Privacy + Security Forum Supplemental Reading Materials:
Big Data: Impact of Privacy Laws on Big Data Analytics
September 2020

Commoditization of Data is the Problem, Not the Solution

Why Placing a Price Tag on Personal Information May Harm Rather Than Protect Consumer Privacy[1]

By Lokke Moerel and Christine Lyon[2]

Friend and foe agree that our society is undergoing a digital revolution that is in the process of transforming our society as we know it. In addition to economic and social progress, every technological revolution also brings along disruption and friction.[3] The new digital technologies (and, in particular, *artificial intelligence* -AI) are fueled by huge volumes of data, leading to the common saying that "data is the new oil." These data-driven technologies transform existing business models and present new privacy issues and ethical dilemmas.[4] Social resistance to the excesses of the new data economy is becoming increasingly visible and leads to calls for new legislation.[5]

Commentators argue that a relatively small number of companies are disproportionately profiting from consumers' data, and that the economic gap continues to grow between technology companies and the consumers whose data drives the profits of these companies.[6] Consumers are also becoming more aware of the fact that free online services come at a cost to their privacy,

---

[1] This essay first appeared on the Future of Privacy Forum (https://fpf.org/2020/06/24/commoditization-of-data-is-the-problem-not-the-solution-why-placing-a-price-tag-on-personal-information-may-harm-rather-than-protect-consumer-privacy/) and a shortened version was posted by the International Association of Privacy Professionals (https://iapp.org/news/a/why-placing-a-price-tag-on-personal-data-may-harm-consumer-privacy/).

[2] Lokke Moerel is a Professor of Global ICT Law at Tilburg University and Senior of Counsel at Morrison & Foerster in Berlin. Christine Lyon is partner at Morrison & Foerster in Palo Alto, California.

[3] E. Brynjolfsson & A. McAfee, *Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant New Technologies*, London: W.W. Norton & Company 2014, which gives a good overview of the friction and disruption that arose from the industrial revolution and how society ultimately responded and regulated negative excesses and a description of the friction and disruption caused by the digital revolution. A less accessible, but very instructive, book, on the risks of digitization and big tech for society is S. Zuboff, *The Age of Surveillance Capitalism*, New York: Public Affairs 2019 (hereinafter, "Zuboff 2019").

[4] An exploration of these new issues, as well as proposals on how to regulate the new reality from a data protection perspective, can be found in L. Moerel, *Big Data Protection: How to Make the Draft EU Regulation on Data Protection Future Proof* (oration Tilburg), Tilburg: Tilburg University 2014 (hereinafter, "Moerel 2014"), pp. 9-13, and L. Moerel & C. Prins, *Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things* (2016), [ssrn.com/abstract=2784123] (hereinafter, "Moerel & Prins 2016"). On ethical design issues, see J. Van den Hoven, S. Miller & T. Pegge (eds.), *Designing in Ethics*, Cambridge: CUP 2017 (hereinafter, "Van den Hoven, Miller & Pegge 2017"), p. 5.

[5] L. Vaas, "FTC renews call for single federal privacy law," *Naked Security by Sophos* (May 10, 2019), https://nakedsecurity.sophos.com/2019/05/10/ftc-renews-call-for-single-federal-privacy-law/.

[6] Jaron Lanier and E. Glen Weyl, "A Blueprint for a Better Digital Society," *Harvard Business Review* (Sept. 26, 2018), https://hbr.org/2018/09/a-blueprint-for-a-better-digital-society ("The foremost challenge in implementing data dignity is the yawning gap between big tech platforms and the individuals they harvest data from…[t]he inevitable concentration of power these platforms create is inimical to competitive markets and an open society.")..

where the modern adage has become that consumers are not the recipients of free online services but are actually the *product itself*.[7]

U.S. legislators are responding by proposing prescriptive notice and choice requirements which intend to serve the dual purpose of providing consumers with greater control over the use of their personal information and at the same time enabling them to profit from that use of their information.

An illustrative example is California Governor Gavin Newsom's proposal that consumers should "share the wealth" that technology companies generate from their data, potentially in the form of a "data dividend" to be paid to Californians for the use of their data.[8] California's Consumer Privacy Act (CCPA) also combines the right of consumers to opt out of the sale of their data with a requirement that any financial incentive offered by companies to consumers for the sale of their personal information should be reasonably related to the value of the consumer's data.[9]

These are not isolated examples. The academic community is also proposing alternative ways to address wealth inequality. Illustrative here is Lanier and Weyl's proposal for the creation of data unions that would negotiate payment terms for user-generated content and personal information supplied by their users, which we will discuss in further detail below.

Though these attempts to protect, empower, and compensate consumers are commendable, the proposals to achieve these goals are actually counterproductive. The remedy is here worse than the ailment.

