# The transformative potential of Enforcement Technology (EnfTech) in Consumer Law

Professor Christine Riefa, University of Reading
Liz Coll, Director, Connected Consumers

www.enftech.org

January 2024

Report funded by the UKRI Policy Support Fund, University of Reading

## Contents

# Executive Summary

EnfTech is short for Enforcement Technology. EnfTech has the potential to change the way consumer law is enforced. While enforcement agencies are by and large proactive in their enforcement approach, they are limited in their capacity to act. This necessarily leaves some harm unchecked, meaning that enforcement often appears reactive (with interventions being rolled out after the harm is experienced by consumers) or altogether lacking.

The use of EnfTech in enforcement can boost the efforts of agencies and enhance their capacity to act to the point where enforcement could become proactive with intervention happening before the harm is even experienced. With the right technology in place, enforcement agencies can make important gains. They can streamline their operations and be able to focus their human capital where it is most needed. Swifter discovery of infringement can in the short to medium term contribute to enhancing deterrence leading to significant reductions in infringements in the long term.

The report documents real use cases of technology in consumer enforcement (18 in total) alongside a further inventory of case studies from other disciplines and actors that could be adapted for consumer enforcement (15 use cases, which includes 7 case studies in public authorities' in related fields and 8 case studies from private and other institutional settings).

The report is aimed primarily at newcomers to the field of EnfTech, but agencies at all levels of developments may regard find the findings of use. The research revealed that while the use of technology in consumer law enforcement is still in its infancy, it is, however, developing at a fast pace, in a small, yet significant number of agencies. The set up employed by those consumer agencies varies and there is no 'one size fits all' model to accommodate the roll out of EnfTech. All agencies studied in this report have employed different models (in-house or outsourced or a mix of both), but all have managed to make gains, sometimes with very simple or readily available off-the-shelf technology. EnfTech tools therefore are not reserved to big agencies with sizeable budgets and can be rolled out in all types and sizes of agencies and at every stage of technological development.

The technologies employed by enforcers indeed are varied, although AI has occupied much of the discussions and attention in the most recent past. The report assesses current use cases by reference to the EnfTech Generational framework which charts five successive generations of technology. Generation 1 rests on fairly basic tech, with data collected from paper-based reports or emails and involves heavy manual processing and only performs descriptive tasks. As the use of technology develops and moves through the generations, the input of data becomes automated and the insights gained from this data are increasingly diagnostic (Generation 2) then evolve to rely on full automation and big data and can, at this stage, help with predictive analysis (Generation 3). Advances in technology will, however, make possible the use of tools feeding on big data architectures and offer real-time monitoring with more advanced AI techniques (Generation 4) than the ones that are currently being rolled out. Generation 5 would cover technology that builds on existing generations and moves away from assistive and partial automation of tasks towards fully machine-enabled delivery of decisions.

Our data shows that currently the highest generation of tools used by consumer enforcement agencies and covered in this report is Generation 3. By contrast, use cases in related fields feature tools in Generation 3, 4 and 5 revealing a gap between consumer enforcement practice and practice further afield. The data also points to the acceleration of the use of AI in consumer enforcement and in other areas, although this result needs to be put into context.

For artificial intelligence to lend a hand it needs a lot of good quality data (in particular, structured data). Because of historical set up, most consumer agencies will not yet have all the required data sets and will need to develop strategies to build them and/or acquire them. There may even be a need to mandate by law that private entities respond to demand for data during investigations. In spite of these difficulties, we have seen quick uptake of AI amongst agencies that were already active in EnfTech.

Our study found evidence that AI can be a very useful technology to deploy, but it is not the only one, nor is it always going to be the solution to go-to to solve all enforcement problems. Approaching it therefore requires caution and a lot of learning. However, if deployed correctly, AI shows promise to improve consumer enforcement. In the foreseeable future, human intervention in the deployment of AI will no doubt remain indispensable. However, as technology develops, human time, skills and judgement can progressively be freed up to focus on more intricate (and interesting) parts of the job, while machines can take over the most repetitive and time-consuming tasks.

But to get to this stage requires some management buy-in and resources being deployed to prepare the ground for a technological roll out in agencies. This includes working through a list of problems (some general issues, others very much technology specific). For example, agencies need to grapple with choosing the most appropriate technology to fulfil their needs, and whether outsourcing to privately provided expertise is the best route or if they are able to attract and retain the right level of skills in-house and foster a culture that embraces the change to EnfTech. Agencies will need to reflect on the response companies will have to their upgraded enforcement tools and how they may seek to circumvent detection. On the legal side in particular, one important risk that comes with deployment of EnfTech may be that of the absence of an appropriate legal framework. If AI is the technique of choice, more specific risks await ranging from avoiding the hype and ensuring AI is able to deliver what is needed rather than what is easy to achieve, having the right data to feed it and avoiding any discrimination in the way the system is built and rolled out. While none of the problems that present themselves appear insurmountable, they need to be addressed in order to ensure that the use of technology is a legitimate and worthwhile addition to any consumer law enforcement strategy.

