UNCTAD
Making Digital Markets Work for Consumers: Competition, Consumer Protection and Data
5 November 2021

Protecting consumer's data in the digital world: Advocating Fairness by Design

Prof. Christine Riefa, University of Reading, School of Law[1]
c.j.a.riefa@reading.ac.uk
@Cyberchristine

There is wide acknowledgment that the use of data has many benefits for consumers. But there is a darker side to the collection and use of data that so far legislators and enforcers have struggled to curb. The failure of the law, where it exists[2], is not in the lack of recognition of privacy and the protection of personal data as a major concern, nor the existence of regulation. Instead, the failure seems to primarily reside in:

- the inability to address, in a timely fashion, a host of challenging factors, notably multi-regulatory concerns;
- and fostering the continuation of pre-established paradigms in legislation and enforcement structures that do not work in the digital sphere.

Challenges to consumer data protection

The challenges come from a number of distinct, yet intertwined factors. Those include first and foremost territoriality. The law is still organised along geographical lines and there is a need for a connection with a state for its laws or courts to have jurisdiction. As a result, enforcement across border is hugely problematic leaving many businesses, who do not abide by the law, unchecked. Lack of compliance is also driven in part by the business structures prominent in the digital economy, where maximisation of profit reigns supreme and recompense of shareholders remains the primary goal. This coupled to the fact big businesses are able to monopolise data for their own profits through economies of scale means that the digital economy is skewed. Differences in social norms and values also play a part in creating a disjointed map of the world, feeding difficulties in cross-border enforcement. Data protection approaches and consumer protection regulatory mixes indeed vary across the world. The UNCTAD Digital Economy 2021 report highlights the divergent approaches to data

[1] *The author wishes to thank the UNCTAD Secretariat for their kind invitation. The author is based in the UK. This piece does rest on primarily EU and UK materials which would require interpretation in a national and regional context.*

[2] For information on the legislative frameworks in place, see UNCTAD Tracker, https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commerce-legislation-worldwide and in particular, on data protection, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide which shows that 1/3rd countries still do not have operational legal frameworks.

and cross-border data flows.[3] It classifies the US approach for example as one that promotes markets and innovations[4] and thus tends to be hand off when it comes to regulation. In China and Russia, the appetite for intervention is far greater and the approach can be described as interventionist. The interventions center around promoting national and public security. The EU also is interventionist because it centers around the protection of individual rights and fundamental values. Because the regulatory framework has different end-goals and rationale it is necessarily difficult to reconcile at international level. As states have different priorities, they have also different red lines. India for example is also positioned to be interventionist in that it has enacted legislation in recent years, but its focus is very much on combatting what is sometimes coined 'data colonialism' and thus diverting data of Indian citizens away from the US big tech sector.[5]

Privacy and data protection as a multi-regulatory concern in the digital world

The protection of consumer data is an issue that cuts across many areas of the law that used to be very distinct and often in regulatory competition. The legislations in place do not, by and large, acknowledge each other's existence or, if they do, they do not always articulate in a detailed manner how the competing regimes may apply in tandem.

The right to privacy is recognized as a human right. The right is recognized at international as well as regional and domestic level. At international level, Art 12 of the Universal Declaration of Human Rights states: 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.'.[6] In the UK, the Right to Respect to Privacy is protected by Human Rights Act 1998 and derives from two distinct instruments: the European Convention of Human Rights (art 8)[7] and the European Charter of fundamental rights.[8] However, privacy is not an all-encompassing right and it has limitations.[9] Article 8 of the European Convention on Human Rights also enables encroachments on the right in accordance with the law, and where necessary in a democratic society in the interests of national security, public safety, for the prevention of disorder and crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. In human rights law, the protection granted is thus very much limited to the relationships between the state

[3] UNCTAD, *Digital Economy Report 2021 Cross-border data flows and development: For whom the data flow* (2021) https://unctad.org/webflyer/digital-economy-report-2021

[4] *Digital Economy Report 2021* (n 3) 100.