To illustrate the underlying issue, let's take the example of misleading advertising and unfair trade practices. If an advertisement is misleading or a trade practice unfair, it is intuitively understood that companies should not be able to remedy this situation by obtaining consent for such practice from the consumer. In the same vein, if companies generate large revenues with their misleading and unfair practices, the solution is not to ensure consumers get their share of

---

[7] Zuboff 2019, p. 94, refers to this by a now commonly cited adage, but nuances it by indicating consumers are not the product, but rather "[the objects from which raw materials are extracted and expropriated for Google's prediction factories. Predictions about our behavior are Google's products, and they are sold to its actual customers but not to us."

[8] Angel Au-Yeung, "California Wants to Copy Alaska and Pay People a 'Data Dividend.' Is It Realistic?" *Forbes* (Feb. 14, 2019), https://www.forbes.com/sites/angelauyeung/2019/02/14/california-wants-to-copy-alaska-and-pay-people-a-data-dividend--is-it-realistic/#30486ee6222c.

[9] Cal. Civ. Code § 1798.125(b)(1) ("A business may offer financial incentives, including payments to consumers as compensation for the collection of personal information, the sale of personal information, or the deletion of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the business by the consumer's data"). The California Attorney General's final proposed CCPA regulations, issued on June 1, 2020 (Final Proposed CCPA Regulations), expand on this obligation by providing that a business must be able to show that the financial incentive or price or service difference is reasonably related to the value of the consumer's data. (Final Proposed CCPA Regulations at 20 CCR § 999.307(b).) The draft regulations also require the business to use and document a reasonable and good faith method for calculating the value of the consumer's data. *Id.*

the illicitly obtained revenues. If anything would provide an incentive to continue misleading and unfair practices, this would be it.

As always with data protection in the digital environment, the issues are far less straightforward than in their offline equivalents and therefore more difficult to understand and address. History shows that whenever a new technology is introduced, society needs time to adjust. As a consequence, the data economy is still driven by the possibilities of technology rather social and legal norms.[10] This inevitably leads to social unrest and calls for new rules, such as the call of Microsoft's CEO, Satya Nadella, for the U.S., China, and Europe to come together and establish a global privacy standard based on the EU General Data Protection Regulation (GDPR).[11]

From *privacy is dead* to *privacy is the future*. The point here is that not only technical developments are moving fast, but also that social standards and customer expectations are evolving.[12]

To begin to understand how our social norms should be translated to the new digital reality, we will need to take the time to understand the underlying rationales of the existing rules and translate them to the new reality. Our main point here is that that the two concepts of consumer control and wealth distribution are separate but intertwined. They seek to empower consumers to take control of their data, but they also treat privacy protection as a right that can be traded or sold. These purposes are equally worthy, but cannot be combined. They need to be regulated separately and in a different manner. Adopting a commercial trade approach to privacy protection will ultimately undermine rather than protect consumer privacy. To complicate matters further, experience with the consent-based model for privacy protection in other countries (and especially under the GDPR) shows that the consent-based model is flawed and fails to achieve privacy protection in the first place. We will first discuss why consent is not the panacea to achieve privacy protection.

Why Should We Be Skeptical of Consent as a Solution for Consumer Privacy?

On the surface, consent may appear to be the best option for privacy protection because it allows consumers to choose how they will allow companies to use their personal information. Consent tended to be the default approach under the EU's Data Protection Directive, and the GDPR still lists consent first among the potential grounds for processing of personal data.[13] Over time, however, confidence in consent as a tool for privacy protection has waned.

---

[10] Moerel 2014, p. 21.
[11] Isobel Asher Hamilton, "Microsoft CEO Satya Nadella made a global call for countries to come together to create new GDPR-style data privacy laws," *Business Insider* (Jan. 24, 2019), available at https://www.businessinsider.com/satya-nadella-on-gdpr-2019-1.
[12] L. Moerel, *Reflections on the Impact of the Digital Revolution on Corporate Governance of Listed Companies*, first published in Dutch by Uitgeverij Paris in 2019, and written in assignment of the Dutch Corporate Law Association for their annual conference, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3519872, at para. 4.
[13] GDPR Art. 6(1): "Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes…."

Before GDPR, many believed that the lack of material privacy compliance was mostly due to lack of enforcement under the Directive, and that all would be well when the European supervisory authorities would have higher fining and broader enforcement powers. However, now these powers are granted under GDPR, not much has changed and privacy violations are still being featured in newspaper headlines.

By now the realization is setting in that non-compliance with privacy laws may also be created by a fundamental flaw in consent-based data protection. The laws are based on the assumption that as long as people are informed about which data are collected, by whom and for which purposes, they can then make an informed decision. The laws seek to ensure people's autonomy by providing choices. In a world driven by AI, however, we can no longer fully understand what is happening to our data. The underlying logic of data-processing operations and the purposes for which they are used have now become so complex that they can only be described by means of intricate privacy policies that are simply not comprehensible to the average citizen. It is an illusion to suppose that by better informing individuals about which data are processed and for which purposes, we can enable them to make more rational choices and to better exercise their rights. In a world of too many choices, autonomy of the individual is reduced rather than increased. We cannot phrase it better than Cass Sunstein in his book, *The Ethics of Influence* (2016):

> [A]utonomy does not require choices everywhere; it does not justify an insistence on active choosing in all contexts. (…) People should be allowed to devote their attention to the questions that, in their view, deserve attention. If people have to make choices everywhere, their autonomy is reduced, if only because they cannot focus on those activities that seem to them most worthy of their time.[14]

More fundamental is the point that a regulatory system that relies on the concept of *free choice* to protect people against consequences of AI is undermined by the very technology this system aims to protect us against. If AI knows us better than we do ourselves, it can manipulate us, and strengthening the information and consent requirements will not help.