Fast forward a few years, we predict that EnfTech will be making its way into the work of all agencies. How to proceed with EnfTech will depend on pre-existing institutional setups and local regulatory and enforcement cultures. Designing EnfTech in a way that works across borders will be vital for protecting consumers active in today's global, digitalised markets. This requires improved international cooperation in areas like cross-border data flows, shared taxonomies, standardisation, databases structure for recording issues, using shared approaches to turning law into code as well as putting in place the safeguards needed to make sure AI is used in a way that produces robust and interpretable results.

# Acknowledgements

The concept of EnfTech[1] was first developed as part of the cross-border enforcement[2] research project at the University of Reading presented to the UNCTAD working group on consumer protection in e-commerce[3] and the UNCTAD Intergovernmental Group of Experts in 2022.[4]

The EnfTech project is hosted by the University of Reading with funding from UKRI policy support fund. It was formally launched with an event (co-organised with UNCTAD) *Introducing EnfTech: A technological approach to consumer law enforcement*[5] held on 20th April 2023 (https://www.enftech.org/events).

We wish to thank the UNCTAD Secretariat and notably Teresa Moreira and Arnau Izaguerri for their support for this project and co-organisation of this project's launch event. We would also like to acknowledge the speakers at our launch event who shared with us their expertise and experiences of EnfTech as well as challenges for the roll out of such solutions:

- Teresa Moreira, Head of Competition and Consumer Policies, UNCTAD
- Arnau Izaguerri Vila, Legal Officer, Competition and Consumer Policies, UNCTAD
- Margarita Tuch, EU e-Lab at the European Commission, EU
- Luisa Crisigiovanni, CICLE project, Euroconsumers / Altroconsumo, Italy
- Ruth Castelo, Undersecretary for Consumers Affairs, DTI, The Philippines
- Dries Cuijpers, Senior Enforcement Officer, Authority for Consumers and Markets, Netherlands
- Piotr Adamczewski, UOKIK, Office of Competition and Consumer Protection, Poland
- Stacy Procter, Federal Trade Commission, USA
- Professor Dr Martin Ebers, President, Robotics and AI Law Society, Germany
- Steven Kamukama, Manager Consumer Welfare, COMESA Competition Commission
- Sita Zempel, GIZ Project Director, ASEAN
- Johanna Calderon, Legal Director, Proconsumidor, Dominican Republic

[1] The concept of EnfTech was coined by Liz Coll during her research for the report on cross-border enforcement of consumer law, in the chapter focused on technological solutions for cross-border enforcement.

[2] https://www.crossborderenforcement.com/ accessed 11 July 2023.

[3] Christine Riefa and others, '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' (2022) https://unctad.org/system/files/information-document/ccpb_WG_e-commerce_cross-Border_Riefa_en.pdf accessed 11 July 2023.

[4] C Riefa, For a technological approach to consumer law and policy making in the digital age, Keynote, UNCTAD Intergovernmental Group of Expert on Consumer Protection (18 July 2022) https://unctad.org/system/files/non-official-document/ccpb_IGECON2022_present_financial_keynote_riefa_digital_en_0.pdf accessed 11 July 2023.

[5] https://unctad.org/meeting/introducing-enftech-technological-approach-consumer-law-enforcement accessed 11 July 2023.

Our thanks to Laura Aade and Constanta Rosca for their assistance running the event. We also would like to thank a number of people who shared their expertise and insights with us during the research phase of this project:

- Jessie Nghiem, Senior Data Scientist, Energy Safe Victoria, Australia
- Adam Murdoch, Head of Electrical Equipment Safety and Efficiency Energy Safe Victoria, Australia
- Simon Corden, Commissioner, Essential Services Commission, Australia
- Anne-Jel Hoelen, Senior Legal Counsel, Authority for Consumers and Markets, Netherlands
- Jared Wright and Rhea Subramanya, Tony Blair Institute for Global Change, UK
- Jerry Spanakis, Assistant Professor at the Department of Advanced Computing Sciences and at Maastricht Law+Tech Lab, Maastricht University, Netherlands
- Catalina Goanta, Associate Professor in Private Law and Technology, University of Utrecht, Netherlands
- Robin Simpson, Consumer Protection Expert and consultant to the UN.

