to a world where you can't opt out of sharing, even if you didn't opt in.[31]

If privacy is a value strongly contingent on the interpersonal and social dimensions of collective life, then privacy self-management through choice and consent may be insufficient for regulating data and defining privacy's limits. Second, given the opacity of the technological landscape and data ecosystem and the absence of a radical reconsideration of the internet's basic functions, assuming that individuals are always well placed to deliberate on their data and privacy is assuming too much. Yet taking informed consent as a basis for lawful data processing and limiting the analysis to the requirements of informed consent instead of evaluating whether the circumstances within which consent is given are appropriate is precisely taking for granted this universal, individual decision-making capacity.

Applications and Ripple Effects

Control as Disclosure and Transparency: French CNIL Decision against Google of January 2019

The first national decision finding that a large technology company had violated EU data protection rules was that of the French Data Protection Commission (CNIL) on January 21, 2019, against Google. The commission imposed a fine of 50 million euros over Google's failure to comply with the requirements for valid consent under the GDPR.[32]

The ruling consists of two parts. First, CNIL ruled that Google had failed to comply with its obligation to provide users with access to transparent information about data processing. It found that the information available to users was too disseminated and that it was not clear and comprehensive. Users did not have convenient, centralized access to information about the purposes of data processing, the modalities of storage, and the types of personal data used in targeted advertising. The information was instead disseminated across several different documents, sometimes requiring five or six steps for a user to get

relevant information on his or her data. Furthermore, the information provided by Google was not always clear or comprehensive. Google's processing operations span about twenty services and entail the collection and use of a wide range of information including (a) data directly provided by users, such as name and date of birth, (b) data generated through a user's activities, such as geolocation, and (c) data inferred about a user on the basis of other available information, such as an interest in baseball or religious faith. CNIL found that the information Google provided to users was too generic and vague to properly notify individuals of the type of processing they had been subjected to.

Second, CNIL found that Google failed to obtain valid consent from users, and thus failed to engage in lawful processing when it relied on consent as a basis for lawfulness under the GDPR. Consent was considered invalid for two reasons. First, it was not sufficiently informed: as explained above, the information provided by Google to its users was lacking in accessibility and clarity. Second, consent was found to be insufficiently "specific" or "unambiguous." When creating an account, users could click on the button "more options" to access certain data processing defaults and untick them. However, CNIL considered that a link that sent the user to a page with pre-ticked boxes opting them into ad personalization defaults placed an excessive burden on users' ability to control processing. Under those circumstances, consent to the defaults could not be considered specific and unambiguous.

CNIL's requirements on information access, transparency, and consent in this case appear weak on at least two fronts. First, they are highly design dependent. CNIL grounded its ruling in the finding that information was not available on a single page, and that it was presented in the form of links to other pages and required a number of steps to be accessed. Google could decide to simply change its design and make the CNIL decision obsolete. In other words, the decision is too contingent upon easy-to-fix technical elements and is therefore weak overall.

Second, complete information is a fiction. Pursuing the ideal of informed consent falls short of creating a more just ecosystem for users absent additional or alternative measures. In spite of this and subsequent decisions on transparency and disclosure, individuals will never get access to enough information and in sufficiently accessible form to be fully informed. As highlighted by a number of behavioral economists and lawyers, this could be because of humans' own physical incapacities or because of constraints on companies' ability to disclose, which fall outside the scope of data protection authorities' competence. Such constraints may be due to trade secrets, language barriers, or availability of corporate resources.

The main concern, however, is not that ideal informed consent is impossible but rather that even if it were possible, consumers would still be left with no alternatives and no choice in the absence of greater oversight over the activities of these companies and of greater competition. Unless alternatives are available, users will keep accepting the terms set by

Google and others no matter what these terms say. Adopting formal, top-down constraints to govern the tech company–user relationship and encouraging greater scrutiny around the background conditions of choice would better protect individuals' freedoms, even when these constraints fall short of giving them facial and direct "control" over data.