Yuval Harari explains it well:

> What then, will happen once we realise that customers and voters never make free choices, and once we have the technology to calculate, design or outsmart their feelings? If the whole universe is pegged to the human experience, what will happen once the human experience becomes just another designable product, no different in essence from any other item in the supermarket?[15]

The reality is that organizations find inscrutable ways of meeting information and consent requirements that discourage individuals from specifying their true preferences and often make

[14] Cass Sunstein, *The Ethics of Influence*, Cambridge University Press 2016 (hereinafter: Sunstein 2016), p. 65. .
[15] Yuval Noah Harari, *Homo Deus: A History of Tomorrow,* Harper 2017 (hereinafter: Harari 2017), p. 277.

them feel forced to click "OK" to obtain access to services.[16] The commercial interests of collecting as many data as possible are so large that in practice all tricks available are often used to entice website visitors and app users to opt in (or to make it difficult for them to opt out). The design thereby exploits the *predictably irrational* behavior of people so that they make choices that are not necessarily in their best interests.[17] A very simple example is that consumers are more likely to click on a blue button than a gray button, even if the blue one is the least favorable option. Telling is that Google once tested 41 shades of blue to measure *user response*.[18] Also established companies deliberately make it difficult for consumers to make their actual choice and seem to have little awareness of doing something wrong. In comparison, if you would deliberately mislead someone in the offline world, everyone would immediately feel that this was unacceptable behavior.[19] Part of the explanation for this is that the digital newcomers have deliberately and systematically pushed the limits of their digital services in order to get their users accustomed to certain processing practices.[20] Although many of these privacy practices are now under investigation by privacy and antitrust authorities around the world,[21] we still see that these practices have obscured the view of what is or is not an ethical use of data.

---

[16] This is separate from the issue that arises where companies require a consumer to provide consent for use of their data for commercial purposes, as a condition of receiving goods or services (so-called tracking walls and cookies walls). It also may arise if a consumer is required to provide a bundled consent that covers multiple data processing activities, without the ability to choose whether to consent to a particular data processing activity within that bundle. In May 2020, the European Data Protection Board (EDPB) updated its guidance on requirements of consent under the GDPR, now specially stating that consent is not considered freely given in the case of cookie walls, see EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.0, Adopted on May 4, 2020, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf (EDPB Guidelines on Consent 2020).

[17] This is the field of behavioral economics. See D. Ariely, *Predictably Irrational*, London: HarperCollinsPublishers 2009 (hereinafter, "Ariely 2009"), at Introduction. For a description of techniques reportedly used by large tech companies, see the report from the Norwegian Consumer Council, *Deceived by Design: How tech companies use dark patterns to discourage our privacy rights* (June 27, 2018), available at https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf (hereinafter, "Norwegian Consumer Council 2018"). The Dutch Authority for Consumers & Market (ACM) has announced that the abuse of this kind of predictable irrational consumer behavior must cease and that companies have a duty of care to design the *choice architecture* in a way that is fair and good for the consumer. Authority for Consumers & Market, *Taking advantage of predictable consumer behavior online should stop* (Sept. 2018), available at https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

[18] See Norwegian Consumer Council 2018, p. 19, reference L.M. Holson, "Putting a Bolder Face on Google," *New York Times* (Feb. 28, 2009), www.nytimes.com/2009/03/01/business/01marissa.html.

[19] See Van den Hoven, Miller & Pegge 2017, p. 25, where the ethical dimension of misleading choice architecture is well illustrated by giving an example in which someone with Alzheimer's is deliberately confused by rearranging his or her system of reminders. For an explanation of a similar phenomenon, see Ariely 2009, Introduction and Chapter 14: "Why Dealing with Cash Makes Us More Honest," where it is demonstrated that most unfair practices are one step removed from stealing cash. Apparently, it feels less bad to mess around in accounting than to steal real money from someone.

[20] Zuboff 2019 convincingly describes that some apparent *failures of judgment* that technology companies' management regard as *missteps* and *bugs* (for examples, see p. 159), are actually deliberate, systematic actions intended to habituate their users to certain practices in order to eventually adapt social norms. For what Zuboff 2019 calls the Disposition Cycle, see pp. 138-166.

[21] Zuboff 2019 deals extensively with the fascinating question of how it is possible that technology companies got away with these practices for so long. See pp. 100-101.