[5] *Digital Economy Report 2021* (n 3) 110.

[6] Article 12, Universal declaration of human rights, https://www.un.org/en/about-us/universal-declaration-of-human-rights. For work carried out by the Office of the High Commissioner relating to this area, see https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx, and the report on the Right to Privacy in the Digital Age https://www.ohchr.org/EN/Issues/DigitalAge/Pages/cfi-digital-age.aspx.

[7] https://www.echr.coe.int/documents/convention_eng.pdf.

[8] https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights_en. Although note this instrument no longer applies post BREXIT, only national legislation subsists.

[9] For eg in the UK, In *Wainwright v Home Office* [2003] UKHL 53 the court confirmed that there is no overarching course of action for an 'invasion of privacy' although claims for misuse of private information in the UK are opened to individuals.

and the individual. The protection does not generally bite when the interference concerns two private parties.

There is clear evidence that data protection laws in the EU (GDPR notably) were devised to ensure the respect of this human right, but it allows this protection to take place in a commercial environment, ie the private law sphere. Recital 1 GDPR explains that the protection of natural persons in relation to processing of personal data is a fundamental right. Art 8(1) of the Charter of Fundamental Rights of the European Union & Art 16(1) of the TFEU provide that everyone has the right to the protection of personal data concerning him or her. Recital 4 GDPR is also evidence of this concern for human rights but recognizes the balance that normally needs to be struck between competing human rights.[10]

Privacy is normally broader than data protection. Data protection covers all personal data regardless of their impact on privacy. Privacy forbids conduct that are an interference on the privacy of the individual whereas data protection is about limited to the conditions of data processing. However, it is true that by improving the conditions of processing, privacy of individuals is protected.

To control the way data is processed, the GDPR recognises 7 rights of data subjects including transparency and fairness. The legislation seeks to ensure that all data subjects are able to give consent to the collection and treatment of their data by private organisations (public entities are also caught, but there are a number of carve out for national security, etc).

For a very long time, human rights and data protection concerns were centred around the use of data by the State or emanations of the state and concerned the interactions with citizens. But the advent of e-commerce and more recently social media have somewhat distorted this primary focus. Data collection is now a commercial activity. The data subject is no longer simply a citizen, but also a consumer.

There is therefore also a recognition of the protection of privacy in the United Nations Guidelines for Consumer Protection in section III on General Principles bridging this gap in scope. Para 5 k) recognizes 'privacy and the global free flow of information' as a legitimate need of consumers, but there is no clear definition of whether privacy is to be understood as a human rights concern or if the terminology is to have a meaning distinct or complementary within the confine of consumer protection.

As a result of the exponential growth of data collection and cross-border data flows, other legal disciplines needs to be explored as a way to control harm that may result from the use and manipulation of data, namely competition law and consumer law.

[10] Recital 4 states: '*The processing of personal data should be designed to serve mankind. The right to protection of personal data is not an absolute right; It must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognized in the Charter as enshrined int eh Treaties, in particular, the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience or religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and the right to a fair trial, and cultural, religious and linguistic diversity.'*

Competition law, for example, can offer some potential protection against the use of consumers' data, by looking at how an entity with dominant market power can make use of information collected and/ or restrict its access for competitors. Competition law however does control the architecture of marketplaces not data itself. Consumer law can also offer some solutions with the use of unfair terms as well as unfair commercial practices regulations notably. In the GDPR and generally in data protection laws, the person protected is a data subject. It is a passive role that is protected. Contrast this with the consumer protected in consumer protection legislation and denotes a more active role undertaken by the individual. Consumer protection laws are looking at the way consumers interact with businesses.

Scholarship has started to engage with exploring how the different regimes may imbricate or intertwine[11] exhibiting some preferences for the application of the consumer law framework as a solution to protection.[12] Although Graef et al. call for more coherent enforcement and closer collaboration between different authorities (data protection, competition and consumer) pointing to the European Digital Clearinghouse (voluntary network of authorities) because they see that the issue is not with a lack of substantive fairness but a lack of enforcement of existing rules.

