COMPETITIVE ENTERPRISE INSTITUTE

OnPOINT

May 23, 2018 **No. 245**

European Union's General Data Protection Regulation and Lessons for U.S. Privacy Policy

GDPR Threatens Innovation in America and Around the World

By Ryan Radia and Ryan Khurana[*]

The European Union's (EU) General Data Protection Regulation (GDPR), which enters into effect on May 25, 2018, is the most significant policy change regarding data collection and retention in history, with implications far beyond the EU. It could significantly impact any businesses or organizations in the United States and around the world that have any interaction with EU residents.[1] The GDPR will affect not only Internet companies, but also businesses that collect or process personal data in the offline world.[2] Worse, it will significantly harm competition and innovation not only in Europe, but around the world.

This will result in greater market concentration, as small firms and startups will find it difficult to comply with the increased regulatory cost burden. When considering new privacy legislation, American lawmakers should consider the GDPR's many flaws, and strive to avoid them.

The GDPR, which significantly updates the EU's 1995 Data Protection Directive,[3] aims to cover all aspects of "personal data" by expanding the term's definition to encompass "any information relating to an identified or identifiable natural person."[4] This definition of personal data, though simpler than the preceding one it updated, significantly increases the scope of data that is considered personal, encompassing information such as IP addresses and location data.[5]

The GDPR seeks to respond to the rise of "big data," a concept that refers to the data sets of high volume, variety, and velocity that have helped fuel technological innovation in the 21st century.[6] Technologies powered by big data, such as artificial intelligence (AI), have sparked concerns regarding privacy, control of user data, and potential monopolization of online commerce.[7] While the GDPR seeks to address some understandable concerns, the regulation is so broad in scope—clocking in at 99 articles over 261 pages[8]—that its various provisions conflict with one another in numerous ways. That is a recipe for unsound policy and regulatory confusion.

In the United States lawmakers from both major parties, most prominently Sens. John Kennedy (R-La.) and Amy Klobuchar (D-Minn.), have expressed interest in the GDPR in the wake of the alleged misappropriation of Facebook user data by the recently defunct political consulting firm Cambridge Analytica, which was based in Great Britain.[9] However,

[*] *Ryan Radia is a research fellow and regulatory counsel at the Competitive Enterprise Institute (CEI). Ryan Khurana is a recent research associate at CEI.*

before rushing to adopt GDPR-style regulation in the United States, lawmakers should consider the unintended consequences of such an all-encompassing regulatory regime. This paper discusses three significant implications of the GDPR:

1. Economic impact, including compliance costs;
2. Establishment of new, mutually contradictory "digital rights;" and goals; and
3. Obstruction of innovation.

GDPR's Economic Impact. The GDPR affects the vast majority of businesses that operate within the European Union, regardless of where they are located.[10] If a business processes the personal data of EU residents, it is subject to the GDPR, even if the data is processed outside the European Union.[11] The GDPR introduces numerous new supposed "rights," including the:

- **Right of portability**, which requires companies to export user data on request in a commonly used machine-readable format; and.[12]
- **Right of erasure**, which requires companies to delete a person's data at his or her request.[13]

These mandates have led companies around the world, including U.S. firms, to make major changes in how they handle data.[14]

While the GDPR was unveiled in 2016, giving businesses two years to reach full compliance, many businesses remain unprepared just weeks before the regulation goes into effect.[15] In the United Kingdom, for example, 70 percent of companies will likely face potential fines as soon as the GDPR enters into force.[16]

The new data protection framework contains so many new compliance criteria—to be implemented at once—that it prompted the wholesale redesign of many business practices. For example, advertising firms may no longer be able to rely on individualized targeting under the GDPR, which permits such tailoring only if users opt in.[17]

As with many top-down regulations, the GDPR will lead to compliance costs that restrict competition by unduly burdening small and mid-sized businesses across a variety of industries. For example, even email marketing, which many small businesses use to try to reach potential customers, can subject a business to GDPR rules. [18]

When crafting the GDPR, EU regulators apparently did not take into account the particulars of each industry.[19] For example, the automobile industry faces challenges due to the GDPR's erasure mandate, because a vehicle equipped with the latest technology will typically leave data on far-flung networks as it travels across cities or even countries.[20]