Consent-based data protection laws have resulted in what is coined as *mechanical proceduralism*,[22] whereby organizations go through the mechanics of notice and consent, without any reflection on whether the relevant use of data is *legitimate* in the first place. In other words, the current preoccupation is with what is *legal*, which is distracting us from asking what is *legitimate* to do with data. We see this reflected in even the EU's highest court having to decide whether a pre-ticked box constitutes consent (surprise: it does not) and the EDPB feeling compelled to update its earlier guidance by spelling out whether cookie walls constitute "freely given" consent (surprise: they do not).[23]

Privacy legislation needs to regain its role of determining what is and is not permissible. Instead of a legal system based on consent, we need to re-think the social contract for our digital society, by having the difficult discussion about where the red lines for data use should be rather than passing the responsibility for a fair digital society to individuals to make choices that they cannot oversee.[24]

The U.S. System: Notice and *Choice* (as Opposed to Notice and *Consent*)

In the United States, companies routinely require consumers to consent to the processing of their data, such as by clicking a box stating that they agree to the company's privacy policy, although there is generally no consent requirement under U.S. law.[25] This may reflect an attempt to hedge the risk of consumers challenging the privacy terms as an 'unfair trade practice'.[26] The argument being that the consumer made an informed decision to accept the privacy terms as part of the transaction, and that the consumer was free to reject the company's offering and choose another. In reality, of course, consumers will have little actual choice, particularly where the competing options are limited and offer similar privacy terms. In economic terms, we have an *imperfect market* where companies do not compete based on privacy given their aligned interest to acquire

[22] Moerel & Prins 2016, para. 3.

[23] EDPB Guidelines on Consent, p. 10.

[24] Lokke Moerel, IAPP The GDPR at Two: Expert Perspectives, "EU data protection laws are flawed — they undermine the very autonomy of the individuals they set out to protect", 26 May 2020, https://iapp.org/resources/article/gdpr-at-two-expert-perspectives/.

[25] U.S. privacy laws require consent only in limited circumstances (e.g., the Children's Online Privacy Protection Act, Fair Credit Reporting Act, and Health Insurance Portability and Accountability Act), and those laws typically would require a more specific form of consent in any event.

[26] For example, Section 5 of the Federal Trade Commission Act empowers the Federal Trade Commission to take action against unfair or deceptive trade practices, and consumer protection laws at the state level empower similar actions by state regulators.[27] See the following for discussion of why, from an economic perspective, information asymmetries and transaction cost lead to market failure which require legal intervention, Frederik. J. Zuiderveen Borgesius, "Consent to Behavioural Targeting in European Law – What Are the Policy Implications of Insights From Behavioural Economics," Amsterdam Law School Legal Studies Research Paper No. 2013-43, Institute for Information Law Research Paper No. 2013-02 -(hereinafter: Borgesius 2013), pp. 28 and 37, SSRN-id2300969.pdf.

as much personal information of consumers as possible.[27] This leads to a *race to the bottom* in terms of privacy protection.[28]

An interesting parallel here is that the EDPB recently rejected the argument that consumers would have *freedom of choice* in these cases:[29]

> The EDPB considers that consent cannot be considered as freely given if a controller argues that a choice exists between its service that includes consenting to the use of personal data for additional purposes on the one hand, and an equivalent service offered by a different controller on the other hand. In such a case, the freedom of choice would be made dependent on what other market players do and whether an individual data subject would find the other controller's services genuinely equivalent. It would furthermore imply an obligation for controllers to monitor market developments to ensure the continued validity of consent for their data processing activities, as a competitor may alter its service at a later stage. Hence, using this argument means a consent relying on an alternative option offered by a third party fails to comply with the GDPR, meaning that a service provider cannot prevent data subjects from accessing a service on the basis that they do not consent.

By now, U.S. privacy advocates also urge the public and private sectors to move away from consent as a privacy tool. For example, Lanier and Weyl argued that privacy concepts of consent "aren't meaningful when the uses of data have become highly technical, obscure, unpredictable, and psychologically manipulative."[30] In a similar vein, Burt argued that consent cannot be expected to play a meaningful role, "[b]ecause the threat of unintended inferences reduces our ability to understand the value of our data, our expectations about our privacy—and therefore what we can meaningfully consent to—are becoming less consequential."[31]

Moving away from consent / choice-based privacy models is only part of the equation, however. In many cases, commentators have even greater concerns about the economic ramifications of large-scale data processing and whether consumers will share in the wealth generated by their data.

Disentangling Economic Objectives from Privacy Objectives

---

[27] See the following for discussion of why, from an economic perspective, information asymmetries and transaction cost lead to market failure which require legal intervention, Frederik. J. Zuiderveen Borgesius, "Consent to Behavioural Targeting in European Law – What Are the Policy Implications of Insights From Behavioural Economics," Amsterdam Law School Legal Studies Research Paper No. 2013-43, Institute for Information Law Research Paper No. 2013-02 -(hereinafter: Borgesius 2013), pp. 28 and 37, SSRN-id2300969.pdf.
[28] Borgesius 2013, p. 201.[29] EDPB Guidelines on Consent, p. 10.
[29] EDPB Guidelines on Consent, p. 10.
[30] Lanier and Weyl, "A Blueprint for a Better Digital Society," *Harvard Business Review* (Sept. 26, 2018).
[31] Andrew Burt, "Privacy and Cybersecurity Are Converging. Here's Why That Matters for People and for Companies," *Harvard Business Review* (Jan. 3, 2019), https://hbr.org/2019/01/privacy-and-cybersecurity-are-converging-heres-why-that-matters-for-people-and-for-companies.