Control as Freedom from Unequal Bargaining: German Bundeskartellamt Decision against Facebook of February 2019

In February 2019, not long after CNIL's decision, the German Competition Authority (Bundeskartellamt) also weighed in on the issue of control and consent, this time in a competition law case.[33] The Bundeskartellamt found that Facebook had violated German antitrust law by forcing those who wanted to access the platform to accept certain data collection and use practices, in breach of data protection law. These practices included the combination of data gathered through Facebook-owned services such as WhatsApp and Instagram, as well as non-Facebook-owned third-party websites, all in one Facebook user account. Much of the Bundeskartellamt's opinion was premised on user control and consent. In the authority's words, "There is no effective consent to the users' information being collected if their consent is a prerequisite for using the Facebook.com service in the first place"[34]; and "The damage for users lies in a loss of control: they are no longer able to control how their personal data are used."[35]

After finding that Facebook was dominant in the German market for social networking services, with a 95 percent market share of daily active users, the Bundeskartellamt found an abuse of dominance under EU competition law. Facebook abused its dominance because its data policy allowed the collection of user- and device-related data from a variety of external sources and because it conditioned user access to the platform on the company's ability to combine data from various Facebook and non-Facebook sources in one profile.

The Bundeskartellamt's foundational philosophy in this case was that "data protection law provides the individual with the right to decide freely and without coercion on the processing of his or her personal data."[36] The competition authority indeed relied on EU data protection law as the standard for determining whether Facebook's practices were abusive. It ruled that consent could not be deemed voluntary and freely given if users were consenting for the sole purpose of concluding a contract with a dominant undertaking, absent alternative contractual terms, and thus that consent here was not valid. Since there were also no alternative grounds for legitimating data processing under Article 6 of the GDPR, the Bundeskartellamt concluded that Facebook's practice violated data protection law.

The further step the Bundeskartellamt took in its analysis was to consider Facebook's violation of data protection sufficient evidence of an abuse of dominance. It reasoned that under German law, a finding of abuse of dominance requires a causal connection between

market dominance and the violation of German and data protection law. The authority offered two reasons for its causality finding. First, consent could not be considered as voluntary and freely given, precisely because Facebook was dominant in the market for social networking services. In the Bundeskartellamt's view, if users had had more options to avoid Facebook's collection and processing of combinations of data, valid consent would have been possible. Second, those unlawful contracts allowed Facebook to access, collect, and benefit from larger amounts of data than its competitors and arguably larger amounts of data than its users would agree to. The authority did not consider the particulars of how Facebook's exploitative data policies can harm individuals other than stating that the combination of these factors undermines users' ability to "decide autonomously on the disclosure of their data."[37] In other words, again, the competition harm in question is a loss of users' control over how their data is processed.

In its focus on consent and loss of control, the decision appears to go both too far and not far enough. It goes too far, in the eyes of many competition lawyers, because it subsumes questions of data protection within the competition-law analysis. This move has been harshly contested on the grounds that it conflates two fields of enquiry, implicates questions that competition law is unequipped to address, or leads to unnecessary jurisdictional complexities.[38]

The authority's approach does not go far enough because it leaves unanswered at least two series of questions. First, if users have no choice but to agree to Facebook's terms, is the abuse constituted by the fact that users are forced to consent to an agreement with a monopolist, or is the abuse constituted by the unconscionable terms included in that agreement? The answer of the Bundeskartellamt appears to be the latter: dominance or unfair contractual terms alone could not constitute an abuse, but the combination of market power and no choice over contractual terms did. If the terms of users' contract with Facebook had been fairer—e.g., if users had been given more options with respect to how their data is collected—then their consent would possibly have been voluntary under data protection law and there would have been no abuse, despite Facebook's dominance. The decision is about users' control over the terms of their relationship with the platform, not about control over whether or not to enter into the relationship itself.

The second question is whether this decision's remedies are plausible. A power imbalance, which the authority seems to recognize, requires more than the remedy it puts forward in this case, i.e., consumer options to accept or reject Facebook's combinations of personal data across different Facebook services and the web. If individuals have reason to resist the kinds of data combinations that Facebook obliges them to accept because they are abusive, then more options or awareness will not address the issue: users will keep opting in to the choice that is least burdensome for them among those that Facebook deems tolerable. Meaningful choice and control imply an ability to negotiate or walk away, which users do not realistically have in the platform context. What is needed are more effective restrictions

on Facebook's ability to engage in limitless data collection and data combination practices and the prohibition of harmful practices, not simply more options for consumers.[39] While the Bundeskartellamt may lack the competence to engage in structural regulation without the intervention of additional actors, it would have been possible for it to impose behavioral measures that went beyond the requirement to provide "more consumer choice." Such actions could have included banning certain behavioral advertising and political targeting practices, which could have been welcome in cases like this one.

