A Social Economic Analysis of the Impact of GDPR on Security and Privacy Practices

Roslyn Layton
Center for Communication, Media and Information Technologies
Aalborg University
Copenhagen, Denmark
rl@es.aau.dk

Silvia Elaluf-Calderwood
Delray Beach, United States of America
silelf@me.com

***Abstract*— The General Data Protection Regulation (GDPR) has been presented by many policymakers as net welfare enhancing policy. It can be also seen from the point of a regulation that does not have adequate parameters to measure its effectiveness. For example, the Gordon-Loeb model [1] which calculates the optimal investment in cybersecurity has not been performed as part of the promulgation of the regulation. It can also be understood within the context of a "privacy overreach," in which the drive to protect privacy becomes absolute and lacks balance with other rights, [46], upsetting the calculus of progress toward a range of social and economic goals.**

Since promulgation of the law in May 2018, important security side effects of the policy have reported which are not insignificant, including the blocking of public information in the WHOIS internet protocol database, identity theft through the hacking of the Right to Access provision (Article 15), and the proliferation of next generation networks in the EU built by Huawei Technologies, the world's leading network equipment provider which is implicated in many data protection debates.

The impact of the GDPR to the local digital economy in EU is also significant. Evidence suggests that the GDPR has made it more difficult for European SMEs to compete.

This paper highlights whether and to what degree security has been impacted by the promulgation of the GDPR and the challenges created for the realization of "security of processing" which provides for the controller and process to "implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk" (Article 32). Unwittingly in implementing the GDPR, it appears that new cyber risks have been created. The authors have identified five areas where the impact of GDPR has been significant and likely counterproductive to the promised goals of the policy.

Keywords— GDPR, security, WHOIS, privacy, Huawei, Identity Theft, Privacy

I. BACKGROUND ON THE GDPR

In April 2016 the European Union (EU) adopted the General Data Protection Regulation (Regulation 2016/679, GDPR) [2]. It includes 99 articles and 173 recitals detailing the regulatory requirements. Failure to comply with the regulation can be met with fines up to four percent of an organization's annual revenue. The GDPR is not the first data protection regulation for the EU. In fact, it repeals EU directive 95/46/EC, which was the basis for prior national data protection legislation. In the intervening years, data collection and storage has become lifeblood of online marketing and services [3]. The rate and severity of data breach is also significant.

Rapid technological development has enabled increasing collection, transmission, and storage of user-generated data. By leveraging existing hardware, such as smartphones, the cost for this collection is decreasing as well. This vast amount of data has also led to substantial new developments in Business Models, which enable vertical as well as horizontal integration of services [4]. It has enabled a shift from product development towards information aggregation: Facebook creates no content, Uber does not employ any drivers, Airbnb does not own any real estate, Apple co-shares serves with Amazon for the storage of iCloud users, etc.

However, the basic culture of the Internet has been wary of national/boundary sovereignty and many have argued against rules that would lessen freedom of the network. Importantly the word privacy does not appear in the text of the GDPR; instead it is a regime to govern personal data and to regulate the conduct of enterprise. The regulation clearly states that any entity which processes the personal data of an EU resident must be compliant with the GDPR [5]. The GDPR has become the de facto standard for many technology based sectors, however the cost of compliance is significant. For example, some estimates suggest that the cost of compliance for Internet of Things (IoT) firms could increase by three to four times on average and by as much as 18 times compared to earlier regulatory regimes [6].

The GDPR does not apply at all to non-personal information and states that disclosure of personal information can be warranted for matters such as consumer protection, public safety, law enforcement, enforcement of rights, cybersecurity, and combating fraud. Moreover, the GDPR does not apply to domain names registered to USA registrants, registrars and registries. Nor does it apply to domain name registrants that are companies, businesses, or other legal entities, rather than "natural persons." All the same, actors including ICANN are practicing voluntary censorship because the GDPR's provisions are so vague and the potential penalties so high.

The paper now illustrates examples of the privacy and security problems created by GDPR– some expected, others not envisaged – and their repercussions.

II. CASES AND ANALYSIS

A. Reinforcement of USA Internet Platforms

Since the implementation of the GDPR, Google, Facebook, and Amazon have increased their market share in the EU [7]. Three things have happened: [8]

(1) The cost of GDPR compliance for most organization is a large, fixed cost. The GDPR imposes this fixed cost on business; large, profitable firms can absorb it; but it falls hard on small, lean firms. As we stated in our abstract there has not been a proper evaluation on the impact of those costs at level of European SMEs.

(2) Many advertisers and publishers have stopped using competing tracking tools to Google and Facebook, giving a greater share of the market to the established players.

(3) Users are less likely to try new platforms and tools, sticking instead with the "devil they know" in the incumbent players because they perceive that the larger companies have more resources to comply with the regulation.