Other than a privacy concept, consent can also be an economic tool: a means of giving consumers leverage to gain value from companies for the use of their data. The privacy objectives and economic objectives may be complementary, even to the point that it may not be easy to distinguish between them. We need to untangle these objectives, however, because they may yield different results.

Where the goal is predominantly economic in nature, the conversation tends to shift away from privacy to economic inequality and fair compensation. We will discuss the relevant proposals in more detail below, but note that all proposals require that we put a 'price tag' on personal information.

> "It is obscene to suppose that this [privacy] harm can be reduced to the obvious fact that users receive no fee for the raw material they supply. That critique is a feat of misdirection that would use a pricing mechanism to institutionalize and therefore legitimate the extraction of human behavior for manufacturing and sale."
>
> Zuboff, p. 94.

A. No Established Valuation Method

Despite personal information being already bought and sold among companies, such as data brokers, there is not yet an established method of calculating the value of personal information.[32] Setting one method will likely prove impossible under all circumstances. For example, the value of such data *to a company* will depend on the relevant use, which may well differ per company. The value of data elements often also differs depending on the combination of data elements available, whereby data analytics of mundane data may lead to valuable inferences that can be sensitive for the consumer. How much value should be placed on the individual data elements, as compared with the insights the company may create by combining these data elements or even by combining these across all customers?[33]

The value of data to *a company* may further have little correlation with the privacy risks to the consumer. The cost to consumers may depend not only on the sensitivity of use of their data but also on the potential impact if their data are lost. For example, information about a consumer's personal proclivities may be worth only a limited dollar amount to a company, but the consumer may have been unwilling to sell that data to the company for that amount (or, potentially, for any amount). When information is lost, the personal harm or embarrassment to the individual may be much greater than the value to the company. The impact of consumers' data being lost will also

[32] *See, e.g.*, Adam Thimmsech, "Transacting in Data: Tax, Privacy, and the New Economy," 94 Denv. L. Rev. 146 (2016) (hereinafter, "Thimmsech"), pp. 174-177 (identifying a number of obstacles to placing a valuation on personal information and noting that "[u]nless and until a market price develops for personal data or for the digital products that are the tools of data collection, it may be impossible to set their value"). *See also* Dante Disparte and Daniel Wagner, "Do You Know What Your Company's Data Is Worth?" *Harvard Business Review* (Sept. 16, 2016) (explaining the importance of being able to accurately quantify the enterprise value of data (EvD) but observing that "[d]efinitions for what constitutes EvD, and methodologies to calculate its value, remain in their infancy").

[33] Thimmsech at 176: "To start, each individual datum is largely worthless to an aggregator. It is the network effects that result in significant gains to the aggregator when enough data are collected. Further complicating matters is the fact that the ultimate value of personal data to an aggregator includes the value generated by that aggregator through the use of its algorithms or other data-management tools. The monetized value of those data is not the value of the raw data, and isolating the value of the raw data may be impossible."

often depend on the combination of data elements. For instance, an email address is not in itself sensitive data, but in combination with a password, it becomes highly sensitive as people often use the same email/password combination to access different websites.

Different Approaches to Valuation

One approach might be to leave it to the consumer and company to negotiate the value of the consumer's data to that company, but this would be susceptible to all of the problems discussed above, such as information asymmetries and unequal bargaining power. It may also make privacy a luxury good for the affluent, who would feel less economic pressure to sell their personal information, thus resulting in less privacy protection for consumers who are less economically secure.[34]

Another approach is suggested by Lanier and Weyl and would require companies to pay consumers for using their data, with the payment terms negotiated by the equivalent of new entities similar to labor unions that would engage in collective bargaining with companies over data rights.[35] However, this proposal also would require consumers to start paying companies for services that today are provided free of charge in exchange for the consumer's data, such as email, social media, and cloud-based services. Thus, a consumer may end up ahead or behind financially, depending on the cost of the services that the consumer chooses to use and the negotiated value of the consumer's data.

A third approach may involve the "data dividend" concept proposed by Governor Newsom. As the concept hasn't yet been clearly defined, some commentators suggest that this proposal involves individualized payments directly to consumers, while others suggest that payments are to be made into a government fund from which fixed payments would be made to consumers, similar to the Alaska pipeline fund that sought to distribute some of the wealth generated from

---

[34] Moerel & Prins 2016, para. 2.3.2. See also Morozov, Evengy (2013), "To Save Everything Click Here. The Folly of Technological Solutionism," *Public Affairs*, who warns that for *pay-as-you-live* insurance for some people the choice will not be a fully free one, since those on a limited budget may not be able to afford privacy-friendly insurance. After all, it is bound to be more expensive.