In addition, this report benefited from the learning at the International Congress on Sanctioning Dosimetry in Consumer Protection organised by the Deputy Superintendent for Consumer Protection (SIC Colombia), (27-28 June 2023). The report also gained insights from the ICPEN 2023 conference in Warsaw (4-6th October 2023) and the United Nations Internet Governance Forum IGF 2023 in Kyoto (8-12 Oct 2023). Particular thanks to Piotr Adamczewski, UOKIK and his team for their invitation to present our research at the events and the opportunity to hear from others.

Thanks to colleagues and stakeholders for their useful comments on the advance copy of this report, including Robin Simpson, Arnau Izaguerri, Simon Corden, Dries Cuijper, Margarita Tuch, Jared Wright, Piotr Adamczewski.

We think of this report as a living document, that will grow with time and as we get to know of other use cases and experiences in consumer agencies. We therefore invite all interested parties to get in touch with comments and suggestions: info@enftech.org to continue to grow our collective knowledge and understanding of the role of technology in consumer enforcement.

# 1. The need for Enforcement Technology (EnfTech) in consumer law

Consumer law was largely developed before the advent of the internet. However, with the expansion of electronic commerce, enforcement frameworks that were developed in the analogue era have become ill-placed to cater for the exponential growth of unfair commercial practices online and changes in market structures and business models (notably those based on the mass collection of data).

Businesses have embraced technology (from cookies to machine learning and AI) to track, predict and influence consumer behaviours and choice whether online or to enhance their face-to-face offerings.[6] The use of technology by businesses in order to shape consumers' decisions is well documented. Starting with the way websites and apps on our devices are designed (sometimes referred to as choice architecture[7]), the journeys that consumers take online are heavily pre-determined. In addition, the growth of global e-commerce means that many unfair practices easily spread across borders.

When suffering detriment, consumers find it increasingly difficult to seek redress and consumer enforcement agencies have struggled to curb wrong doing. Both public and private consumer enforcement are limited in their ability to protect consumers and have been notoriously difficult to achieve.[8] At the private level, the onus is on individual consumers to identify when their rights have been breached and equip themselves with the knowledge, evidence, time and financial resources to quantify and seek redress. For many of the covert practices now occurring online (for example 'dark patterns' or 'deceptive design') this is of course not realistic. Consumers are unable to claim their rights as they may be unaware of the practices they have fallen prey to. Even knowledge and understanding of these practices may not equip them to avoid the practice let alone provide evidence of it in order to seek a remedy.

Public enforcement is also by and large insufficient. Many substantive rules are not adapted to cater for digital unfairness. Besides, according to Hunt: 'the use of massive data sets, complex machine learning and artificial intelligence (AI) algorithms, user experience testing, and a raft of other technologies has caused the information asymmetry between firms and agencies to grow'.[9] In addition, limited resources in enforcement agencies mean only a fraction of problems are prioritised by agencies, leaving many harms unchecked in the marketplace.

[6] Businesses have also developed some tech products to deliver services to consumers that some agencies in regulated industries may have to oversee. See for eg: FinTech. But similar issues may befall generalist consumer agencies, for example with the application of consumer laws to Internet of things. This report is focussed on the use of tech in the enforcement process, not on the supply side.

[7] CMA, Online Choice Architecture, how digital design can harm competition and consumers, discussion paper (2022) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1066524/Online_choice_architecture_discussion_paper.pdf accessed 22 June 2023.

[8] Riefa, Christine, Coronavirus as a Catalyst to Transform Consumer Policy and Enforcement 43 (2020) Journal of Consumer Policy 451-461 https://link.springer.com/article/10.1007/s10603-020-09462-0

[9] Stefan Hunt, The Technology-led transformation of competition and consumer agencies: The Competition and Markets Authority's experience, Discussion Paper (14 June 2022) 4.

This report seeks to explore novel means of combating wrongdoing in digital and other consumer marketplaces.[10]

It explores the need for the use of technology in enforcement and its transformative potential (part 1). The report also introduces some insights into the institutional set up (part 2) necessary for EnfTech to develop, as well as a generational framework to better understand how the use of technology can evolve and be harnessed for enforcement needs (part 3). The report is written primarily for newcomers to the field of EnfTech and is based on desk research, while benefiting from input by professionals on the ground. For this report we have conducted an initial review of the tools used by a variety of agencies, specifically those being applied in the context of consumer law enforcement. This review of EnfTech tools is not exhaustive and has, by practical necessity, been limited by a number of factors which are explored in more detail in part 3.