This outcome runs counter to the GDPR proponents declarations that the EU would somehow "tame" the large USA players. There was an expectation that large fines would deter the platforms' business, that companies would be less aggressive in data collection, and that a space would open for small firms, but as Politico reported, large firms with financial and regulatory resources have "gamed" the system. Rules that were supposed to empower citizens have instead helped "Big Tech." [9]

The GDPR has affected the downstream advertising market. Given the scope of Google's advertising platform and its affiliates on syndicated networks, its compliance with the GDPR has caused ripple effects in ancillary markets. Independent ad exchanges noted prices plummeting 20 to 40 percent [10]. Some advertisers report being shut out from exchanges [11]. The GDPR's complex and arcane designations for "controllers" and "processors" can ensnare third-party chipmakers, component suppliers, and software vendors that have never interfaced with end users, as European courts have ruled that any part of the internet ecosystem can be liable for data breaches [12].

One online publisher calls the GDPR the "Google Data Protection Regulation and explains: "We have suddenly become even more dependent on Google, while other exchanges are hurting." [13]. Some large firms may welcome the GDPR because they can afford the cost of compliance and thereby reduce the threat of disruptive startups. means there are fewer competitors, but in a more pernicious

For those who study the empirical outcomes of regulation, this is not a surprise. As Nobel Memorial Prize on Economics George Stigler observed more than 40 years ago, "Regulation is acquired by industry and operated for its benefit." [14]

B. SMEs in Europe

The GDPR has weakened small- and medium-sized firms (SMEs). One study suggests that small- and medium-sized ad tech competitors have lost up to one-third of their market position since the GDPR took effect [15]. Researchers at Aalborg University found that the GDPR has led to smaller third-party trackers disappearing to the advantage of the big ones, enhancing concentration of power for access to and collecting of user data [16].

Despite some years of notice about the GDPR's coming implementation, only 20 percent of EU companies, primarily the large firms, are digitized [17]. There is little to no data that show that SMEs are growing in the EU because of the regulation [18]. The European Commission's Digital Scoreboard reports show a consistent lag in the small to medium enterprise segment, particularly to modernize their websites and market outside their own EU countries [19].

Many USA media, retailers, game companies, and service providers no longer operate in the EU because of the GDPR. The Williams-Sonoma and Pottery Barn websites are dark [20]. Over 1000 US newspapers no longer show their content in the EU for fear of breaking the rules [21]. Such heavy-handed regulation would likely be considered a violation of free speech in US.

There are numerous examples of how the regulation has already impacted USA based firms. The San Francisco–based Klout, an innovative online service that used social media analytics to rate its users according to online social influence, closed down completely. [22] Drawbridge, an identity-management company from San Mateo, California, exited the EU and sold off its ad-tracking business because of the GDPR activation [23].

Verve, a leading mobile marketing platform with offices in six US cities, closed its European operation in advance of the GDPR, affecting 15 EU employees [24]. Valve, an award-winning video game company in Bellevue, Washington, shut down an entire game community rather than invest in GDPR compliance [25]. Uber Entertainment, also based in Washington, similarly shut down one of its most popular games entirely after a six-year run because upgrading the platform to GDPR compliance was too expensive [26]. California-based Gravity Interactive no longer offers games in the EU and refunded its European customers [27]. The Las Vegas–based Brent Ozar Unlimited, which offers a range of information technology and software support services, stopped serving the EU [28]. San Francisco's Payver, the dashboard camera app that pays drivers to collect road information on potholes, fallen road signs, and other inputs to build maps to improve the safety of self-driving cars, no longer supports the EU [29].

Legal news website Above the Law describes the EU closures of Ragnarok Online, Unroll.me, SMNC, Tunngle, and Steel Root, noting that the GPDR is splintering the internet and that GDPR policymakers refused to listen to concerns from startups before the launch and now refuse to fix its problems [30]. Even the Association of National Advertisers website is not available in the EU [31].

Indeed, the GDPR can be examined as a trade barrier to keep small USA firms out so that European SMEs can get a foothold [32]. Even so, the GDPR has also made it difficult for European startups to comply and grow. SMEunited, which represents 12 million of the 24 million micro- to medium-sized enterprises in Europe (99.8 percent of all enterprises, two-thirds of employment, and close to 60 percent of the added value created in the EU) observes, "Overall this legislation creates severe difficulties for micro-enterprises and SMEs as it is not proportional. The legislation was conceived to tackle attitudes of big players, not those of SMEs. The administrative burden for documentation has increased and SMEs suffer from the lack of human and economic resources to cope with this legislation." [33]

The regulation has also hurt the European venture capital market which funds startups. An important study

published by the USA National Bureau of Economic Research and coauthored by the USA Federal Trade Commission's (FTC) former chief economist notes a $3.38 million decrease in total dollars raised per country per week from July 2017 to September 2018, a 17.6 percent reduction in weekly venture deals, and a 39.6 percent decrease in the amount raised per deal. The numbers are associated with between 3,000 and 30,000 job losses. [34]

Allied for Startups, a pan-European advocacy group, recognized that while there are fewer examples of *European* firms closing because of the GDPR, the regulation has not made it easier for startups. "Shutting down is not the same of growing slower. Every small startup, NGO or one person blog has to comply" [35]. A Bitkom (German tech industry association) survey found that eight out of ten companies had a significantly increased workload. Ninety-six percent of companies ask for corrections to the new rules. Six out of ten companies even demand a simplification of the GDPR" [36].