[35] Lanier and Weyl, "A Blueprint for a Better Digital Society," *Harvard Business Review* (Sept. 26, 2018) ("For data dignity to work, we need an additional layer of organizations of intermediate size to bridge the gap. We call these organizations 'mediators of individual data,' or MIDs. A MID is a group of volunteers with its own rules that represents its members in a wide range of ways. It will negotiate data royalties or wages, to bring the power of collective bargaining to the people who are the sources of valuable data…."). Lanier extends this theory more explicitly to personal information in his *New York Times* video essay at https://www.nytimes.com/interactive/2019/09/23/opinion/data-privacy-jaron-lanier.html. *See also* Imanol Arrieta Ibarra, Leonard Goff, Eigo Jiminez Hernandez, Jaron Lanier, and E. Glen Weyl, "Should We Treat Data as Labor?: Moving Beyond "Free," American Economic Association Papers & Proceedings, Vol. 1, No. 1 (May 2018) at https://www.aeaweb.org/articles?id=10.1257/pandp.20181003, at p. 4 (suggesting that data unions could also exert power through the equivalent of labor strikes: "[D]ata laborers could organize a "data labor union" that would collectively bargain with [large technology companies]. While no individual user has much bargaining power, a union that filters platform access to user data could credibly call a powerful strike. Such a union could be an access gateway, making a strike easy to enforce and on a social network, where users would be pressured by friends not to break a strike, this might be particularly effective.").

Alaska's oil resources to its residents. Given that data has been called the "new oil," the idea of a data dividend modeled on the Alaska pipeline payments may seem apt, although the analogy quickly breaks down due to the greater difficulty of calculating the value of data.[36] Moreover, commentators have rightly noted that the data dividend paid to an individual is likely to be mere "peanuts," given the vast numbers of consumers whose information is being used.[37] Whatever valuation and payment model - if any - might be adopted, it risks devaluing privacy protection. The data dividend concept, as well as the CCPA's approach to financial incentives, each suggest that the value of a consumer's personal information is measured by its value *to the company.* [38] As indicated before, this value may have little correlation with the privacy risks to the consumer. Though it is commendable that these proposals seek to provide some measure of compensation to consumers, it is important to avoid conflating economic and privacy considerations, and avoid a situation where consumers will be trading away their data or privacy rights.[39] Although societies certainly may decide to require some degree of compensation to

---

[36] *See, e.g.*, Marco della Cava, "Calif. tech law would compensate for data," *USA Today* (Mar. 11, 2019) ("[U]nlike the Alaska Permanent Fund, which in the '80s started doling out $1,000-and-up checks to residents who were sharing in the state's easily tallied oil wealth, a California data dividend would have to apply a concrete value to largely intangible and often anonymized digital information. There also is concern that such a dividend would establish a pay-for-privacy construct that would be biased against the poor, or spawn a tech-tax to cover the dividend that might push some tech companies out of the state.").

[37] Steven Hill, "Opinion: Newsom's California Data Dividend Idea is a Dead End," *East Bay Times* (Mar. 7, 2019) ("While Newsom has yet to release details…the money each individual would receive amounts to peanuts. Each of Twitter's 321 million users would receive about $2.83 [if the company proportionally distributed its revenue to users]; a Reddit user about 30 cents. And paying those amounts to users would leave these companies with zero revenue or profits. So in reality, users would receive far less. Online discount coupons for McDonald's would be more lucrative.").

[38] Cal. Civ. Code § 1798.125(a)(2) ("Nothing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer's data."). The CCPA originally provided that the difference must be "directly related to the value provided *to the consumer* by the consumer's data," but it was later amended to require the difference to be "directly related to the value provided *to the business* by the consumer's data." (Emphases added.) The CCPA does not prescribe how a business should make this calculation. The Final Proposed CCPA Regulations would require businesses to use one or more of the following calculation methods, or "any other practical and reliable method of calculation used in good-faith" (Final Proposed CCPA Regulations, 20 CCR § 999.307(b)):

- The marginal value to the business of the sale, collection, or deletion of a consumer's data or a typical consumer's data;
- The average value to the business of the sale, collection, or deletion of a consumer's data or a typical consumer's data;
- Revenue or profit generated by the business from separate tiers, categories, or classes of consumers or typical consumers whose data provides differing value;
- Revenue generated by the business from sale, collection, or retention of consumers' personal information;
- Expenses related to the sale, collection, or retention of consumers' personal information;
- Expenses related to the offer, provision, or imposition of any financial incentive or price or service difference; or
- Profit generated by the business from sale, collection, or retention of consumers' personal information.

[39] *German Data Ethics Commission, Standards for the Use of Personal Data*, Standard 5: "The Data Ethics Commission believes that "data ownership" (i.e., exclusive rights in data modelled on the ownership of tangible assets or on intellectual property) would not solve any of the problems we are currently facing, but would create new problems instead, and recommends refraining from their recognition. It also advises against granting to data subjects

consumers as a wealth redistribution measure, it will be important to present this as an economic tool and not as a privacy measure.