However, as the first review of its kind in consumer law enforcement, this report adds valuable understanding of current activity and of the different types of technologies in use for particular enforcement tasks or goals. An important added value is the listing and documenting of real use cases of technology in consumer enforcement (part 4) alongside an inventory of case studies from other disciplines and actors that could be adapted for consumer enforcement (part 5 on cross-fertilisation potential). Key challenges to rolling out EnfTech are then explored, featuring a list of problems that might be encountered to help enforcement agencies better navigate their transition to EnfTech (part 6). Part 7 draws our observations together and reflects on next steps.

In this first part we start with defining EnfTech (A) and charting the development of the EnfTech concept (B), before briefly looking at the technologies underpinning enforcement technology (C) and exploring its long-term transformative potential (D).

## A. Defining EnfTech

Consumer enforcement agencies are already familiar with the use of technology. For example, there are multiple examples of ODR (online dispute resolution) platforms or consumer dashboards being used in the EU, Brazil or India.[11] Authorities may run their own complaints' databases or be familiar with those run by some consumer associations. They may also have consulted some online databases detailing the state of legislation or policy in different countries to inform their cross border strategies.[12] Authorities dealing with product safety are

[10] The report focuses primarily on how technology can be used to address digital harms but acknowledges and touches on technology's role in managing more long standing, offline harms for example via managing complaints or licensing etc.

[11] Eg, ODR platform in the EU: https://ec.europa.eu/consumers/odr/main/?event=main.home2.show; in Brazil: https://consumidor.gov.br/pages/principal/?1694255631579 and for more information on ODR in India, see https://unctad.org/system/files/non-official-document/ccpb_IGECON2023_OP_India_en.pdf. Note also the report from UNCTAD, Technology and the future of Online Dispute Resolution (2023) https://unctad.org/system/files/official-document/tcsditcinf2023d5_en.pdf, accessed 2 December 2023.

[12] Note the existence of a number of databases focussed on exchange of information on laws and policies, notably the Consumers International Digital Index (https://www.consumersinternational.org/what-we-do/digital-rights/digital-index/ accessed 18 October 2023) and the UNCTAD World Consumer Protection Map (https://unctad.org/topic/competition-and-consumer-protection/consumer-protection-map accessed 23 October 2023) which can assist with cross-border enforcement efforts.

also familiar with databases used to exchange information on unsafe products as is the case in the UK, the EU or St Kitts and Nevis.[13] By and large however, few generalist consumer agencies around the world have fully harnessed the power of tech or incorporated technology into their daily practice to enable the monitoring and sanctioning of non-compliant behaviours.

By contrast, the use of technology in aid of supervision, regulation (and some aspects of enforcement) or compliance is now well developed in other fields. Indeed, tech-enabled regulation and supervision can be found across many market sectors and is used in public as well as private settings.

Technology is perhaps better known for its application in financial services, where public supervisory authorities make use of it to facilitate and enhance supervisory processes. In this area, 'SupTech'[14] as it is commonly called, has become the de facto standard. SupTech is used to assist with regulatory and supervisory efforts as it would not be practically possible to perform all supervisory tasks relying on human power alone. This field has grown substantially, in part because the financial industry is a regulated industry whereby market players are subject to numerous statutory reporting requirements.

However, private companies also make use of 'regulatory technology' or RegTech[15] to manage their regulatory processes and compliance, including the facilitation of the delivery of regulatory procedures in the regulated sectors and/or to ensure compliance with legal requirements.[16][17] In this sphere detection of wrongdoing on online platforms has developed at pace, notably in the field of intellectual property where it can be used to detect and stop copyright infringements[18]

[13] See for eg in the UK: <https://www.gov.uk/guidance/product-recalls-and-alerts>, in the EU: <https://ec.europa.eu/safety-gate-alerts/screen/webReport> or in St Kitts and Nevis <https://sknbs.org/category/product-recalls/>. Note the existence of an OECD version, the Global Recall Portal, <https://globalrecalls.oecd.org/#/> (all accessed 09 September 2023).

[14] The World Bank defines SupTech as referring to the use of technology to facilitate and enhance supervisory processes from the perspective of supervisory authorities. See, World Bank, 'From Spreadsheets to Suptech Technology Solutions for Market Conduct Supervision', Discussion Note (June 2018) <127577-REVISED-Suptech-Technology-Solutions-for-Market-Conduct-Supervision.pdf> accessed 21 April 2023.