Despite relatively clear and well-defined legal regimes and enforcement frameworks to boot, regulatory areas and enforcers alike struggle to make sense of the use of data in the digital economy because it cuts across all traditional divides. In addition, the competing application of the existing legislation requires in many cases adaptations, not least enabling the cooperation of enforcers needed to intervene to protect consumers.

In the UK, in a case concerning Google's privacy sandbox, the Competition and Market Authority (CMA) and the Information Commissioner's Office (ICO) were presented with a dual submission to both authorities having agreed that the authorities would consider the case together.[13] They have as a result created a Digital Regulation Cooperation Forum, entered an MoU and issued a statement detailing how they will cooperate moving forward.[14] However, as the systems pertaining to data protection, competition law and consumer law were developed in silos, i.e. independently from one another, the sharing of information between enforcers is not always possible and may require additional enabling legislation.

Besides, other obstacles may lie in the way: budgets may be allocated in ways that do not account for activities that will bridge over another area of law; individuals may feel threatened by the inability to retain control of enforcement strategies.

[11] See for eg, Inge Graef, Damian Clifford and Peggy Valcke, 'Fairness and Enforcement: Bridging Competition, Data Protection, and Consumer Law' (2018) 8 *International Data Privacy Law* 200; Frederik Zuiderveen Borgesius, Natali Helberger, Agustin Reyna, The perfect match? a closer look at the relationship between eu consumer law and data protection law 54 (2017) 5 *CMLR* 1427.

[12] See, Goanta, Editorial - European Consumer Law: The Hero of our Time, 10 (2021) 5 *EuCML*; Leiser, Caruana, Dark Patterns: Light to be found in Europe's Consumer Protection Regime 10 (2021) 6 *EuCML* forthcoming.

[13] https://www.thelawyer.com/festival-talent-2021-stephen-dnas-preiskel/

[14] https://www.gov.uk/government/publications/cma-ico-joint-statement-on-competition-and-data-protection-law

Old standards do not fit new paradigms

In addition, in many instances, the law may also be ineffective because it may require consumers or enforcement authorities to act in order to correct the practice and repair consumer harm after the event rather than prevent it. All too often, information is used as a proxy to protection. This is for example the case in the EU, where both consumer laws and the General Data Protection Regulation require the provision of a long list of information to the consumer, expecting that the rational consumer will either be able to avoid the practices altogether or at the very least claim the rights the legislation grants. The issue with those methods of protection is that, with regards to data use by big tech, they are not always terribly effective. Simply telling the consumer the way the information will be processed, and its purpose is sufficient under the GDPR. The GDPR does not really take into account the potential efficacy of those disclosure and/ or if the consumer is able to find an alternative on the market.

Consumer law also relies on information as a proxy to protection in many situations. But it offers some remedies. For example, a business term that reserves all rights to the data of an individual might be judged unfair (and struck out of a contract) or it may be considered an unfair commercial practice if the collection and treatment was done in violation of data protection principles. But in many countries, the law requires consumers or enforcement authorities to act in order to correct the practice and repair consumer harm after the event.

Indeed, the premise of consumer protection laws and data protection laws in many regards has rested on the idea that informed consumers will make optimal choices. This is anchored in neo-classical economic theories that have underpinned the development of legislation in the EU and many other regions. The belief is that armed with the information about a product or service, or with the data privacy notice of the website or internet of things product they use, they will be able to make the right decision. And if they have not, it is expected that they will exercise the rights they are granted and seek redress. What this means is that we expect consumers to effectively be the arbiter of markets. But competition in the digital marketplace can only work if consumers can fulfil this function. At present, they are not.