Closing Thoughts

As the late Giovanni Buttarelli in his final vision statement forewarned, "Notions of 'data ownership' and legitimization of a market for data risks a further commoditization of the self and atomization of society…. The right to human dignity demands limits to the degree to which an individual can be scanned, monitored and monetized—irrespective of any claims to putative 'consent.'"[40]

There are many reasons why societies may seek to distribute a portion of the wealth generated from personal information to the consumers who are the source and subject of this personal information. This does not lessen the need for privacy laws to protect this personal information, however. By distinguishing clearly between economic objectives and privacy objectives, and moving away from consent-based models that fall short of both objectives, we can best protect consumers and their data, while still enabling companies to unlock the benefits of AI and machine learning for industry, society, and consumers.

---

copyright-like rights of economic exploitation in respect of their personal data (which might then be managed by collective societies)", See further Standard 6:6, where it argues that data should not be referred to as a "counter-performance" provided in exchange for a service, even though the term sums up the issue in a nutshell and has helped to raise awareness among the general public. https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_EN.pdf?__blob=publicationFile&v=2.

[40] International Association of Privacy Professionals, Privacy 2030 for Europe: A New Vision for Europe at p. 19, https://iapp.org/media/pdf/resource_center/giovanni_manifesto.pdf.

UK Enforcement Actions Underscore the Importance of Due Diligence When Using Third-Party Marketing Providers

Alice Brunning, Annabel Gillham, and Christine Lyon
December 2019

Recent UK enforcement actions highlight the risks to companies of relying on third-party providers to obtain marketing consents from individuals on their behalf. A claims company has been separately fined by both the UK's Information Commissioner's Office (ICO) and by its functional regulator, the UK's Claims Management Regulator (CMR), for improper marketing activities conducted on its behalf by marketing companies. Specifically, the company reportedly engaged several third-party marketing companies to send marketing text messages to UK consumers on its behalf. The company did not itself obtain the consumers' personal data or their consent to receive the messages; rather, it relied on the third-party marketing companies to obtain the consumers' data and their consent to receive marketing, and to send the messages on its behalf.[41] This reliance proved unfounded, as the ICO and CMR found that sufficient consents had not been obtained from the consumers, and the company was fined £120,000 by the ICO and £91,000 by the CMR for these violations. Further, in upholding the fine issued by the CMR, the UK's First Tier Tribunal Court (FTT) recently identified suggested measures for companies to take in acquiring data from third-party providers for marketing purposes.

What was the contravention?

Hall & Hanley Limited (H&H) was a UK company set up to assist consumers with claiming refunds of mis-sold Payment Protection Insurance (PPI)[42]. H&H allegedly instigated the transmission of over 3.5 million direct marketing messages, which requested individuals to get in touch directly with H&H if they wanted to discuss PPI.

The CMR issued a fine of £91,000 to H&H earlier this year for a breach of the claims management sector regulations that were in place at the time of the contravention (the "**Regulations**"). The Regulations required regulated firms to take reasonable steps in relation to any arrangement with third parties to confirm that any referrals, leads or data have been obtained in accordance with the requirements of UK legislation and the Regulations.[43] H&H failed to conduct proper due diligence on the data and it was therefore acquired in breach of the UK's Privacy and Electronic Communications Regulations (PECR), as the proper consents had not been obtained from individuals.

In a separate investigation in May 2019, the ICO issued H&H a fine of £120,000 for breaching the PECR. The ICO found the company had sent 3.5 million text messages about compensation claims

[41] https://ico.org.uk/media/action-weve-taken/mpns/2614866/hall-and-handley-ltd-mpn-201905.pdf, para. 20.
[42] PPI was designed to cover repayments in certain circumstances. It was often sold to UK consumers when they purchased credit arrangements or loan products. After an investigation, the UK's Financial Conduct Authority (FCA) found that PPI was often mis-sold and therefore introduced rules that allowed customers to potentially reclaim the cost of the PPI from banks and other providers.
[43] Principle 2(e) of the Conduct of Authorised Persons Rules 2014.

without having the correct consent. As the instigator of the direct marketing messages, the ICO concluded that it was the responsibility of H&H to sure that valid consent to send those messages had been acquired.

What did the FTT say?