Consider the case of Momio, a social network for children started to offer an alternative to Facebook. Momio is an online social network designed and operated exclusively for children age 5–15 with one million users across the Nordic region and Netherlands, Germany, and Poland [37]. Launched in 2013, it operates a flagship version and Momio Lite, which does not process any personal data. The Lite version does not allow posting of text or images. Parental consent is required for users under the age of 13. Kids access the platform via a mobile device and interact with avatars they individually create. The platform is funded by partnerships with kid-friendly content and media companies. The platform is grounded in concepts of digital life skills with a focus on digital use, safety, security, emotional intelligence, communication, and literacy. As explained in an email by the company's CEO Mikael Jensen, "…as far as I know, the GDPR legislative work has not involved parents and children in the development of the law when it comes to child protection. GDPR has not made it easier to be a child on digital platforms, but on the contrary, more difficult." [38]

C. WHOIS and Cyberrisks

The GDPR has created increased cyber risk notably with the WHOIS [39] and identity theft [40]. A key unintended consequence of the GDPR is that it undermines the transparency of the international systems and architectures that organize the internet. The WHOIS query and response protocol for internet domain names, IP addresses, and autonomous systems is used by law enforcement, cybersecurity professionals, researchers, and trademark and intellectual property rights holders [41]. The Internet Corporation for Assigned Names and Numbers (ICANN) recently announced a Temporary Specification that allows registries and registrars to obscure WHOIS information they were previously required to make public, ostensibly to comply with the GDPR [42]. This has hindered efforts to combat unlawful activity online, including terrorism [43], identity theft, cyberattacks, online espionage, theft of intellectual property, fraud, unlawful sale of drugs, human trafficking, and other criminal behavior, and it is not even required by the GDPR.

The GDPR does not apply at all to non-personal information and states that disclosure of even personal information can be warranted for matters such as consumer protection, public safety, law enforcement, enforcement of rights, cybersecurity, and combating fraud. Moreover, the GDPR does not apply to domain names registered to US registrants by USA registrars and registries. Nor does it apply to domain name registrants that are companies, businesses, or other legal entities, rather than "natural persons." All the same, actors including ICANN are practicing voluntary censorship because the GDPR's provisions are so vague and the potential penalties so high. GDPR proponents have likely contributed to the impression that the GDPR urges measures such as the Temporary Specification. For example, in her role in the Article 29 Working Party, the group that drove the promulgation of the GDPR, Andrea Jelinek said that the elimination and masking of WHOIS information is justified under the GDPR [44].

The WHOIS problem can be described as the conflict between the individual's right to privacy and the public's right to know [45]. The situation harkens back to a policy fallacy which emerged to challenge the rollout of caller ID arguing that the technology violated the privacy rights of callers. Today the receiver's right to know who is calling is prioritized over the caller's right to remain anonymous [47]. Similarly, it is understood that the needs of public safety will supersede data protection, particularly in situations of danger to human life. Moreover, one should expect intellectual property to be in balance with data protection, not in conflict, as it is under the GDPR. The pace of development of privacy and data protection law is significantly faster than that of other kinds of law, leading one scholar to suggest that it threatens to upend the balance with other fundamental rights [48]. This point is underscored by Richard Epstein in his critique of the idea of privacy rights established by the Warren Court noting the theory that assumes that it is "always easy, if not inevitable, to expand the set of rights without adverse social consequences," but it never stops to consider that, when rights are expanded, correlative duties are imposed on others [49].

The GDPR has unwittingly created incentives for identity theft and online fraud. The GDPR and the California Consumer Privacy Act (CCPA) purportedly give users the ability to control their data by facilitating user requests. However, they also give hackers and identity thieves the ability to steal data because there is no provision for user authentication. Companies now must develop data pools to respond to user requests, creating a target-rich environment for cyber criminals [50]. This outcome is indicative both of the zeal of policymakers to regulate without thinking through the consequences (let alone consulting users about their preferences) and the general sloppiness of a law stitched together in a mere week, as was the case of the CCPA.

There are additional security problems. In their rush to declare moral superiority over the US, European policymakers disregarded the threats to privacy posed by network hardware manufacturers Huawei, ZTE, and Lenovo. European authorities, wanting to expand service networks cheaply, blessed the construction of communications networks with equipment from dubious Chinese vendors. Data-protection standards mean little if affiliates of the Chinese government and military can access

data in the cloud, through backdoors, by hacking, or through other illicit means.