[15] It is widely thought that the first uses of the term RegTech were around 2015 in relation to FinTech, when the UK government and the UK's financial conduct regulator the FCA published strategies and innovation plans for the development of fintech, and related regulatory processes "technologies that may facilitate the delivery of regulatory requirements more efficiently and effectively than existing capabilities.". See: FCA, Call for input on supporting the development and adopters of RegTech (2016) <https://www.fca.org.uk/publication/feedback/fs-16-04.pdf> accessed 21 April 2023; UK Government Office for Science 'FinTech Futures The UK as a World Leader in Financial Technologies' A report by the UK Government Chief Scientific Adviser (2015) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/413095/gs-15-3-fintech-futures.pdf> accessed 21 April 2023.

[16] Note the potential for consumers to make direct use of the same information and analysis available through SupTech and RegTech applications. Making assessments of compliance or non-compliance with consumer law for various different services available to consumers choosing apps or services or transacting with companies could be widely rolled out to consumers individually or used by consumer associations. In this sense, what is now called RegTech could be better framed as Compliance Tech. For more on the ability of tech to assist consumers, see Giuseppe Contissa and others, 'Towards Consumer-Empowering Artificial Intelligence', Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence (International Joint Conferences on Artificial Intelligence Organization 2018) 5151 <https://www.ijcai.org/proceedings/2018/714> accessed 09 September 2023.

[17] In some cases, the term RegTech is used as a catch-all term for technology used by the private sector and public regulators to support compliance, for example: the World Economic Forum's article 'What is RegTech and what does it mean for policymakers?, 21 June 2022 <https://www.weforum.org/agenda/2022/06/what-is-regtech-and-what-does-it-mean-for-policymakers/> accessed 13 December 2023

[18] Perel, M and Elkin-Koren, N (2016) Accountability in Algorithmic Copyright enforcement. Stanford Technology Law Review 473 http://dx.doi.org/10.2139/ssrn.2607910

as well as to assist in the detection and removal of unsafe products sold via the intermediary of online platforms.[19] Banks have also been long-standing users of similar technology to enable detection of credit card fraud.[20]

LegalTech uses technologies that enhance analysis and application of law and is used by lawyers in private firms for example, for analysing documents during disclosure.[21] In this field, and despite some obvious problems and errors that can creep up, the technology has been found to enable efficiency gains and improvements in quality when compared with manual work.[22]

Some variations and overlap exist between these uses for technology in the field of regulation and compliance. For example, in the field of competition law, the CodeX Center for legal informatics at the University of Stanford hosts the Computational Antitrust project which explores how legal informatics (the academic discipline underlying the technological transformation and economics of the legal industry[23]) could 'foster the automation of antitrust procedures and the improvement of antitrust analysis'.[24]

Legal informatics is linked to Legal Tech in that it developed out of a need to manage volumes of information that could no longer be solely managed by manual review.[25] Computational antitrust is anchored in the study of computational law (or CompLaw) which is concerned with the mechanisation of legal reasoning. This area is itself connected to RegTech in that, while there are multiple applications of CompLaw, the main focus is on compliance management: 'the development and deployment of computer systems capable of assessing, facilitating or enforcing compliance with rules and regulations'.[26]

The table below maps the typology of the use of technology in regulatory, compliance and enforcement as well as in what sphere they are predominantly deployed. Those technologies tend to be defined by the technology user but can also be defined by the types of tasks that the technology performs (as is the case for EnfTech).

[19] Ibid.

[20] Ibid.

[21] For more on legal tech see for eg, Martin Ebers, 'Legal Tech and EU Consumer Law' in Larry A DiMatteo and others (eds), The Cambridge Handbook of Lawyering in the Digital Age (1st edn, Cambridge University Press 2021) <https://www.cambridge.org/core/product/identifier/9781108936040%23CN-bp-11/type/book_part> accessed 22 March 2023.

[22] Ron Dolin, Legal Informatics, Taking the tediousness out of law (2021) The Practice <https://clp.law.harvard.edu/knowledge-hub/magazine/issues/legal-informatics/legal-informatics/> accessed 26 June 2023.

[23] https://clp.law.harvard.edu/knowledge-hub/magazine/issues/legal-informatics/legal-informatics/ accessed 26 June 2023.

[24] https://law.stanford.edu/codex-the-stanford-center-for-legal-informatics/computational-antitrust/ accessed 26 June 2023.

[25] https://clp.law.harvard.edu/knowledge-hub/magazine/issues/legal-informatics/legal-informatics/ accessed 26 June 2023.

[26] https://law.stanford.edu/2021/03/10/what-is-computational-law/ accessed 26 June 2023.