Earlier this month, the FTT upheld the fine issued by the CMR for a breach of the Regulations on the basis that the fine was not disproportionate or unjust. Although the FTT's decision is specific to claims management organizations, it also provides some useful guidance about using data collected by a third party for an organization's own purposes:

- **FTT's suggested action steps.** The FTT advised that it would not be appropriate to be prescriptive about the steps that should be taken in order to comply with the Regulations. However, the FTT did set out some steps that it considers to be reasonable for organizations with a similar business model to that of H&H to follow, these include:
    - Reviewing relevant website privacy policies;
    - Reviewing the opt-in mechanisms and checking that all opt-in mechanisms are consistent with the privacy policies of the websites concerned;
    - Reviewing an appropriate sample of the data to be supplied before purchase to confirm that appropriate opt-ins had been obtained;
    - Putting a degree of responsibility on the part of the supplier to provide compliant data by seeking a warranty from it that all relevant data supplied will be in compliance with the legislation; and
    - Seeking guidance from the regulator on points of difficulty or where clarification of the regulator's approach or policy is needed.
- **Contractual assurances alone are not sufficient.** The FTT said that the responsibility is on each person in the chain of the transaction to take reasonable steps to ensure that the data is being used compliantly.
- **Timing of due diligence.** Due diligence should also carried out by the controller of the data before it uses it for commercial purposes.
- **It is not necessary to review all data**. The FTT advised that is it not necessary to review all data before it is used. However, "all reasonable steps" should be taken. Therefore, a process of sampling of data is a reasonable step to take and the question then is whether the sample is large enough to give a reasonable indication of whether substantially all of the data acquired will be compliant.

- **Shifting responsibility.** A regulated firm cannot shift the responsibility for establishing that data will be used compliantly onto the regulator. The FTT stated that the regulator is under no duty to prescribe to an authorized firm the precise steps that the firm should take to ensure compliance.

What can we learn from this?

The FTT has made it very clear that it is not adequate to solely rely on contractual assurances from the supplier that the data has been supplied in accordance with relevant legislation. Organizations should ensure that they are taking reasonable steps so that they can lawfully engage a third-party marketing company to send marketing to its own lists.

It is also clear that regulated firms are under additional scrutiny from the UK's Financial Conduct Authority (FCA) and may even be subject to fines from multiple regulators. It should also be noted that there is a memorandum of understanding between the FCA (which has now taken over the duties of the CRM) and the ICO about how they deal with enforcement issues. We therefore expect to see further overlap between these regulators as the awareness of data protection continues to grow.

Final thoughts

The importance of proper due diligence when using data collected by third parties is not just UK-specific. For example, the draft regulations issued under the California Consumer Privacy Act of 2018 (the "**CCPA**") would impose due diligence requirements on companies that "sell" personal information that they did not collect directly from the consumers: specifically, the draft regulations would require such companies to confirm that the source of the information provided appropriate privacy notices to the consumers, and also obtain a signed attestation from the source of the information describing how the notice was provided, and including a copy of the notice.[44] Although these draft regulations are not yet final, FTT's decision in the UK and the draft CCPA regulations in the U.S. suggests that companies may face heightened expectations to conduct due diligence when acquiring consumer data from third parties.

[44] Draft CCPA regulations at 999.305(d)(2).

California AG Issues Advisory on California Data Broker Law

Christine Lyon
January 2020

California's Attorney General has issued a brief advisory providing consumers with an overview of their rights under the California Consumer Privacy Act (CCPA), which went into effect on January 1, 2020, as well as additional information relating to California's new data broker law. Although the advisory offers no new guidance on CCPA requirements, it demonstrates the Attorney General's desire to ensure that California consumers are informed of their rights under the CCPA. The advisory also serves as an important reminder of the new California data broker law, including the new requirement for companies acting as "data brokers" to file an online registration.

The advisory briefly describes consumers' rights to know, delete, and prevent sales of their personal information, and explains that businesses may not discriminate against consumers who exercise their CCPA rights. The advisory also summarizes the thresholds an entity must meet in order to be considered a "business" subject to the CCPA, and explains that the CCPA affords consumers a private right of action if their personal information is subject to certain types of data breach.

In addition to its CCPA overview, the advisory also contains important information related to California's new data broker law. As described in our prior client alert, this data broker law was enacted in October 2019, but received limited attention at the time given the near-simultaneous enactment of five other bills amending the CCPA. However, the law is significant and requires action on the part of those businesses that may be classified as "data brokers."

The data broker law – codified at Cal. Civ. Code §§ 1798.99.80 *et seq*. – applies to "data brokers," which it defines as businesses that knowingly collect and sell to third parties the personal information of consumers with whom the businesses do not have direct relationships. ("Business" has the same meaning that it has under the CCPA.)

Under the law, a data broker must register with the California Attorney General on or before January 31 following each year when it meets the requirements of the "data broker" definition. The law requires the Attorney General to make a registration website available to the public, and the Attorney General's advisory provides a link to that registration website for data brokers. The data broker law also requires the Attorney General to create a page on its website where information provided through data broker registrations will be accessible to the public, and the Attorney General has set up this page at https://www.oag.ca.gov/data-brokers. In order to complete registration, data brokers must provide their names and contact information (including their primary physical, email, and website addresses), as well as any additional information they wish to provide regarding their data collection practices. Data brokers must also pay an annual registration fee. Any data broker that fails to register may be subject to a civil penalty of $100 for each day it remains unregistered, along with other penalties, fees, and costs.

Although California's new data broker law is separate from the CCPA, it is also related to the CCPA because both of these laws seek to give consumers greater visibility concerning the companies that process their personal information.

For additional thought leadership and compliance tools on these topics, please visit MoFo's CCPA Resource Center.