D. Consumer Trust and Digital Services

The GDPR might be justified if it created greater trust in the digital ecosystem, but there is no such evidence. After a decade of GDPR-type regulations—in which users endure intrusive pop-ups and disclosures on every digital property they visit [51] —Europeans report no greater sense of trust online [52]. More than half of survey respondents in the UK say that they feel no better off since the GDPR took effect and that it has not helped them understand how their data are used [53]. As of 2017, only 30 percent of Europeans shop outside their own country (a paltry increase of 10 percent in a decade), demonstrating that the European Commission's Digital Single Market goals are still elusive and below expectations [54].

Political science could suggest that the GDPR is a response to reduced voter confidence slipping, and is thus an attempt by European policymakers to solidify legitimacy for Brussels during a period of deep skepticism among voters. The GDPR can be examined in the context of a heightened pro v. anti-EU debate, fueled by a rise in Euroscepticism and nationalist parties which charge that European integration weakens national sovereignty [55]. Smarting from a disgruntled electorate and the Brexit bombshell [56], pro-European coalitions support pan-European regulation such as the GDPR to legitimize the EU project. It should be noted that Eurosceptic political actors are not necessarily opposed to data protection regulation; they merely prefer the primacy of national institutions over European ones, largely because of concerns that EU institutions and policies are subverting democracy.

In the case of the GDPR, there was no groundswell of public support calling for the enactment of greater data protection regulation. The GDPR was enacted during a period of voter "disengagement." [57] Participation in European Parliament elections has dwindled from 62 percent in 1979 to just 42 percent in 2014. [58] This environment of voter disengagement is conducive for the collective action of organized special interests to defeat a diffuse, disgruntled, and unorganized majority [59]. Relatively few Europeans are even aware of the GDPR. For example, a survey found that only 34 percent of respondents recognized the law, and even fewer knew what it covered [60]. Essentially, a relatively small group of GDPR advocates successfully implemented massive pan-European regulation without significant voter buy-in. Public opinion as measured by the Eurobarometer poll [61] suggests that most people would prefer a more nuanced approach to data protection over the GDPR, and that most would rather strengthen regulation at the nation-state level than at the EU. [62]

E. Privacy Expectations

To do business in the EU today, the average firm of 500 employees must spend about $3 million to comply with the GDPR [63]. Thousands of US firms have decided it is not worthwhile and have exited [64]. Of course, $3 million, or even $300 million, is nothing for Google, Facebook, and Amazon (many Fortune 500 firms have reportedly earmarked $8 billion for GDPR upgrades [65]), but it would bankrupt many online enterprises. Indeed, less than half of eligible firms are fully compliant with the GDPR; one-fifth say that full compliance is impossible [66]. In a recent survey of small business owners in the EU, a whopping nine out of ten reported not knowing about the GDPR and that its fines for non-compliance could adversely impact them [67].

Firms are right to be concerned about non-compliance. Failing to meet one of the 45 business regulations of the GDPR appears to be the leading cause of complaints against individuals, small businesses, and nonprofit organizations, as noted by the of Ireland's Data Protection Commission [68]. She reported that the bulk of complaints are billing issues with retailers and bank statement disputes with financial institutions. While these issues are already covered under other laws, plaintiffs use the GDPR to win additional leverage for separate legal actions and litigation such as wrongful termination, personal injury, identity theft, inappropriate disclosure, and so on. The direct welfare loss of the GDPR is *estimated* to be about €260 per European citizen [69].

It does not appear that consumers are so empowered by the GDPR, however litigants received many new "rights" as a result of the GDPR including the right to organize class actions [72], lodge complaints [73], and receive compensation [74] from fines levied on firms' annual revenue, as high as four percent of annual revenue [75]. Historically, Europe has largely eschewed "U.S.-style" class actions [76], noting that they *disproportionately reward lawyers and litigation financiers over consumers [77]*. But policymakers have engineered the GDPR so that privacy activists can bring cases without overcoming legal barriers of standing and jurisdiction, which are traditional safeguards against the abuse of the legal system for private gain. A mere 7 hours after the GDPR was implemented, complaints requesting over $8 billion in damages and compensation had already been filed by professional litigants who helped craft the law [78].

Another issue with the GDPR is selective enforcement or enforcement discretion, which occurs when authorities choose whether and how to punish an actor which has violated the law, including to what degree it turns a blind eye to lack of compliance. While selective enforcement may sometimes be more efficient, it can also produce bias, corruption, and prejudice. For example, there is evidence of bias in the selective enforcement of human rights laws [79], as well as in the selective enforcement of industrial regulation [80]. A recent doctoral thesis in the European University Institute's Department of Law documents the European Commission's policy of selective law enforcement and argues that it is based upon the pillars of confidentiality, bilateralism, flexibility, and autonomy [81]. While it has been pressured to increase its legitimacy by improving enforcement with standards such as transparency, trilateralism, objectivity, and accountability, the Commission has resisted, and its position has been upheld in the European Court of Justice. The thesis explains that selective enforcement is prevalent because the Commission's ability to enforce the law is limited. Indeed, the Commission is perceived as reluctant to improve standards and formalize enforcement because doing so would create administrative burdens, which would in turn decrease its efficiency [82].