Issuing decisions that focus on "voluntary consent" as the desired goal makes authorities vulnerable to responses, such as Facebook's public response in this case, that users in fact have a lot of choice on these markets and that other options are only a click away.[40] No matter what we think about the decision's political importance, validity, and general ethos, for reasons outlined throughout this paper, focusing on individual consent and on increasing control and choice is a red herring that fails to adequately protect individuals.

Content DIY and Control: EU-Level Efforts on Speech and Misinformation

The language of individual consent, control, and choice also features heavily in the domain of speech regulation, both in relation to and independently from data protection matters. Here, too, individual user control is referred to as a panacea. But in fact that means different things in different contexts, is not always desirable, and has the potential to obscure broader debates about how to render individual online choices truly meaningful.

Even in areas without direct connections to the GDPR, the language of control is pervasive. An example is the Final Report of the EU High Level Expert Group on Fake News and Online Disinformation (HLEG). One of its ten guiding principles for online speech reads:"Platforms should make available to their users advanced settings and controls to empower them to customise their online experience."[41] In the report, the expert group develops this point further, e.g.:

> Platforms should consider ways to encourage users' control over the selection of the content to be displayed as results of a search and/or in news feeds. . . . Content recommendation systems that expose different sources and different viewpoints around trending topics should be made available to users in online platforms. Such system should provide a certain degree of control to users.[42]

This is somewhat confusing. One of the problems of algorithmic recommender systems is precisely that they take away some of our human ability to understand how and why certain pieces of highly relevant or addictive content have appeared on our screen. Would more choice among several kinds of recommender systems really empower individuals or would it simply signal a surrender of ambitious regulation to echo chambers and speech bubbles? If the former, is this the form of empowerment we want going forward? Can choice

of recommender systems ever protect fundamental rights? What would control actually mean in the digital sphere? How can we foster a healthier information ecosystem over which we can exert actual collective self-determination? It seems important to be clearer as to the ultimate goals of regulation in this context, especially when one is advocating for greater transparency overall, as the HLEG is doing.

"Control" is also referred to in the latest European Data Protection Supervisor's Opinion on online manipulation and personal data, yet with a different connotation:

> The concern of using data from profiles for different purposes through algorithms is that the data loses its original context. Repurposing of data is likely to affect a person's informational self-determination, further reduce the control of data subjects' over their data, thus affecting the trust in digital environments and services.[43]

Thus, according to this view, algorithms may undermine control, and loss of control is correlated with a loss of trust. Similarly:

> Data brokers, advertising networks, social network providers and other digital business actors have ever more complete files on individuals participating in today's digital society, and individuals are losing control over the digital footprints they leave behind. Targeted, profiled and assessed by actors often beyond their control or even knowledge, individuals may feel helpless and need to be empowered to take control of their identity. Even where formally having been given some form of a "notice" and opportunity to "consent" to general terms and conditions, individuals often find themselves inside a system designed to maximise the monetisation of personal data, which leaves no real choice or control to individuals.[44]

Here control is used as a synonym of freedom: users have lost control, because they have lost the freedom to opt out of a system that diffusely determines the course of their lives. They have also lost the freedom or the power to collectively determine that course. We should rebuild a richer meaning of control by starting from this realization.

The Road Not (Yet) Taken

To use a term coined by Margot Kaminski, the GDPR is an instrument of "binary governance"[45]—it is centered around a system of individual due-process rights and notice and consent mechanisms, yet also contains a number of provisions that incentivize voluntary compliance, opening the door to new forms of auditing, of collaborative governance, and of private-public partnerships. These provisions include soft requirements to establish codes of conduct, to carry out data protection impact assessments, and to put in place infrastructure to incentivize the minimization of data collection and use. While

litigation and regulatory case law clarify the conditions for valid informed consent, and as the exercise of data subject rights is increasingly explored as a strategy for advancing digital justice,[46] insufficient focus is being placed on these other aspects of the GDPR, which remain unspecified and untested. Companies are encouraged to use these mechanisms, but the risk of suffering fines for lack of compliance with them remains theoretical. Aspects that are not covered by the GDPR—such as the need to design more consistent ongoing regulatory oversight over data-driven business models—are being substantially ignored. In parallel, in areas such as the regulation of speech and disinformation, simple user control–based fixes have for long been myopically advanced to address systemic polarization and radicalization questions.