In response to the GDPR's burdensome requirements, a new compliance industry in data auditing has arisen to help companies navigate through the regulatory morass.[21] Fortune 500 companies are estimated by the International Association of Privacy Professionals (IAPP) and EY (formerly Ernst & Young) to have spent an average of $16 million to

comply with the GDPR in the two years leading up to its effective date, while mid-sized firms have spent an average of $550,000.[22] Despite these significant costs, the cost of non-compliance is potentially greater still, with fines of up to €20m ($23.86 million) or 4 percent of a company's global revenue—whichever is greater.[23]

Most of the GDRP's compliance costs fall on high tech and financial services firms, which almost invariably process and control user data and are thus required to hire a data protection officer[24]—a position that many companies have failed to fill to date due to a shortage of qualified applicants.[25] Meanwhile, many businesses remain unprepared. Non-tech firms that process or collect personal data are experiencing their own compliance challenges—including determining the extent to which the GDPR applies to them and what they will need to spend to comply with it.[26]

In addition, changing the terms and conditions governing data collection and use will endanger many popular and beneficial business models. The GDPR requires firms to:

- Use simple language;
- Describe how they use personal data;
- Ensure that users opt in to collection, and
- Obtain user consent before permitting any third parties to use their data.[27]

While these requirements may seem reasonable on their face, they are likely to result in a worse online experience for most users. By forcing websites supported by advertising to obtain express consent from users, the GDPR will result in EU subjects being inundated with pop-ups and similar warnings that users often fail to understand. As a result, users will see fewer ads that are relevant to their individual interests, while online services will suffer from reduced ad revenue on a per-user basis.

Under the GDPR, by default, a user must opt in to the collection and use of his or her information by Internet advertising networks, among other companies. While some users may prefer not to receive individualized ads, most users tend to stick with whichever default option is presented to them. In the advertising context, when presented with the option of opting in to persistent tracking—which allows advertisers to tailor ads to users as they browse online—the majority of users are reluctant to grant their consent.[28] This reluctance is at odds with users' general preference for ad-subsidized services and tailored advertisements.[29]

Similarly, to comply with the GDPR, Facebook will begin requiring EU users to opt-in to the social media platform's facial recognition feature.[30] In the United States, by contrast, Facebook's facial recognition feature is enabled by default.[31] Because consumers, when presented with multiple choices, typically stick with the default option, a likely consequence of Facebook's opt-in regime for EU users will be a reduction in the usefulness of its facial recognition feature for automatically identifying users in photos.[32]

The GDPR imposes a major new liability on data collectors, requiring that they provide a mechanism for authenticating users who want their data erased, along with a mechanism

for erasing the data.[33] Although economic relationships that either party may terminate at any time and for any reason are often desirable, such as in the context of at-will employment, other transactions become far less attractive when long-term agreements are forbidden, such as landlord-tenant relationships and many business-to-business service contracts.[34] By depriving users of the freedom to grant irrevocable or long-term consent to companies that process and control their data, the GDPR may actually diminish the value of user data—and, with it, users' ability to obtain beneficial goods and services in exchange for sharing information about themselves with third parties.

The GDPR's rules purport to enhance transparency, privacy, and security, but they would result in reduced consumer choice. When users are free to decide to share certain information with companies on an indefinite basis, companies can accumulate, acquire, and sell large data sets for a variety of purposes, from improving ad tailoring to building better models for pricing credit risk. The GDPR, however, would bar consumers from obtaining a valuable service in exchange for letting that company use their data for a fixed period of time. An April 2018 study by RMIT University in Melbourne, Australia, found that these stipulations will alter the economics of data-driven businesses by introducing considerable uncertainty around the value of personal data.[35] Under U.S. law, whether and when a user may revoke consent to the storage or processing of his or her data by a third party generally depends on the terms by which the user originally shared the information. But under the GDPR, a company that collects personal data can only speculate as to how long it will remain free to retain such data.[36]

As American consumers have seen from experience, a focus on notice and choice, rather than prescriptive mandates, has enabled new and innovative companies to form and thrive in the United States much more than in Europe.[37] Although many reasons explain the lackluster track record of high-tech entrepreneurship in Europe as compared to the United States,[38] the EU regulatory regime is among the major factors behind the greater success of Silicon Valley.[39] The previous European Data Protection Directive was more stringent than the U.S. regime, especially with respect to user consent requirements. That caused demonstrable harms to economic dynamism and the technology startup ecosystem.[40] For instance, implementation of past EU data regulations has contributed to a 65 percent reduction in the effectiveness of Internet advertising in the following months.[41] The GDPR will greatly add to these costs.