The use of data puts a real spanner in the works. When the machines can make inferences[15] about you, can present advertising and frame product choices for you and generally apply dark patterns[16], can track your every moves[17] and even calculate what you may find an acceptable price (willingness to pay)[18], consumers become powerless. Choice is no longer

[15] S Wachter, B Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) 1 *Columbia Business Law Review* 494.

[16] Norwegian Consumer Council (Forbrukerrådet), *Deceived by Design. How Tech Companies use dark patterns to discourage us from exercising our rights to privacy* (2018) https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/

[17] On tracking and other behavioural advertising practices being an unfair commercial practice, see C Riefa and C Markou, Online marketing: advertisers know you are a dog on the Internet! in A Savin and J Trzaskowski (eds.), *Research Handbook of EU Internet Law* (Edward Elgar 2014) 402.

[18] C Riefa, Consumer law enforcement as a tool to bolster competition in digital markets: A case study on personalised pricing in UNCTAD, *Competition and Consumer Policies for Inclusive Development in the Digital Era* (UNCTAD 2021) 15, https://unctad.org/system/files/official-document/ditccplp2021d2_en_0.pdf

'real'. Consumers cannot influence the way the market works. They cannot vote with their feet. Worse, the high concentration in those markets means that there is often no meaningful alternative choice.[19] Even those consumers who are aware of the issue and willing to go elsewhere are often unable to do so. Besides, even if those consumers wanted to obtain redress after the event, they would find it quite a difficult task and very few, in the absence of collective action mechanisms[20] or effective dispute resolution mechanisms (courts or ADR), would be able to pursue the matter. As a result, here again, consumers are not in a position to really force a change of behavior on the supply side no matter how diligent they may be.

This in turn can damage the trust consumers experience in markets. Consumers become disengaged and apathetic because it is in fact the most rational thing to do.[21] As a result, they no longer fulfil their role as 'regulators' of markets. Competition on its own is no longer an effective tool. Worse, this creates a race to the bottom – to remain competitive, even 'fair' businesses struggle to operate without using the same techniques. Exploitative practices become the default. Recent studies have confirmed the alarming use of dark patterns, those underhand techniques to nudge consumers into options that are intrusive of privacy and are based on unethical and exploitative principles.[22]

Paradigm shift required to protect consumers' data in the digital world

In countries where the law is already established, there is a need for a paradigm shift, particularly in consumer law but also in other areas. For too long, the expectation has been for consumers to beware making it their responsibility to protect their privacy and more generally their data. It has been expected of them to take action to redress the balance thanks to the tools legislators have put at their disposal and they are often blamed (although perhaps not always openly) for their inaction and their failure to go to court or to use other avenues for redress (ADR) to claim their rights. Competition failures have also pointed to consumer disengagement or inactivity as a cause.

The reality however is that consumers are not able to be all those things. We must expect that businesses will behave fairly by design[23] and make invasive treatment of our data an opt-in rather than an opt-out activity. We must demand that data privacy friendly solutions become a commercial argument and a marker of quality.

[19] Note however that privacy friendly rivals are starting to emerge, but to date their reach remains quite limited. See for example in the search engine market, Duckduckgo.com and Quant.com.

[20] For example in the UK, see Lloyds v Google where the Supreme Court rejected unanimously the ability of consumers to mount a group representative action (called group litigation) for enforcement of Section 13 of the Data Protection Act 2018, https://www.supremecourt.uk/cases/uksc-2019-0213.html

[21] P Siciliani, C. Riefa, H Gamper, *Consumer Theories of Harm: An economic approach to consumer law enforcement and policy making* (Hart Publishing 2019).

[22] See for eg. A Mathur, G Acar, M.J Friedman, E Lucherini, J Mayer, M Chetty, A Narayanan, 'Dark patterns at scale: Findings from a crawl of 11K shopping websites' (2019) ACM Conference on Computer-Supported Cooperative Work and Social Computing (CSCW 2019), https://arxiv.org/abs/1907.07032.