The current quasi-exclusive focus on consent and individual control over data and information may be temporary. Complex collaborative governance mechanisms take time to put in place and clarify. Misinformation is a hard problem that might require personalized online experiences as a first step. This article, however, argues that it is not just a question of time. The focus on fixing consent and making it as free and informed as possible, the focus on letting us individually control information about ourselves and others, is not a mere first step in a longer process toward better data and information governance. The belief in the effectiveness of individual-centric solutions is here to stay. It favors the interests of the industry, which does not want burdensome requirements around data collection and use to be imposed from the outside. It is rhetorically and ideologically entrenched.

So we are left with notice and consent, and voluntary compliance mechanisms. The imperative to go further is obscured. We need, instead, to start thinking of ways to regulate the information economy that go beyond individual rights and voluntary compliance but that consider the kinds of data processing activities that are too harmful to be tolerated by a modern democratic society. We need to think of new forms of collective, rather than individualized and fragmented, self-determination. The questions we should be asking at this historical moment are, for example: Which kinds of data or data uses are beneficial and good for people? Which kinds of data or data uses are instead harmful and should be banned? Which kinds of data uses can be tolerated and subjected to market-based preferences? The emphasis on consent and control too often prevents us from taking these questions seriously. We are made to believe that these questions are intractable, that they go too far, which curtails our engagement and ability to push for change.

Conclusion

This paper provides a bird's-eye view of recent developments in EU data protection regulation, including its rhetorical leakage into competition enforcement and the language used in misinformation policy documents. It argues that EU data protection enforcers still focus excessively on consent and control and that this operates as an obscuring device for

all other forms of regulation. In order to actually protect individuals against objectionable privacy interferences by technology companies, such as behavioral advertising, misinformation, and other algorithmic harms, focusing on consent as a means of ensuring control over data generation, collection, combination, and use practices is a precarious endeavor. Further, understanding individual control and self-determination as the central goals of data protection and privacy is misleading in light of the complexity of the digital ecosystem and the collective nature of the data that can be linked to our persons. We must therefore ask again what kinds of control and self-determination we might want to secure for individuals, if at all, and then devise ways for such self-determination to become possible—not by contract, but by creating new feedback channels and devising novel ways for the community of users to weigh in on platform governance. Ultimately, there is an urgent need to ask better questions on how our data should be governed. Embedded as we are in discourses premised on entrenched faith in individual consent and control, we are prevented from asking these questions. This is not to say that the GDPR lacks potential. The possibilities it introduced can surely lead us some way toward a more transparent and fair data and platform economy. Yet thinking beyond the GDPR's central premises will be key going forward.

NOTES

1 Yasmeen Serhan, "In a Bid to 'Take Back Control,' Britain Lost It," *The Atlantic,* March 28, 2019, https://www.theatlantic.com/international/archive/2019/03/brexit-britain-control-may-eu/585940.

2 Charlie Warzel, "Opinion: Privacy Is Too Big to Understand," *New York Times,* April 18, 2019, https://www.nytimes.com/2019/04/16/opinion/privacy-technology.html.

3 See, e.g., Josh Constine, "Zuckerberg Says Facebook Will Offer GDPR Privacy Controls Everywhere," TechCrunch, April 4, 2018, http://social.techcrunch.com/2018/04/04/zuckerberg-gdpr. Google's privacy controls state that: "When it comes to privacy, we know one size does not fit all. That's why we build controls that are easy to use so you can choose the privacy settings that are right for you," Google Safety Center, https://safety.google/privacy/privacy-controls, accessed December 13, 2019.