New "Digital Rights" and their Conflicting Goals. The GDPR introduces new "digital rights," many of which conflict with one another.

The first significant change is the right to data portability, which is aimed at reducing perceived "lock in" effects online.[42] The idea is that companies that exploit network effects to acquire more data online gain a competitive advantage, which makes it likely for them to remain dominant players.[43] There is little empirical evidence to support this claim, especially in light of the large number of once seemingly dominant online companies that have disappeared.[44] Yet, GDPR advocates argue that data portability will increase competition by reducing whatever network effects exist.

Allowing users to request all their data in a commonly used machine-readable format comes into conflict with another GDPR value called privacy by design, which calls for privacy to be considered at each stage at which any new product that involves individual data is developed.[45] Demanding that firms furnish each user a portable copy of their data on request creates a major point of vulnerability, especially given the potential for a malicious actor to impersonate a user or infiltrate a user's devices. To mitigate this privacy risk while complying with the GDPR, many companies will have to spend considerably more on security while redesigning their systems to create a new access point for certain types of user data.[46] Both of these options add significant costs onto companies, and cannot be neatly remedied into a unified framework. As Professor Gus Hurwitz of the Nebraska College of Law has noted, "the easier that [a company] makes it for its users' data to be exported at scale, the easier [a company] makes it for its users' data to be exfiltrated at scale."[47]

The right to erasure, an extension of the EU's controversial "right to be forgotten," poses significant challenges to freedom of expression.[48] The right to be forgotten, which was established in the EU prior to the GDPR, has already led to the censorship of truthful speech, especially given a recent ruling that forced Google to remove links to websites that accurately reported on the prior convictions of an EU-based businessman.[49] Since 2014, Google alone has received over 650,000 requests to remove websites from its search results pursuant to the EU's right to be forgotten.[50] The rule has hampered the ease with which data moves globally.[51] U.S. law does not recognize certain European digital rights, which has led to some U.S. companies being sued for moving EU residents' data to U.S. facilities.[52]

As U.S. policy makers consider GDPR-style regulations, they must consider the conflicts such rules pose not only with each other, but with more fundamental constitutional rights.[53]

How the GDPR Obstructs Innovation. GDPR rules risk hampering innovation in important ways beyond the large costs and technological complexities of compliance. Major disruptive technologies—including blockchain, artificial intelligence, and the Internet of things (IoT)—are all at risk of either delayed implementation or of being banned outright due to the measures in the GDPR. More stringent consent requirements will harm startups that need to access data to improve their products and grow their user base.

The GDPR's "data minimization" requirement would limit the freedom researchers have long enjoyed to harness large data sets to accomplish technological breakthroughs. Under the GDPR, data minimization allows companies to collect and store data only to the extent that it is necessary to render the services for which the data were obtained, and requires companies to seek additional user approval before using their data in any way not originally specified.[54] However, future beneficial uses of data are often unforeseen at the time of its collection. The freedom to experiment with data, including through serendipitous uses, is crucial to enabling innovation. Restricting collection and experimental use severely impairs innovation. In fact, many of the most successful online companies, such as Facebook, arose out of data experimentation for unrelated purposes.