[23] P Siciliani, C. Riefa, H Gamper, *Consumer Theories of Harm: An economic approach to consumer law enforcement and policy making* (Hart Publishing 2019).

There is therefore a need to reverse expectations. It should no longer be about consumers defending themselves against data privacy abuses (using rather imperfect instruments in the process); but it should be about businesses behaving fairly. The recognition of a general and positive duty to trade fairly in consumer law (and potentially in other fields) is a way forward to enable consumer to be truly and effectively protected. There is room for more forceful public enforcement to step in where consumers cannot defend themselves effectively. In digital markets, this constitutes undoubtedly the largest amounts of transactions and interactions. There is also room for using consumer law as an apt complement to competition policy[24] and data protection alike.

Conclusion

The road to consumer data protection is likely long and arduous. Consumers the world over face unprecedented challenges to the use made of their data for good and bad. The legislative framework where they exist were set up in an era that predates large cross-border data flows. The system is not set to tackle many of the challenges the Internet and digitalization have brought to the fore. Competing legal systems of different traditions, enforcers with limited means and often a lack of cooperation networks at the national, regional or international level compound the difficulties consumers encounter. In addition, consumers who are normally conceptualized in legislation as competent market actors have seen their ability to behave as is expected of them increasingly difficult. The digital world has the propensity to render all consumers vulnerable and in need of additional protection.[25] Help hopefully is on the way before we reach the point of no return and enter the Metaverse, where all life will be digital and regulated by contract (as opposed to leaving room for public intervention in Business to consumer relationships as is currently the case).[26] There is no one size fits all for intervention. The work underway at UNCTAD is well placed to assist in finding some workable middle ground but it will take time. However, we see some encouraging emerging convergence. There seems to be an agreement that platform dominance and the architecture of digital markets needs revising. Competition law does take care of this in large part. The EU is currently reforming this area notably with the Digital Market Act and the Digital Services Act. In the US, some signs are afoot of a different approach also, most notably with the appointment of Lina Kahn as the Chair of the FTC. It is in large part her work on antitrust that

[24] C Riefa, Consumer law enforcement as a tool to bolster competition in digital markets: A case study on personalised pricing in UNCTAD, *Competition and Consumer Policies for Inclusive Development in the Digital Era* (UNCTAD 2021) 15, https://unctad.org/system/files/official-document/ditccplp2021d2_en_0.pdf

[25] See for eg, C Riefa, The protection of vulnerable consumers in the digital age, (UNCTAD RPP 2020), https://unctad.org/system/files/non-official-document/ccpb_RPP_2020_05_Present_Christina_Riefa.pdf who conceptualises the digital sphere as a systemic vulnerability; Also see Natali Helberger, Orla Lynskey, Hans-W Micklitz, Peter Rott, Marijn Sax, Joanna Strycharz, *EU Consumer Protection 2.0., Structural Asymetries in Digital Consumer Markets* (BEUC, March 2021) 5 who explain: 'in digital markets, consumer vulnerability is not simply a vantage point from which to assess some consumers' lack of ability to activate their awareness of persuasion. In digital marketplaces, most if not all consumers are potentially vulnerable'.

[26] See the announcement by Facebook to rebrand as Meta and move a different type of interface, one of social online experiences in 3D, https://about.fb.com/news/2021/10/facebook-company-is-now-meta/.

turned the wave into bringing more focus on digital market structures.[27] Action is also underway ramping up efforts to combat data breaches and cyberattacks that have exposed Americans to monetary loss, identify theft and other harms. The FTC has strengthened a data security rule, requiring financial institutions to put more safeguards in place to protect user data.[28] We also see more interventions coming from consumer law. Many of the practices relating to data collection are perceived as unfair and most countries in the world that do have a body of legislation protecting consumers also have provisions catching unfair commercial practices. Some enforcement authorities have also had great success using this route for enforcement.[29] Consumers have also made use of collective actions to obtain remedies for the misuse of data.[30] However, the systems, no matter how well they cope, seldom offer consumers ex ante protection. It is often too little too late and the remedies cannot neutralize the 'unfair' use of data that has already been made. As a result, there is a need for a paradigm shift. The expectation should be for businesses to behave fairly by design[31] and make invasive treatment of our data an opt-in rather than an opt-out activity.