4 See, e.g., Tim Berners-Lee's ideas for a new web in "Three Challenges for the Web, According to Its Inventor," World Wide Web Foundation, March 12, 2017, https://webfoundation.org/2017/03/web-turns-28-letter.

5 California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.198(a) (2018).

6 See Daniel J. Solove, "Privacy Self-Management and the Consent Dilemma," *Harvard Law Review* 126 (2013): 1880–1903.

7 See, e.g., Californians for Consumer Privacy, "About the California Consumer Privacy Act," https://www.caprivacy.org/about.

8 Regulation (EU) 2016/679, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [GDPR], *Official Journal of the European Union,* April 27, 2016 (L 119), Article 7, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1490179745294&from=en.

9 "Personal data" is defined at GDPR Article 4 as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

10 See Charter of Fundamental Rights of the European Union, *Official Journal of the European Union,* October 26, 2012 (C326), Article 8, which does not contain the specific language of individual control. Also see the European Data Protection Supervisor's website entry on "Data Protection": "In the EU, human dignity is recognised as an absolute fundamental right. In this notion of dignity, privacy or the right to a private life, to be autonomous, *in control of information about yourself,* to be let alone, plays a pivotal role. Privacy is not only an individual right but also a social value" (emphasis added), https://edps.europa.eu/data-protection_en.

11 GDPR, Recital 7.

12 GDPR, Recital 75.

13 Article 29 Working Party, *Opinion 15/2011: On the Definition of Consent,* July 13, 2011, 8, https://iapp.org/media/pdf/resource_center/wp187_definition-of-consent_07-2011.pdf.

14 Directive 95/46/EC, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, *Official Journal of the European Communities,* October 24, 1995 (L 281).

15 GDPR, Articles 12 to 23.

16 GDPR, Article 40.

17 GDPR, Article 35.

18 Article 29 Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679,* October 4, 2017, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

19 GDPR, Articles 42 and 43.

20 GDPR, Article 6(1)(a).

21 GDPR, Article 4(11).

22 On the question of specific consent and ambiguity, see Opinion of Advocate General Szpunar in CJEU Case C-673/17 of March 21, 2019, *Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände–Verbraucherzentrale Bundesverband e.V,* http://curia.europa.eu/juris/document/document.jsf?text=&docid=212023&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=5458852.

23 See, more generally, Article 29 Working Party, *Guidelines on Consent under Regulation 2016/679,* April 10, 2018, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

24 GDPR, Article 7(3).

25 GDPR, Article 7(2).

26 Warzel, "Privacy."

27 Constine, "Zuckerberg." Also see Google's privacy controls.

28 See, e.g., Alan Westin and Charles Fried's work on privacy as control; Paul M. Schwartz's work on privacy and its relation to property.

29 Charles Fried, "Privacy: A Moral Analysis," *Yale Law Journal* 77, no. 3 (1968): 475–83, 482.

30 Julie E. Cohen, chapter 5 in *Configuring the Networked Self: Law, Code and the Play of Everyday Practice* (New Haven, CT: Yale University Press, 2012); Helen Nissenbaum, *Privacy in Context: Technology, Policy and the Integrity of Social Life* (Stanford, CA: Stanford University Press, 2010).

31 Maggie Koerth-Baker, "You Can't Opt Out of Sharing Your Data, Even If You Didn't Opt In," FiveThirtyEight, May 3, 2018, https://fivethirtyeight.com/features/you-cant-opt-out-of-sharing-your-data-even-if-you-didnt-opt-in; after Garrett Hardin, "The Tragedy of the Commons," *Science* 162, no. 3859 (1968): 1243–48, https://science.sciencemag.org/content/162/3859/1243.

32 Commission nationale de l'informatique et des libertés [CNIL] [French Data Protection Commission], *Délibération de la formation restreinte n° SAN–2019-001 prononçant une sanction pécuniaire à l'encontre de la société GOOGLE LLC,* SAN-2019-001, January 21, 2019, https://www.legifrance.gouv.fr/affichCnil.do?&id=CNILTEXT000038032552.

33 Bundeskartellamt [BKA] [German Competition Authority], *Prohibition Decision: Facebook Inc. i.a.: The Use of Abusive Business Terms Pursuant to Section 19 (1) GWB,* June 2, 2019 https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.html?nn=3591568.