*Figure 1: The use of technology in regulatory compliance and enforcement*

| Sphere in which deployed | Name | Role of Technologies | Main users |
|---|---|---|---|
| **Private** | **LegalTech** | To enhance analysis and application of law | Lawyers, law firms |
| | **RegTech** | To facilitate delivery of regulatory procedures and legal requirements | Regulated companies |
| **Public** | **SupTech** | To facilitate and enhance supervisory processes | Supervisory authorities |
| | **Computational Anti-trust** | To assess compliance with legal rules | Competition authorities |
| | **EnfTech** | To facilitate a range of enforcement needs | Enforcement agencies, **plus** enforcement functions of other authorities |

Looking at the way technology can be deployed to service consumer enforcement agencies requires acknowledging specific needs, amid some overlap with other fields. Copy and pasting solutions developed in Legal Tech, RegTech, SupTech or even computational antitrust may not yield the best results in consumer enforcement tasks. While many processes can be duplicated across the tasks that those different actors such as supervisory authorities, private entities reporting on regulatory requirements, or law firms in discovery of evidence at trial have to perform, they can often focus on different end goals. For example, tools currently in use focus on detection and identification whereas enforcement agencies, while needing to detect, also need to be ready to sanction wrongdoing.

Besides, any of the tools currently in use focus on detection and identification whereas enforcement agencies, while needing to detect, also need to be ready to sanction wrongdoing.

Thus, to avoid shoehorning the use of tech in consumer law enforcement into pre-existing categories this report focuses instead on ‘Enforcement technology’ or ‘EnfTech’ to describe the use of technology by enforcement agencies, carving out a more specialised field (although not limited to consumer enforcement).

## B. Development of the EnfTech concept

The concept of EnfTech[27] was first developed as part of the cross-border enforcement[28] research project at the University of Reading presented to the UNCTAD working group on consumer protection in e-commerce[29] and the UNCTAD Intergovernmental Group of Experts in 2022.[30] The EnfTech project is hosted by the University of Reading with funding from UKRI policy support fund. It was formally launched with an event (co-organised with UNCTAD) in 2023, *Introducing EnfTech: A technological approach to consumer law enforcement*[31] held on 20th April 2023.

EnfTech, as a concept, describes a set of tech tools (which may rest on a wide range of technologies described in Annex 1) that assists in enforcement-specific tasks (i.e. what enforcers need to do, including detect wrong-doing, carry out investigations, monitor behaviours, order sanctions). EnfTech also describes the tools necessary to assist in implementing the direct execution of an enforcement action (such as a warning, takedown or a fine). In time, as technology develops, this latter meaning will potentially become more prominent. At today's date however, EnfTech more accurately describes the set of tools that service the needs of consumer enforcement agencies. In this report, however, we illustrate how the evolution of technology can lead to EnfTech being a practical and effective tool to directly enforce and even prevent harm from occurring.

## C. Technology underpinning EnfTech

Technology is now increasingly capable of attending to enforcement needs. But it can only be usefully rolled out if the right technology is selected to perform what so far remain discrete enforcement tasks.

At the heart of a successful transformation of consumer law enforcement is the question of how best to harness the technology available to serve consumers. Artificial Intelligence (AI) is now monopolising much of the discussions on technology and enforcement. While potentially very useful, the family of AI technologies may not always be best placed to deliver results - this will depend on the task, data available and resources. We have however, found use of AI in more

[27] The concept of EnfTech was coined by Liz Coll during her research for the report on cross-border enforcement of consumer law, in the chapter focused on technological solutions for cross-border enforcement.

[28] https://www.crossborderenforcement.com/ accessed 11 July 2023.

[29] Christine Riefa and others, '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' (2022) https://unctad.org/system/files/information-document/ccpb_WG_e-commerce_cross-Border_Riefa_en.pdf accessed 11 July 2023.

[30] C Riefa, For a technological approach to consumer law and policy making in the digital age, Keynote, UNCTAD Intergovernmental Group of Expert on Consumer Protection (18 July 2022) https://unctad.org/system/files/non-official-document/ccpb_IGECON2022_present_financial_keynote_riefa_digital_en_0.pdf accessed 11 July 2023.

[31] https://unctad.org/meeting/introducing-enftech-technological-approach-consumer-law-enforcement accessed 11 July 2023.

discreet tasks[32] largely to assist the work of enforcement agency staff notably to detect wrongdoing, for example identifying unfair terms or flagging fake price reductions online.

EnfTech is much broader than AI, encompassing many types of technologies able to service the work of enforcement agencies. Annex 1 gives a summary of the different technologies that can be used in the rollout of EnfTech tools for readers unfamiliar with this aspect.

