Sixth Intergovernmental Group of Experts on

Consumer Law and Policy

18-19 July 2022

Room XVII, Palais des Nations, Geneva

For a Technological Approach to Consumer Law Enforcement and Policy Making in the Digital Age

Presentation

KEYNOTE Address

Prof. Christine Riefa,
University of Reading

For a technological approach to consumer law enforcement and policy making in the digital age

Prof. Christine Riefa, University of Reading[1]

Thank you, Madame Chair. Madame Secretary-General, Excellencies, Distinguished experts, Ladies and Gentlemen. It is a great honour to address you to reflect on the future of consumer law enforcement.[2] In the short time I have today, I wish to advocate for the adoption of a technological approach to consumer law enforcement and policy making in the digital age.

Consumer law was largely developed before the advent of the internet. With the recent expansion of electronic commerce, enforcement frameworks that were developed in the analogue era are ill-placed to cater for the exponential growth of unfair commercial practices online and the changes in market structures and business models (notably those based on the mass collection of data). While acknowledging that the use of technology has had many welcomed benefits for consumers, it has also facilitated the spread of consumer detriment on a scale never seen before.

Businesses engaged in e-commerce have embraced technology, from cookies to machine learning and AI, to track, predict and influence consumer behaviours and choice. However, so far, national enforcers have not incorporated technology to enable the monitoring and sanctioning of the supply side as readily as industry

---

[2] Christine Riefa et al., Cross-border enforcement of consumer law: looking to the future – a report to UNCTAD's working group on e-commerce, sub-working group 3: cross-border enforcement cooperation (forthcoming).

have embraced it to deliver new goods and services to consumers.[3] Indeed, the use of technology in consumer law enforcement is only nascent[4] with merely a handful of consumer enforcement authorities around the world harnessing technology (that goes beyond the running of databases) in their enforcement practice.[5]

However, to take effective enforcement actions against price discrimination, choice architecture[6], dark patterns (including greenwashing)[7] or against AI biases[8], enforcers need to 'tool up' to continue to meet their legal obligations. Their intervention is needed more than ever because consumers are in fact made more vulnerable by the very structure of digital markets.[9] Consumers alone are unable to claim their rights, mostly because unfair practices are hard to spot and even harder to evidence. Their covert nature is indeed essential to impair or worse remove consumers' decision-making abilities.

---

[3] Coll L, Riefa C, *Exploring the role of technology in consumer law enforcement* Loyola Consumer Law Review (forthcoming, August 2022).

[4] Although note it is more developed and already more widely adopted in the field of financial services. See for more details, Christine Riefa et al., Cross-border enforcement of consumer law: looking to the future – a report to UNCTAD's working group on e-commerce, sub-working group 3: cross-border enforcement cooperation (forthcoming).

[5] Stefan Hunt, *The technology-led transformation of competition and consumer agencies: the Competition and Markets Authority's experience*, CMA Discussion Paper (14 June 2022) 4-5; note that on the competition law side, embracing technology has moved faster, notably thanks to the work of the Stanford Codex research centre, working on computational antitrust under the leadership of T. Schrepel, see https://law.stanford.edu/codex-the-stanford-center-for-legal-informatics/computational-antitrust/

[6] The study of the design of information and the impact this has on decision making. See on this topic, CMA, Online choice architecture, how digital design can harm competition and consumers (April 2022), https://www.gov.uk/government/publications/online-choice-architecture-how-digital-design-can-harm-competition-and-consumers

[7] In this area, see the work of the UNCTAD working group on e-commerce, [add ref to reports].

[8] See for eg, Sandra Wachter, Brent Mittelstadt, Chris Russell, Bias prevention in machine learning: the legality of fairness metrics under EU non-discrimination law, 3 *West Virginia Law Review* (2021) 123. Also see, https://www.wired.co.uk/article/ai-bias-black-box-sandra-wachter

[9] See notably Micklitz, Helberger et al., (2021) *EU Consumer Protection 2.0: Structural asymmetries in consumer markets* (report for BEUC); also see Riefa, Protecting vulnerable consumers in the digital single market, *European Review of Business Law* Vol. 3, issue 4, August 2022.