34 BKA, *Case Summary: Facebook, Exploitative Business Terms Pursuant to Section 19(1) GWB for Inadequate Data Processing,* February 15, 2019, 1, https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=3.

35 BKA, *Background Information on the Facebook Proceeding,* February 7, 2019, 5, https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook_FAQs.pdf?__blob=publicationFile&v=6.

36 See BKA, *Case Summary,* 8, https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=3.

37 BKA, *Background Information,* 12. This lack of detail on the meaning of exploitative terms was one of the grounds that led the German Regional Court to overrule the case on August 26, 2019; see "German Court: Facebook's Use of Non-Facebook Data, Even If a Privacy Violation, Is Not Anti-Competitive," *National Law Review,* September 8, 2019, https://www.natlawreview.com/article/german-court-facebook-s-use-non-facebook-data-even-if-privacy-violation-not-anti.

38 See, e.g., Jakob Kucharczyk, "The German FCO's Facebook Case: Blurring the Line between Competition and Data Protection Enforcement," Disruptive Competition Project, February 8, 2019, http://www.project-disco.org/european-union/020819-german-fcos-facebook-case-competition-and-data-protection-enforcement/; Geoffrey Manne, "Doing Double Damage: The German Competition Authority's Facebook Decision Manages to Undermine Both Antitrust and Data Protection Law," *Truth on the Market* (blog), February 8, 2019, https://truthonthemarket.com/2019/02/08/doing-double-damage-bundeskartellamt-facebook.

39 Although attempts to do so have failed in many instances. See European Commission decision of October 3, 2014, in Case COMP M.7217—*Facebook/WhatsApp* and subsequent breaches found by various national authorities.

40 Yvonne Cunnane and Nikhil Shanbhag, "Why We Disagree with the Bundeskartellamt," Facebook Newsroom, February 7, 2019, https://newsroom.fb.com/news/2019/02/bundeskartellamt-order.

41 European Commission Directorate-General for Communication Networks and Technology, *A Multi-Dimensional Approach to Disinformation: Final Report of the High Level Expert Group on Fake News and Online Disinformation,* March 12, 2018, 33, https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation.

42 European Commission, *A Multi-Dimensional Approach,* 28.

43 European Data Protection Supervisor (EDPS), *Opinion 3/2018: EDPS Opinion on Online Manipulation and Personal Data,* March 19, 2018, 15–16 https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf.

44 EDPS, *Opinion 3/2018,* 21.

45 Margot E. Kaminski, "Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability," *Southern California Law Review* 92, no. 6 (2019): 1529–1616.

46 Jeff Ausloos, "GDPR Transparency as a Research Method," May 3, 2019, abstract available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3465680.

26 25 24 23 22 21 20 7 6 5 4 3 2 1

The preferred citation for this publication is Elettra Bietti, *The Discourse of Control and Consent over Data in EU Data Protection Law and Beyond,* Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 2001, available at https://www.lawfareblog.com/discourse-control-and-consent-over-EU-data-protection-law-and-beyond

About the Author

MELISSA BLACKALL PHOTOGRAPHY

ELETTRA BIETTI

Elettra Bietti is a doctoral candidate at Harvard Law School studying the governance of information gatekeepers. She is also a Kennedy-Sinclair Scholar and an affiliate of the Berkman-Klein Center. She is currently based at Cambridge University and collaborates with Privacy International. Previously, she was an antitrust and intellectual property lawyer in London and Brussels. She is admitted to practice law in New York and England.

Working Group on National Security, Technology, and Law

The Working Group on National Security, Technology, and Law brings together national and international specialists with broad interdisciplinary expertise to analyze how technology affects national security and national security law and how governments can use that technology to defend themselves, consistent with constitutional values and the rule of law.

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cybersecurity, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The group's output will also be published on the Lawfare blog, which covers the merits of the underlying legal and policy debates of actions taken or contemplated to protect the nation and the nation's laws and legal institutions.

Jack Goldsmith is the chair of the National Security, Technology, and Law Working Group.

For more information about this Hoover Institution Working Group, visit us online at http://www.hoover.org/research-teams /national-security-technology-law-working-group.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
The Johnson Center
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200

HOOVER INSTITUTION