## D. Transformative potential of EnfTech

The deployment of unfair practices online (such as dark patterns[33], or misleading influencer marketing on social media[34]) alongside the soaring sale of unsafe products on online platforms[35] exposes the limitations of consumer enforcement agencies. Agencies face many of the same challenges faced by consumers. Indeed, few currently have the technical capacity to detect wrongdoing at a scale matching that of industry targeting consumers, even if they have good internal knowledge of the technology deployed to cause harm to consumers. This leads to under-enforcement and may, in time, lead to the lack of credible deterrence and effective sanctioning of harm now prevalent in consumer markets.[36]

There is therefore a need to tool up[37], to equip consumer agencies with the means to provide effective controls of consumer markets as well as maintain consumer trust. Indeed, the use of EnfTech, as documented in this report, can greatly assist in enforcement efforts, leading to cost efficiencies and maximising the value of staff time. It can assist to reach better diagnosis of problems in consumer markets and can enable agencies to cope with high rates of change as well as stress test their interventions.[38]

Perhaps more importantly, it can also enable agencies to prevent their obsolescence. In a fast-moving technological landscape where unfair commercial practices are ripe and often hard to detect, delaying the modernisation of processes in enforcement may mean agencies lose their grit and relevance. EnfTech can also assist in the response to cross-border, industry-dominated digital consumer markets because of its ability to detect wrongdoing beyond the confine of

[32] Note that AI can also be used in combination with other strands of technology or processes such as robotics, IoT or even Blockchain but we have seen no evidence of this in practice yet. See C Riefa, L Coll, The use of AI in the enforcement of Technology (EnfTech) toolbox: is AI a friend or a foe? In Larry Di Matteo, Cristina Poncibo, Geraint Howells, *AI and Consumers* (Cambridge University Press, forthcoming 2024).

[33] To get a sense of scale and enforcement limitations, see Arunesh Mathur and others, 'Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites' (2019) 3 Proceedings of the ACM on Human-Computer Interaction 1; Constanta Rosca and others, 'Defence Against the (Digital) Dark Arts: Defining, Detecting and Measuring Unlawful Dark Patterns in the EU' (2021).

[34] See for example Frithjof Michaelsen and others, 'The Impact of Influencers on Advertising and Consumer Protection in the Single Market' (IMCO European Parliament 2022).

[35] 'Unsafe Products Exact a High Price on Consumers Globally | UNCTAD' (19 July 2022) <https://unctad.org/news/unsafe-products-exact-high-price-consumers-globally> accessed 21 April 2023.

[36] C Riefa, L Coll, The use of AI in the Enforcement Technology (EnfTech) toolbox: is AI a friend or a foe? in Larry Di Matteo, Cristina Poncibo, Geraint Howells, *AI and Consumers* (Cambridge University Press, forthcoming 2024).

[37] Christine Riefa, 'For a Technological Approach to Consumer Law Enforcement and Policy Making in the Digital Age, Keynote Address to UNCTAD's Sixth Intergovernmental Group of Experts on Consumer Law and Policy' (2022).

[38] Bill Kovacic, Professor of Law and Policy, George Washington at CMA Data, Technology and ANalytics Conference, June 2022 https://www.youtube.com/watch?v=q6cJ43v3AcY&list=PLJREEEp2I-xckXWl5O-_BELnqA0tf1bu-&index=4 accessed 27 September 2023.

national geographical borders as well as help compute solutions that are already common, but may have escaped the knowledge of a small pool of individuals in an agency or set of agencies.

Above all, EnfTech has transformative potential.[39] It can transform consumer enforcement which is *de facto* largely reactive and comes after the harm has occurred, into a more proactive exercise. It can help improve consumer protection by moving enforcement from ex-post to ex-ante, helping to prevent harm from occurring in the first place.

A useful analogy is to think of the enforcement agency as a 'driving instructor' in the backseat, a non-punitive agent who would alert a novice driver if they are about to break a traffic law and advise an alternative action.[40] To anticipate contraventions to consumer law, a punitive version of this could involve an agent with the power to immediately alert the authorities of violations when the 'driver' ignores the advice (albeit with the same rights to reply as currently enjoyed by an alleged perpetrator). In the business field, this is a job many RegTech applications already perform, altering prior to action where rules might be broken. We might easily then imagine the 'computerised police enforcer' able to notify authorities or consumers directly that a law has been broken and enabling the next stage of enforcement or redress. This might be automating an immediate refund to consumers or initiating a change to service terms and practice.