As a result, digital markets call for more focus and resources to be placed on public enforcement[10] as a vehicle to keep businesses in check. This is vital to continue to foster trust in electronic commerce.

Fighting the excesses of technology with yet more technology may seem counterintuitive. Still, it now seems inevitable. Technical expertise, the ability to look under the bonnet, so to speak, is vital. Embedding technology in consumer protection enforcement could be well suited to the challenges we are facing. Indeed, in order to police digital markets, it is necessary to be able to analyse a high volume of data at a high speed. It is no longer sustainable to monitor markets through sweeps requiring humans to collect information, when 'scrapping' uses machine learning to plow through much larger volumes of data. It is also necessary to understand how algorithms work and their role in the creation of online choice architecture in order to protect consumers effectively. Technology can also enable the analysis of transactions and complaints data to identify patterns of bad practice as well as gaps in legislation, something that humans would have taken years to do; technology could also help with automatically executing remedies directly to consumers to reverse the current, unsatisfactory enforcement journey that many consumers face.[11]

There are already much technological tools available, servicing the many functions that come within the current remit of consumer enforcement agencies.[12]

---

[10] C Riefa, Coronavirus as a catalyst to transform consumer policy and enforcement 43 (2020) *Journal of Consumer Policy*, 451-461.

[11] See Coll, Riefa (ftn 3). The consumer journey includes: a consumer experiencing a harm, being able to relate it to a specific legal breach, gathering evidence of the harm, bringing it to an alternative dispute resolution system or to a court, or reporting it to a public authority in the hope of action being taken to remedy or prevent it. It is already possible to apply technological tools in an ex-ante enforcement set up by anticipating misconduct.

[12] For a review of the field, see Riefa et al., *Cross border enforcement of consumer law: looking to the future* (forthcoming 2022). For more details on the project see, www.crossborderenforcement.com

They could be adapted to their needs, alongside the development of more specific tools. [13]

As I wish to encourage you to look at developing a technological approach to consumer enforcement, it must come with a warning that while tech solutions look promising, they present some challenges, many of which will require further research.

A key problem resides in the quality of the data required by enforcement authorities as well as the ability for this data to be transferred from one enforcement agency to another.[14] As it stands, there is no standard way of recording and classifying consumer complaints, or scams for example.[15]

Another issue may come with the businesses subject to regulatory scrutiny being inclined to game the system by adapting their behaviour, thus neutralising enforcement efforts.[16]

---

[13] Riefa et al. (ftn 12).

[14] Data set will need to be compatible with each other and able to be communicated effectively within and across jurisdictions. For example, the European Commission is developing a strategy on supervisory data which will involve standardisation and interoperability. European Commission, DG Financial Stability, Financial Services and Capital Markets Union, *Strategy on supervisory data in EU financial service*s (2021), retrieved from: Strategy on supervisory data in EU financial services | European Commission (europa.eu)

[15] A related point to note is that the over reliance on data which reflects existing structures and biases and exacerbates prevalent bias is well-recognised as a risk in AI systems. See The Council of Europe, *Artificial intelligence, human rights, democracy, and the rule of law: a primer* (2021). The same risks are likely to arise in using technology in consumer enforcement, where for example, data on consumer complaints used to develop or train machine learning models may unlikely to represent the experiences of all consumers, particularly those who face particular disadvantages as they tend to underreport.