Blockchain technology, which has major promising implications for areas from financial services to land registry, faces perhaps the greatest compliance risk under the GDPR. This

distributed ledger technology, best known for empowering the global cryptocurrency market, is predicated in large part on its "immutability"—the inability of users to alter items on the blockchain after they have been processed. This security feature conflicts with the right of erasure, because information on the blockchain cannot be destroyed.[55]

The public nature of blockchain, which allows for independent verifiability of transactions, comes into conflict with the GDPR's principles of privacy by design, given that the information is still potentially identifiable to an individual.[56] How these features of blockchain can be reconciled with the GDPR is yet to be seen. However, given the current global market cap of cryptocurrencies is in excess of $350 billion as of April 19, 2018, there is considerable forgone economic potential if these issues are not resolved.[57]

How the GDPR will affect artificial intelligence is less clear, as the regulations contain no single provision implementing the "right to explanation" for algorithmic decision-making, which holds that individuals affected by machine learning models have the right to understand how the model made its decision.[58] In the field of artificial intelligence, there is a clear tradeoff between a decision's interpretability and its predictive accuracy.[59] Therefore, the right to explanation reduces the ability to adopt more advanced and accurate algorithms, in favor of less accurate—but more interpretable—ones. This would discourage investment in more innovative AI techniques, as they would not be implementable on the market. In fact, some legal scholars and policy makers have inferred that such a right not only exists, but is potentially enforceable in the future.[60] The UK House of Lords recommended a right to explanation in its recent report on AI.[61] And given that interpreting the GDPR is left to individual EU member states, certain countries will likely adopt this new digital right, granting individuals an entitlement to receive a lay explanation of how an algorithmic decision was made, and the ability to human review of AI-based decisions.

If the GDPR's consent requirements are interpreted and enforced strictly, they will harm the adoption of the many Internet of things technologies that depend on linking disparate data sets.[62] Because IoT technology often requires linking different activities, new consent rules would require constant user verification of changes made, reducing the total accessible data set. In the UK, where consent requirements have been interpreted the strongest, the economics consultancy London Economics found that the requirements have caused firms to "move data collection and analysis in-house rather than outsourcing it to specialist analytics and data providers, thereby undoing the benefits of specialization and entrenching the market power of larger firms."[63] This presents increased barriers to market entry by startups and reduces the incentive to innovate.

Conclusion. The General Data Protection Regulation is the most significant change to the legal treatment of data in history, with implications that have already spilled well-beyond the European Union's borders. The rapid demand for implementing these sweeping policy changes has left companies unprepared for a complex set of legal and technological challenges. The economic effects will include greater market concentration, as small firms and startups struggle to comply, conflicting priorities for businesses, greater inconvenience for users, and reduced innovation. As the United States considers new privacy legislation, lawmakers should learn from the GDPR's many flaws, rather than adopting it wholesale.