For developing countries, who may not yet have a fully functioning system of consumer law, competition, or data protection laws, officials will likely have to adopt some framework in the not-too-distant future. In doing so they will likely have to reflect on the lessons that other regions have learned. Many countries are indeed embracing consumer protection and other areas of law at a time where they struggle to move from analogue to digital. It is therefore an opportunity to design systems of governance that are adapted to this new paradigm and forward looking. Leapfrogging as much as possible and bypassing the period of adaptation many countries have experienced may bring great advantages. Designing laws that focus on principles rather than be too constrictive (as they can often act as a straightjacket (e.g. gap cases in competition law, mishaps of the GDPR and its control of cross-border data flows) would also be recommended. Developing countries in particular have an opportunity to design laws and enforcement infrastructures that build in fairness and privacy by design and by default.

My hope is that other countries, already equipped with legislation and infrastructures, will be willing to embrace the idea of change. A change of course, to ensure a more prosperous digital future for all. A change that leads to fairness for all in consumer digital markets.

---

[27] Lina Kahn, Amazon's Antitrust Paradox (2017) 126 *Yale Law Journal*, 710-805, https://www.yalelawjournal.org/pdf/e.710.Khan.805_zuvfyyeh.pdf; See also Nancy Scola, 'Lina Kahn is not worried about going too far' https://nymag.com/intelligencer/article/lina-khan-ftc-profile.html

[28] https://www.ftc.gov/news-events/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial

[29] See notably the Italian consumer enforcement authority, the AGCM. See for example, WhatsApp and Unfair Terms https://www.agcm.it/dotcmsDOC/allegati-news/CV154_vessestratto_omi.pdf and data sharing by Facebook/ WhatsApp https://www.agcm.it/dotcmsDOC/allegati-news/PS10601_scorrsanz_omi.pdf.

[30] See for eg, https://www.beuc.eu/press-media/news-events/euroconsumers-launch-collective-action-against-facebook. However, note that this is not the case everywhere. Notably see in the UK, *Llyods v Google* where the Supreme Court rejected the possibility of group litigation for the enforcement of section 13 of the Data Protection Act 2018 (https://www.supremecourt.uk/cases/docs/uksc-2019-0213-judgment.pdf).

[31] P Siciliani, C. Riefa, H Gamper, *Consumer Theories of Harm: An economic approach to consumer law enforcement and policy making* (Hart Publishing 2019).

About the author:

Prof Christine Riefa (University of Reading) specialises in consumer and e-commerce/new-tech law. Prof Riefa is widely published on these topics with work cited in official documents from international institutions (incl. The World Economic Forum, UNCTAD, the OECD) and academic scholarship. Her latest books include: *Consumer Theories of Harm, an economic approach to consumer law enforcement and policy making* (Hart 2019)with P Siciliani and H Gamper ; *Vulnerable Consumers and the Law*, *Consumer Protection and Access to Justice* (Routledge 2021) with S Saintier; *Consumer Protection and Online Auction Platforms* (Routledge 2016). Prof Riefa currently serves as a member of the United Nations Working Group on Consumer Protection in E-Commerce as part of UNCTAD Inter-Governmental Group of Experts. She is a member of the Consultative Group of Experts of the Committee for the development of an International Code for the Protection of Tourists at the World Tourism Organisation (A specialised agency of the United Nations). She was the expert to the rapporteur on the reform of the product safety directive at the European Economic and Social Committee, helping to draft Opinion INT/957-EESC-2021.

Prof Riefa is also a Board Member of the International Association of Consumer Law and a founding editor of the Journal of European Consumer and Market Law (EuCML, published by Beck and available on Kluwer).