III. Conclusions

The paper presents five major outcomes which appear to contradict the policy expectation of the GDPR:

1. The largest USA platforms have increased market share. Success EU data protection regulation does not appear to incentivize the creation or formation of European native platforms of global importance.

2. The GDPR has weakened already small and medium sized firms and has not made it easier for them to grow in the EU. The impact in the ability to create internal markets for competition in emergent services (e.g. IoT) is now limited by the compliance of the regulation.

3. Consumers' trust online has fallen to its lowest point in a decade. While it is not suggested that there is a direct relationship between GDPR and trust; it is merely observed that successive data protection regulation is not associated with greater trust. The dip in the indicator is concerning at a time when policymakers have messaged repeatedly that the GDPR is a pro-consumer regulation.

4. The GDPR has increased cyber risk around WHOIS, identity theft, and fraud. This risk has not been quantified in monetary terms nor is there a clear economic figure on the impact of implementation the regulation.

5. The GDPR may in fact create an illusion of privacy, with the presence of a strong regulation to which less than half of applicable firms comply because of the high cost and discretionary enforcement.

It is not evident that the GDPR which was purported to ensure users' rights and privileges will necessarily discipline the largest online players. In particular there is a need to review data breaches and conceptualize threats of data processing to individual privacy within the large hierarchy of threats: individual, community, country, industry or sector based, primary or critical infrastructure (e.g. nuclear stations, hospitals, water supplies) and civilian and military uses. Moreover a comprehensive economic analysis of the real costs and impact of the implementation of the GDPR rules is required to understand the impact in the European digital economy.

References

[1] Gordon, Lawrence A., Martin P. Loeb, and Lei Zhou. 'Investing in Cybersecurity: Insights from the Gordon-Loeb Model'. Journal of Information Security 7 (2016): 49–59.

[2] European Union: Regulation 2016/679 of the European Parliament and the Council of the European Union (2016)

[3] Menon, Mohan. 'GDPR and Data Powered Marketing: The Beginning of a New Paradigm'. Journal of Marketing Development and Competiviness 13, no. 2 (2019): 73–84.

[4] Huth, Dominik. 'A Pattern Catalog for GDPR Compliant Data Protection'. In PoEM 2017 Doctoral Consortium and Industry Track Papers, 2027:34–40. Leuven, Belgium: CEURS-WS.org, 2017. Accesible at : https://pdfs.semanticscholar.org/8516/123f68307638c6c95f202e43624afe9ab74d.pdf.

[5] Garcia Martines, Francisco. 'Analysis of the US Privacy Model: Implications of the GDPR in the US'. IGI Global Diseminator of Kwoledge, 2019. https://www.igi-global.com/article/analysis-of-the-us-privacy-model/234344.

[6] Seo, Junwoo, Kyoungmin Kim, Mookyu Park, and Kyungho Lee. 'An Analysis of Economic Impact on IoT Industry under GDPR'. Mobile Information Systems Vol 2018, no. Online (2018): 6. https://doi.org/10.1155/2018/6792028.

[7] Mark Scott, Laurens Cerulus, and Laura Kayali, "Six Months in, Europe's Privacy Revolution Favors Google, Facebook," *Politico*, November 27, 2018, https://www.politico.eu/article/gdpr-facebook-google-privacy-data-6-months-in-europes-privacy-revolution-favors-google-facebook/.
Also:
Schechner, Sam, and Nick Kostov. 'Google and Facebook Likely to Benefit From Europe's Privacy Crackdown'. The Wall Street Journal, 2018. https://www.wsj.com/articles/how-europes-new-privacy-rules-favor-google-and-facebook-1524536324.
Webb, Alex. 'Google's Mortal Enemy Does It a $95 Billion Favor'. Bloomberg.com. Technology and Ideas (blog), 2018. https://www.bloomberg.com/opinion/articles/2018-07-20/google-s-mortal-enemy-does-it-a-95-billion-favor.
Webb, Alex. 'Google and Facebook Turn On the Fake Riviera Charm The Silicon Valley Giants Want to Cut out the Ad Agencies, and New EU Data Rules Will Help Them.' Bloomberg.com. Technology and Ideas (blog), 2018. https://www.bloomberg.com/opinion/articles/2018-06-25/google-and-facebook-turn-on-the-fake-riviera-charm.

[8] Campbell, James, Avi Goldfarb, and Catherine Tucker. "Privacy regulation and market structure." *Journal of Economics & Management Strategy* 24.1 (2015): 47-73.

[9] Scott, Mark, Laurens Cerulus, and Steven Overly. 'How Silicon Valley Gamed Europe's Privacy Rules The Region's Data Protection Overhaul Was Supposed to Help Citizens. Instead, It's Helped Big Tech.' Politico.eu, 2019. https://www.politico.eu/article/europe-data-protection-gdpr-general-data-protection-regulation-facebook-google/.