Notes

[1] General Data Protection Regulation, approved April 14, 2016; in effect on May 25, 2018, https://gdpr-info.eu/.
[2] An ePrivacy Regulation targeting online businesses is in the process of securing approval in the European Union. Barry Levine, "Right behind the GDPR, there's the ePrivacy Regulation," *MarTech Today*, December 21, 2017, https://martechtoday.com/right-behind-gdpr-theres-eprivacy-regulation-208717.
[3] European Directive 95/46/EC, October 24, 1995, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.
[4] GDPR, ch. 1, art. 4.1.
[5] Thomas Jørgen Jacobsen, "GDPR: New definition of personal data and why it matters," RushFiles, August 25, 2017, https://rushfiles.com/blog/gdpr-the-new-definition-of-personal-data-and-why-it-matters/. Under the EU Data Protection Directive, personal data is defined as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." EU Data Protection Directive Ch. I, Art. 2(a).
[6] Big data is defined as data of high volume (quantity of data points), variety (quantity of data sources), and velocity (speed of data generation), which has enabled advanced analytics to develop new forms of business insights. The effective use of big data has vastly improved internal firm productivity and is associated with the rise of "superstar firms" that outcompete all rivals due to technological advantage. Ernst & Young Global Limited, "Big data: Changing the way businesses compete and operate," *EY Insights on Governance, Risk and Compliance*, April 2014, http://www.ey.com/Publication/vwLUAssets/EY_-_Big_data:_changing_the_way_businesses_operate/%24FILE/EY-Insights-on-GRC-Big-data.pdf.
[7] Concerns surrounding market power and potential abuse of big data by dominant firms in the new markets, such as the platform economy, has relied on a one-sided analysis. The forces behind the virtuous cycles that enable dominance also often work in reverse, so market dominance is temporary. "Why Winner-Takes-All Thinking Doesn't Apply to the Platform Economy," *Harvard Business Review* (May 4, 2016), https://hbr.org/2016/05/why-winner-takes-all-thinking-doesnt-apply-to-silicon-valley.
[8] See generally GDPR (99 articles).
[9] The Cambridge Analytica controversy led to Mark Zuckerberg, Facebook's CEO, testifying before both the U.S. House and Senate in April 2018. Shortly thereafter, Sens. John Kennedy (R-La.) and Amy Klobuchar (D-Minn.) introduced a bipartisan privacy bill that echoes many of the provisions of the GDPR. Li Zhou, Kennedy, "Klobuchar drop data privacy bill," *Politico*, April 24, 2018, https://www.politico.com/newsletters/morning-tech/2018/04/24/kennedy-klobuchar-drop-data-privacy-bill-181251. Cambridge Analytica ceased operations in May 2018 after filing for bankruptcy in the wake of the scandal involving Facebook user data. Nicholas Confessore and Matthew Rosenberg, "Cambridge Analytica to File for Bankruptcy after Misuse of Facebook Data," *New York Times*, May 2, 2018, https://www.nytimes.com/2018/05/02/us/politics/cambridge-analytica-shut-down.html.
[10] GDPR ch. 1, art. 3 (explaining territorial scope of the GDPR).
[11] Ibid.
[12] GDPR Ch. 3, Art. 20.
[13] GDPR Ch. 3, Art. 17.
[14] Thuy Ong, "Facebook announces new European privacy controls, for the world," The Verge, April 18, 2018, https://www.theverge.com/2018/4/18/17250840/facebook-privacy-protections-europe-world-gdpr.
[15] Tiffany Robertson, "Study finds organizations are not ready for GDPR compliance issues," Thomson Reuters Inside Financial & Risk, August 15, 2017, https://blogs.thomsonreuters.com/financial-risk/risk-management-compliance/study-finds-organizations-not-ready-gdpr-compliance-issues/.
[16] Emily Schimelpfenig, "Businesses and Data Protection: Are European Firms Ready?" European Policy Information Center, August 1, 2017, http://www.epicenternetwork.eu/blog/businesses-and-data-protection-are-european-firms-ready/.
[17] Laurie Sullivan, "A New Challenge for Ad Targeting: GDPR Compliance," MediaPost, January 15, 2018, https://www.mediapost.com/publications/article/312895/a-new-challenge-for-ad-targeting-gdpr-compliance.html.