[16] There has been speculation for example that companies may increase the use of self-destructing encrypted data to make evidence for investigations difficult. See Competition Bureau Canada (2020) Digital Enforcement Summit 2020, retrieved from https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04563.html#panel3; see also Cao, Sean S. and Jiang, Wei and Yang, Baozhong and Zhang, Alan L (2020*), How to Talk When a Machine is Listening: Corporate Disclosure in the Age of AI.* https://dx.doi.org/10.2139/ssrn.3683802 who found that '*growing AI readership…motivates firms to prepare filings that are friendlier to machine parsing and processing. Firms avoid words that are perceived as negative by computational algorithms, as compared to those deemed negative only by dictionaries meant for human readers.*'

There is also a real danger that enforcers, for lack of in-house expertise or driven by economic efficiency, come to rely on already existing commercial technologies and become 'tech users 'rather than 'tech makers'[17], potentially leading to the rather ironic privatisation of public enforcement.

With this in mind, the development of technology-based supervision and enforcement solutions by authorities would require co-ordination and collaboration in ensuring that best practice is not just limited to handful of jurisdictions and to avoid costly duplication of development work[18] something that is supported by Guideline 79 of the United Nations Guidelines for Consumer Protection which encourages member states to cooperate in the implementation of consumer protection policies to achieve greater results within existing resources.

Embracing the use of enforcement technology or Enf Tech[19] for short, seems inevitable. National enforcement agencies are likely to become quickly obsolete if they cannot keep digital markets in check, potentially contributing to diminishing consumer trust and impacting on economic recovery and growth in the process.

---

[17] Goanta, Spanakis, Discussing the legitimacy of digital market surveillance (2022) Stanford Computational Antitrust vol II, 54. Note also that in private enforcement, the privatisation of the process has been highly criticised. ADR has come to largely replace courts in many countries and is not delivering well for consumers.

[18] There is to date very little talk of developing a global approach although the 2019 OECD report is worthy of notice in that it recommended fostering peer learning with regards to the successes and failures of 'SupTech' uses. See OECD (2019), "Using digital technologies to improve the design and enforcement of public policies", OECD Digital Economy Papers, No. 274, OECD Publishing, Paris, https://dx.doi.org/10.1787/99b9ba70-en. Open DOI.; See also, Stefan Hunt, *The technology-led transformation of competition and consumer agencies: the Competition and Markets Authority's experience*, CMA Discussion Paper (14 June 2022).

[19] For more on the subject and its meaning, see Riefa et al., *Cross border enforcement of consumer law: looking to the future* (ftn 2) and Coll, Riefa, *Exploring the role of technology in consumer law enforcement* (forthcoming, Loyola Consumer Law Review, Aug 2022).

With the help of technology, we can look to a future where consumer enforcement authorities are not only able to comfortably enforce consumer laws, keeping up with technological developments in the marketplace, but are also able to move their practice from being reactive to being proactive.[20] Machine learning for example can indeed predict with some great accuracy where laws may be broken or detect trends that can enable authorities as well as policy makers to decide where to focus efforts. It is hoped that the use of Enf Tech can help bypass the more clunky parts of the current system of enforcement and can signal a shift in the way enforcement functions are thought of and executed.[21] Fairness in digital markets should be by design[22] and not something that is offered to consumers simply as an elusive remedy. For this to happen a technological approach to consumer enforcement and policy making seems the way forward.

---

[20] Stefan Hunt, *The technology-led transformation of competition and consumer agencies: the Competition and Markets Authority's experience*, CMA Discussion Paper (14 June 2022).

[21] This trend towards the use of technology in enforcement links well with already established academic work that signalled a clear shift for the approach towards what Willis has coined performance-based consumer law. See Willis, Lauren E., Performance-Based Remedies: Ordering Firms to Eradicate Their Own Fraud. 80 Law and Contemporary Problems 7-41 (2017), Loyola-LA Legal Studies Research Paper No. 2017-26. https://ssrn.com/abstract=3018168 and Willis, Lauren E., Performance-Based Consumer Law. 82 University of Chicago Law Review 1309 (2015), Loyola-LA Legal Studies Paper No. 2014-39, Available at SSRN: https://ssrn.com/abstract=2485667.

[22] Siciliani, Riefa, Gamper, *Consumer Theories of Harm, An economic approach to consumer enforcement and policy making* (Hart 2019).