[10] Jessica Davies, 'The Google Data Protection Regulation': GDPR is Strafing Ad Sellers, Digiday (June 4, 2018), https://digiday.com/media/google-data-protection-regulation-gdpr-strafing-ad-sellers/.

[11] Catherine Armitage, "Life After GDPR: What Next for the Advertising Industry?," World Federation of Advertisers, July 10, 2018, https://www.wfanet.org/news-centre/life-after-gdpr-what-next-for-the-advertising-industry/.

[12] European Union, Judgment of the Court (Grand Chamber), June 5, 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62016CJ0210&qid=1531145885864&from=EN.

[13] https://digiday.com/media/google-data-protection-regulation-gdpr-strafing-ad-sellers/

[14] George Stigler, "The Theory of Economic Regulation," *Bell Journal of Economics* 2, no. 1 (1971): 3–21.

[15] Björn Grelf, "Study: Google Is the Biggest Beneficiary of the GDPR," Cliqz, October 10, 2018, https://cliqz.com/en/magazine/study-google-is-the-biggest-beneficiary-of-the-gdpr.

[16] Jannick Kirk, Sorensen and Van den Bulck, Hilde and Kosta, Sokol, Privacy Policies Caught Between the Legal and the Ethical: European Media and Third Party Trackers Before and After GDPR. (July 26, 2019). Available at SSRN: https://ssrn.com/abstract=3427207

[17] European Commission, "Integration of Digital Technology," 2018, accesisble at : http://ec.europa.eu/information_society/newsroom/image/document/2018-20/4_desi_report_integration_of_digital_technology_B61BEB6B-F21D-9DD7-72F1FAA836E36515_52243.pdf.

[18] https://ec.europa.eu/digital-single-market/en/digital-scoreboard

[19] European Commission, "Better Access for Consumers and Business to Online Goods," 2015, https://ec.europa.eu/digital-single-market/en/better-access-consumers-and-business-online-goods.

[20] Associated Press, "Amid Confusion, EU Data Privacy Law Goes into Effect," WTOP, May 25, 2018, https://wtop.com/news/2018/05/amid-confusion-eu-data-privacy-law-goes-into-effect/.

[21] Jeff South, "More Than 1,000 U.S. News Sites Are Still Unavailable in Europe, Two Months After GDPR Took Effect," Nieman Lab, August 7, 2018, http://www.niemanlab.org/2018/08/more-than-1000-u-s-news-sites-are-still-unavailable-in-europe-two-months-after-gdpr-took-effect/.

[22] Jon Russel, "RIP Klout," TechCrunch, May 2018, https://techcrunch.com/2018/05/10/rip-klout/.

[23] Allison Schiff, "Drawbridge Sells Its Media Arm and Exits Ad Tech," AdExchanger, May 8, 2018, https://adexchanger.com/data-exchanges/drawbridge-sells-its-media-arm-and-exits-ad-tech/.

[24] Ronan Shields." Verve to Focus on US Growth as It Plans Closure of European Offices Ahead of GDPR," Drum, April 18, 2018, https://www.thedrum.com/news/2018/04/18/verve-focus-us-growth-it-plans-closure-european-offices-ahead-gdpr.

[25] Steam, "Super Monday Night Combat," https://steamcommunity.com/app/104700/allnews/.