[18] Bettina Specht, "GDPR: What Europe's New Privacy Law Means for Email Marketers," *Litmus Software Blog*, November 21, 2016, https://litmus.com/blog/gdpr-what-europes-new-privacy-law-means-for-email-marketers.
[19] The automotive industry serves as an example of compliance issues, given that new car models collect user data to improve safety and convenience, being highly influential on the design of future models. The automotive industry shows some struggles in balancing the needs for privacy and security. Brian Conroy, "What Should the Auto Industry Do about New European Data Rules?" *IoT Evolution World*, September 14, 2017, http://www.iotevolutionworld.com/smart-transport/articles/434511-what-should-auto-industry-about-new-european-data.htm.
[20] Ibid.
[21] Natasha Lomas, "WTF is GDPR?" *TechCrunch*, January 20, 2018, https://techcrunch.com/2018/01/20/wtf-is-gdpr/.
[22] Mehreen Khan, "Companies face high cost to meet new EU data protection rules," *Financial Times*, November 19, 2017, https://www.ft.com/content/0d47ffe4-ccb6-11e7-b781-794ce08b24dc.
[23] Ibid.
[24] GDPR ch. 4, art. 37.
[25] Rita Heimes and Sam Pfeifle, "Study: GDPR's global reach to require at least 75,000 DPOs worldwide," *IAPP The Privacy Advisor*, November 9, 2016, https://iapp.org/news/a/study-gdprs-global-reach-to-require-at-least-75000-dpos-worldwide/.
[26] Dana Simberkoff, "GDPR Affects Small Businesses Too," *CMSWire*, February 20, 2018, https://www.cmswire.com/information-management/gdpr-affects-small-businesses-too/.
[27] GDPR ch. 2, art. 7.
[28] Johnny Ryan, "Research result: what percentage will consent to tracking for advertising?" PageFair, September 12, 2017, https://pagefair.com/blog/2017/new-research-how-many-consent-to-tracking/.
[29] IAB Europe, "Europe Online: An Experience Driven by Advertising," September 2017, https://www.iabeurope.eu/wp-content/uploads/2017/09/EuropeOnline_FINAL.pdf.
[30] Thuy Ong, "Facebook announces new European privacy controls, for the world," *The Verge*, April 18, 2018, https://www.theverge.com/2018/4/18/17250840/facebook-privacy-protections-europe-world-gdpr.
[31] Lily Hay Newman, "How to Turn off Facebook's Face Recognition Features," *Wired*, Feb. 28, 2018, https://www.wired.com/story/how-to-turn-off-facebook-face-recognition-features/.
[32] Lauren Willis, "Why Not Privacy by Default," *Berkeley Technology Law Journal*, Vol. 29, pp. 69–80 (2014), https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=2019&context=btlj.
[33] Ibid.
[34] For instance, a longstanding maxim in the employment context holds that "absent explicit contrary contractual guarantees, employment may ordinarily be terminated at will for a good reason, a bad reason, or no reason at all." Karl E. Klare, "The Public/Private Distinction in Labor Law," *University of Pennsylvania Law Review*, Vol. 130 (1982), pp. 1358, 1362, https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=4676&context=penn_law_review.
[35] Darcy Allen, Alastair Berg, Chris Berg, and Jason Potts, "Some Economic Consequences of the GDPR," RMIT Blockchain Innovation Hub paper, April 11, 2018, https://ssrn.com/abstract=3160404.
[36] Ibid. p. 6.
[37] Adam Thierer, "How Attitudes about Risk and Failure Affect Innovation on Either Side of the Atlantic," Technology Liberation Front, June 19, 2015, https://techliberation.com/2015/06/19/how-attitudes-about-risk-failure-affect-innovation-on-either-side-of-the-atlantic/.
[38] For a discussion of these reasons, see James Pethokoukis, "Why can't Europe create its own Facebook, Apple, Netflix, or Google? Here's what Europeans think," AEIdeas, April 25, 2016, http://www.aei.org/publication/why-cant-europe-create-its-own/.
[39] Larry Downes, "How More Regulation for U.S. Tech Could Backfire," *Harvard Business Review*, February 9, 2018, https://hbr.org/2018/02/how-more-regulation-for-u-s-tech-could-backfire.
[40] Matthew Le Merle, Raju Sarma, Tashfeen Ahmed, and Christopher Pencavel, "The Impact of E.U. Internet Privacy Regulations on Early-Stage Investment: A Quantitative Study," Booz & Company, 2012, https://www.strategyand.pwc.com/media/uploads/Strategyand-Impact-EU-Internet-Privacy-Regulations-Early-Stage-Investment.pdf.