[26] Owen Good, “Super Monday Night Combat Will Close Down, Citing EU’s New Digital Privacy Law,” Polygon, April 28, 2018, https://www.polygon.com/2018/4/28/17295498/super-monday-night-combat-shutting-down-gdpr.
[27] Warportal, “Important Notice Regarding European Region Access,” http://blog.warpportal.com/?p=10892.
[28] Brent Ozar, “GDPR: Why We Stopped Selling Stuff to Europe,” December 18, 2017, https://www.brentozar.com/archive/2017/12/gdpr-stopped-selling-stuff-europe/.
[29] Payver (@getpayver), “Sorry European Payver users! Come May 24th we’re discontinuing Payver support in Europe due to #GDPR. Talk to your lawmakers...,”Twitter, April 5, 2018, 5:30 p.m., https://twitter.com/getpayver/status/981992477392437249.
[30] Techdirt, “Companies Respond to the GDPR by Blocking All EU Users,” Above the Law, May 11, 2018, https://abovethelaw.com/legal-innovation-center/2018/05/11/companies-respond-to-the-gdpr-by-blocking-all-eu-users/.
[31] George P. Slefo, “ANA Doesn’t Have GDPR-Compliant Website; Says It Will Be up in ‘Two Weeks,’” AdAge, June 7, 2018, https://adage.com/article/digital/ana-misses-deadline-create-gdpr-compliant-website/313775/.
[32] Daniel Lyons, “GDPR: Privacy as Europe’s Tariff by Other Means?,” AEIdeas, July 3, 2018, http://www.aei.org/publication/gdpr-privacy-as-europes-tariff-by-other-means/.
[33] https://smeunited.eu/news/smeunited-members-contributions-on-the-application-of-gdpr
[34] Jian Jia, Ginger Zhe Jin, Liad Wagman, “The Short-Run Effects of GDPR on Technology Venture Investment” (working paper, National Bureau of Economic Research, November 2018), https://www.nber.org/papers/w25248
[35] Quoting Melissa Blaustein private email to one of the authors from at http://alliedforstartups.org
[36] Survey at https://www.bitkom.org/Presse/Presseinformation/Germany-Little-Progress-in-Implementation-of-GDPR.html
[37] Momio, “About Momio,” http://company.momio.me/about-us/
[38] Email from Mikael Jensen, March 6, 2019. Momio ApS, Lergravsvej 53, 2nd floor, 2300 Copenhagen S, Denmark
[39] Anthony J. Ferrante, “The Impact of GDPR on WHOIS: Implications for Businesses Facing Cybercrime,” Text, 2018, https://www.ingentaconnect.com/content/hsp/jcs/2018/00000002/00000002/art00006.
[40] Zac Cohen, “The Fraud Risk Underlying GDPR’s ‘Right to Be Forgotten,’” *Trulioo: Global Identity Verification* (blog), July 3, 2018, https://www.trulioo.com/blog/fraud-risk-gdpr/.
[41] Shane Tews, “How European Data Protection Law Is Upending the Domain Name System,” AEIdeas, February 26, 2018, https://www.aei.org/publication/how-european-data-protection-law-is-upending-the-domain-name-system/.
[42] Temporary Specification for gTLD Registration Data, ICANN, adopted May 17, 2018, https://www.icann.org/resources/pages/gtld-registration-data-specs-en.
[43] https://www.bloomberg.com/news/articles/2019-07-08/european-privacy-laws-may
-be-hampering-those-catching-terrorists
[44] Letter from Andrea Jelinek, Chairperson of Article 29 Data Protection Working Party, to Göran Marby, President of ICANN, April 11, 2018, https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-11apr18-en.pdf.
[45] Shane Tews, Privacy and Europe’s Data Protection Law: Problems and Implications for the US, AEIdeas, May 8, 2018, http://www.aei.org/publication/privacy-and-europes-data-protection-law-problems-and-implications-for-the-us/.
[46] See Maja Brkan, “The Unstoppable Expansion of the EU Fundamental Right to Data Protection,” *Maastricht Journal of European and Comparative Law* 23 no. 812 (2016), http://journals.sagepub.com/doi/abs/10.1177/1023263X1602300505?journalCode=maaa.
[47] See Hurwitz and Jaffer, “Modern Privacy Advocacy,” 179.
[48] See Brkan, “The Unstoppable Expansion of the EU Fundamental Right to Data Protection,” 180.
[49] Richard Epstein, “A Not Quite Contemporary View of Privacy,” *Harvard Journal of Public Policy* 41 no. 95 (2018), http://www.harvard-jlpp.com/wp-content/uploads/2018/01/EpsteinPanel_FINAL.pdf.
[50] ANA, “The CCPA—Making Things Worse,” March 4, 2019, https://www.ana.net/blogs/show/id/rr-blog-2019-01-The-CCPA-Making-Things-Worse.
[51] GDPR pop-up disclosures have become so intrusive that Europeans download pop-up blockers on their phones.
[52] Daniel Castro and Alan McQuinn, “The Economic Cost of the European Union’s Cookie Notification Policy,” Information Technology & Innovation Foundation, November 6, 2014, https://itif.org/publications/2014/11/06/economic-cost-european-unions-cookie-notification-policy.
[53] GDPR three months on: Most consumers feel no better off. Marketing Week. Lucy Tesseras 24 August 2018. https://www.marketingweek.com/2018/08/24/gdpr-three-months-on/?ct_5bf3f166954e0=5bf3f16695585
[54] European Commission, “Use of Internet Services,” 2018, 4, http://ec.europa.eu/information_society/newsroom/image/document/2018-20/3_desi_report_use_of_internet_services_18E82700-A071-AF2B-16420BCE813AF9F0_52241.pdf.
[55] Euroscepticism as a Transnational and Pan-European Phenomenon 133 (John FitzGibbon, Benjamin Leruth, Nick Startin eds., 2016).
[56] *Id.* Euroscepticism is the notion that the European integration undermines the national sovereignty of its members states, that the EU lacks democratic legitimacy, is too bureaucratic, encourages high migration, and the perception that it is a neoliberal organization benefitting the elite at the expense of the working class—remains an obstacle to the goals some have for the European continent. *See also* Dalibor Rohac, *Europe’s Pressure Points*, AEI, January 17, 2017, http://www.aei.org/feature/europes-pressure-points/.
[57] Curtice, John. ‘How Deeply Does Britain’s Euroscepticism Run?’ London, UK: NatCen Social Research, 2016. https://www.bsa.natcen.ac.uk/media/39024/euroscepticism.pdf.
[58] Turnout 2014 - European Parliament, European Parliament, http://www.europarl.europa.eu/elections2014-results/en/turnout.html (accessed July 27, 2018).
[59] *See generally* MANCUR OLSON, THE LOGIC OF COLLECTIVE ACTION (1971).
[60] Kirsty Cooke, *Data Shows Awareness of GDPR Is Low amongst Consumers*, KANTAR, March 27, 2018, https://uk.kantar.com/public-opinion/policy/2018/data-shows-awareness-of-gdpr-is-low-amongst-consumers/.
[61] European Commission, Public Opinion, http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm.
[62] Roslyn Layton, *How the GDPR Compares to Best Practices for Privacy, Accountability and Trust*, SSRN Scholarly Paper, March 31, 2017, https://papers.ssrn.com/abstract=2944358.
[63] International Association of Privacy Professionals, “IAPP-EY Annual Governance Report 2018,” 2019, https://iapp.org/resources/article/iapp-ey-annual-governance-report-2018/.
[64] Jeff South, “More Than 1,000 U.S. News Sites Are Still Unavailable in Europe, Two Months After GDPR Took Effect,” Nieman Lab, August 7, 2018, http://www.niemanlab.org/2018/08/more-than-1000-u-s-news-sites-are-still-unavailable-in-europe-two-months-after-gdpr-took-effect/.
[65] https://iapp.org/news/a/survey-fortune-500-companies-to-spend-7-8b-on-gdpr-compliance/
[66] International Association of Privacy Professionals, “IAPP-EY Annual Governance Report 2018.”
[67] https://www.hiscox.co.uk/business-blog/gdpr-still-mystery-smes-risks-non-compliance/
[68] https://www.commerce.senate.gov/public/_cache/files/82740fd0-dc86-4665-9c3f-378892c6fca0/649B8DBDAF3E93DC2B0B79B982E83585.05-01-19dixon-testimony.pdf
[69] Hosuk Lee-Makiyama, “The Political Economy of Data: EU Privacy Regulation and the International Redistribution of Its Costs,” in *Protection of Information and the Right to Privacy—A New Equilibrium?*, ed. Luciano Floridi (Springer, 2014), 85–94. This methodology is expanded in Erik Van der Marel et al., “A Methodology to Estimate the Costs of Data Regulations,” *International Economics* 146 (2016): 12–39.
[70] Jonathan Spalter, “Broadband CapEx Investment Looking Up in 2017,” USTelecom, July 25, 2018, https://www.ustelecom.org/blog/broadband-capex-investment-looking-2017.
[71] US Census Bureau, “Quarterly Retail E-Commerce Sales 1st Quarter 2018,” May 17, 2018, https://www2.census.gov/retail/releases/historical/ecomm/18q1.pdf.
[72] GDPR, Recital 142, Article 80.
[73] GDPR, Recital 141, Article 77.