[41] Ibid., p. 15.
[42] Will Rinehart, "Why A Data Portability Act Might Not Be an Effective Policy Path," American Action Forum, February 6, 2018, https://www.americanactionforum.org/insight/data-portability-act-might-not-effective-policy-path/.
[43] Stan J. Leibowitz and Stephen E. Margolis, "Network Externality: An Uncommon Tragedy," *Journal of Economic Perspectives*, Vol. 8, No. 2 (Spring 1994), https://www.utdallas.edu/~liebowit/jep.html.
[44] Will Rinehart, "The Social Graph Portability Act Doesn't Take Tech Seriously, and That's Worrying," Tech Policy Corner, October 13, 2017, https://techpolicycorner.org/the-social-graph-portability-act-doesnt-take-tech-seriously-and-that-s-worrying-63c7259a6fec.
[45] Ann Cavoukian, "Privacy by Design: The 7 Foundational Principles," Information and Privacy Commissioner of Ontario, 2011, https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf.
[46] Although Facebook lets users download much of the data the company holds about them, it currently does not make all user data exportable, such as users' Web browsing history collected via Facebook's advertising network. Facebook, "Accessing & Downloading Your Information," accessed May 5, 2018, https://www.facebook.com/help/1701730696756992?helpref=hc_global_nav.
[47] Gus Hurwitz, "Soylent Analytica: The Graph is too Damn Open," Truth on the Market, March 21, 2018, https://truthonthemarket.com/2018/03/21/soylent-analytica-the-graph-is-too-damn-open/.
[48] Muge Fazlioglu, "Forget me not: the clash of the right to be forgotten and freedom of expression on the Internet," *International Data Privacy Law*, Vol. 3, No. 3, (August 2013), https://academic.oup.com/idpl/article/3/3/149/622037.
[49] Jamie Grierson and Ben Quinn, "Google loses landmark 'right to be forgotten' case," *The Guardian*, April 13, 2018, https://www.theguardian.com/technology/2018/apr/13/google-loses-right-to-be-forgotten-case.
[50] James Doubek, "Google Has Received 650,000 'Right to Be Forgotten' Requests Since 2014," National Public Radio, February 28, 2018, https://www.npr.org/sections/thetwo-way/2018/02/28/589411543/google-received-650-000-right-to-be-forgotten-requests-since-2014.
[51] Yvonne McDermott, "Conceptualising the right to data protection in an era of Big Data," *Big Data & Society*, January-June 2017, http://journals.sagepub.com/doi/full/10.1177/2053951716686994.
[52] Mary Carolan, "High Court sets out 11 questions for ECJ on EU-US data transfers," *Irish Times*, April 12, 2018, https://www.irishtimes.com/business/technology/high-court-sets-out-11-questions-for-ecj-on-eu-us-data-transfers-1.3459549.
[53] Eugene Volokh, "Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking about You," *Stanford Law Review*, Vol. 52 (2000), p. 1049, http://www2.law.ucla.edu/volokh/privacy.htm.
[54] Nikolaus Forgó, Stefanie Hänold and Benjamin Schütze, "The Principle of Purpose Limitation and Big Data," *New Technology, Big Data and the Law* (2017), https://www.springer.com/cda/content/document/cda_downloaddocument/9789811050374-c2.pdf?SGWID=0-0-45-1616269-p180883267.
[55] Olga Kharif, "Is Your Blockchain Business Doomed?" Bloomberg, March 22, 2018, https://www.bloomberg.com/news/articles/2018-03-22/is-your-blockchain-business-doomed.
[56] Roberta Filippone, "Blockchain and individuals' control over personal data in European data protection law," *Tilburg University* (August 2017), http://arno.uvt.nl/show.cgi?fid=143638.
[57] CoinMarketCap "Global Charts," accessed April 19, 2018, https://coinmarketcap.com/charts/.
[58] Andrew Burt, "Is there a 'right to explanation' for machine learning in the GDPR?" IAPP Privacy Tech, June 1, 2017, https://iapp.org/news/a/is-there-a-right-to-explanation-for-machine-learning-in-the-gdpr/.
[59] Aaron Bornstein, "Is Artificial Intelligence Permanently Inscrutable?" Nautilus, September 1, 2016, http://nautil.us/issue/40/learning/is-artificial-intelligence-permanently-inscrutable.
[60] Andrew D. Selbst and Julia Powles, "Meaningful information and the right to explanation," *International Data Privacy Law*, Vol. 7, No. 4 (November 2017), https://academic.oup.com/idpl/article/7/4/233/4762325.
[61] Ryan Khurana, "AI in the UK: Lords' Report Makes Startups Less Competitive," Competitive Enterprise Institute Blog, April 17, 2018, https://cei.org/blog/ai-uk-lords%E2%80%99-report-makes-startups-less-competitive.
[62] Manuel Nau, "GDPR and IoT—The Problem of Consent," IoT Business News, February 26, 2018, https://iotbusinessnews.com/2018/02/26/79400-gdpr-iot-problem-consent/.

[63] London Economics, "Analysis of the potential economic impact of GDPR Implications of the ICO's Draft Guidelines on consent," October 2017, https://londoneconomics.co.uk/wp-content/uploads/2017/10/Analysis-of-the-potential-economic-impact-of-GDPR-FINAL-October-2017.pdf.