[74] GDPR, Recital 143, Articles 78-79, 82.
[75] GDPR, Recital 143, Article 83.
[76] Lisa A. Rickard, *Consumers Are the Losers in EU's Collective Action Proposal*, POLITICO (Aug. 3, 2018), https://www.politico.eu/article/opinion-consumers-are-the-losers-in-eus-collective-action-proposal-european-commission-collective-action/.
[77] Martin Redish, Wholesale Justice: Constitutional Democracy and the Problem of the Class Action Lawsuit. Stanford Books, 2009. https://www.amazon.com/Wholesale-Justice-Constitutional-Democracy-Stanford/dp/0804752753
[78] Roslyn Layton and Julian McLendon, "The GDPR: What It Really Does and How the U.S. Can Chart a Better Course," Federalist Society, https://fedsoc.org/commentary/publications/the-gdpr-what-it-really-does-and-how-the-u-s-can-chart-a-better-course.
[79] Binder, Martin. 'The Selective Enforcement of Human Rights? The International Response to Violent Humanitarian Crises and Gross Violations of Human Rights in the Post-Cold-War Era'. Discussion Paper. Berlin, Germany: Social Science Research Center, 2007. https://ideas.repec.org/p/zbw/wzbtci/spiv2007307.html.
[80] Fenn, P, and C.G Veljanovski. 'A Positive Economic Theory of Regulatory Enforcement'. The Economic Journal 98, no. 393 (1988): 1055–70. https://doi.org/10.2307/2233719.
[81] Boiret, Karolina. 'Selective Enforcement of EU Law : Explaining Institutional Choice'. PhD Thesis, Department of Law - European University Institute, 2016. http://hdl.handle.net/1814/44326.
[82] Roslyn Layton, "Trump Should Ignore Chinese Manufacturers' Phony Promises," *Forbes*, February 20, 2019, https://www.forbes.com/sites/roslynlayton/2019/02/20/trump-should-ignore-chinese-manufacturers-phony-promises/#257b924d50ec.
[83] ANA, "The CCPA—Making Things Worse," March 4, 2019, https://www.ana.net/blogs/show/id/rr-blog-2019-01-The-CCPA-Making-Things-Worse.