The move to the use of tech in consumer law enforcement could thus signal a shift in the way enforcement functions are thought about and executed.[41] Tech can be a game changer. It can make consumer law enforcement stronger than it has ever been, thus going some way to addressing the lack of incentives to stick to the law which impacts on competition. It will give consumer law enforcement the visibility it needs to instil confidence in consumers that bad behaviours will no longer be part of doing business and that they can expect better treatment.

This trend towards the use of technology in enforcement complements already established academic work that advocates for a shift in approach in consumer enforcement[42] towards one where fairness is expected by design.[43] A shift to automatic sanctioning of non-compliant behaviour will enable enforcers to ensure consumer markets work more optimally for consumers and competitors alike. The tools required to help make this shift happen are

[39] What Hunt termed the 'technology led transformation of competition and consumer agencies'. See Stefan Hunt, 'The Technology-Led Transformation of Competition and Consumer Agencies' (2022). Note also the Stanford project in the field of competition law 'computational antitrust' which gathers 65 antitrust agencies and explores 'how legal informatics could foster the automation of antitrust procedures and the improvement of antitrust analysis', <https://law.stanford.edu/codex-the-stanford-center-for-legal-informatics/computational-antitrust/> accessed 12 September 2023.

[40] See Genesereth, M 'Computational Law: The Cop in the Backseat', CodeX: The Center for Legal Informatics Stanford University (200) http://complaw.stanford.edu/readings/complaw.pdf <accessed 12 October 2023>

[41] C Riefa, L Coll, The use of AI in the Enforcement Technology (EnfTech) toolbox: is AI a friend or a foe? in Larry Di Matteo, Cristina Poncibo, Geraint Howells, *AI and Consumers* (Cambridge University Press, forthcoming 2024).

[42] See for eg, 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; 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; see also Siciliani, P, Riefa, C, & Gamper, H. (2019). Consumer Theories of Harm: An Economic Approach to Consumer Law Enforcement and Policy Making.

[43] Siciliani, P, Riefa, C, & Gamper, H. (2019). Consumer Theories of Harm: An Economic Approach to Consumer Law Enforcement and Policy Making.

explored in more detail throughout this report, in particular part 3, section B.ii 'The transformative potential of a fifth EnfTech generation'.

# 2. Institutional framework for the deployment of EnfTech in agencies

Rolling out EnfTech effectively will require some structural changes or adjustments. It may need to fit into existing structures and or be the object of the creation of new functions or departments. The structure of consumer enforcement at the time of writing varies widely across the world and there is no 'one size fits all model' employed by enforcement agencies to dispense their traditional tasks.[44] Equally, our research found that there is no single mode when it comes to structuring the deployment of technology in enforcement agencies. This part charts the developments of relevant infrastructures at national (A) as well as international level (B). All deployment to date seems to have occurred incrementally and remains limited to a small number of agencies. The annex to this report contains some details of the institutional set up adopted by a sample of agencies that were selected because they were recognised in early and/or connected literature as leading the field.[45]

## A. Institutional models at national level

We have found two main institutional models: (i) in-house expertise and (ii) outsourcing of technical expertise although the latter is rarer. However, agencies by and large use a mix of in-house and outsourcing by default, in that some in-house teams may be using third party software alongside their own proprietary tools to help them in their enforcement efforts.

### i. In-house technological expertise

For those agencies that have chosen to bring technological expertise in-house, they have done so in a variety of ways. Some teams started out ad hoc, housed in specialised units. For example, at the US Federal Trade Commission (FTC), OTECH sat in the Consumer Protection Bureau before being centralised with its competition counterpart (and other units) to form the Office of Technology. By contrast, at the Competition & Markets Authority (CMA) in the UK, technologists started out in the same unit as economists, where they remain, although the team has now been consolidated into a DaTA unit. Possible advantages of proceeding with the creation of specialised units are that it reduces some overheads and ensures that oversight of tasks is provided by a person who has the relevant technical expertise. At present, the size of the tech teams are relatively small, but as tech use in enforcement develops, they are uniquely

[44] Christine Riefa and others, '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' (2022) 21, part 2, para 2 https://unctad.org/system/files/information-document/ccpb_WG_e-commerce_cross-Border_Riefa_en.pdf accessed 11 July 2023.

[45] Most notably, the agencies were selected because they feature in 2 key pre-existing sources: Stefan Hunt, The technology led transformation of competition and consumer agencies: The CMA's experience, discussion paper (14 June 2022) and Stephanie Nguyen, A Century of Technological Evolution at the Federal Trade Commission (https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/02/century-technological-evolution-federal-trade-commission accessed 3 July 2023).

placed to be growing in capacity and indeed, the FTC and CMA have been actively recruiting in recent years.

### ii. Outsourcing of technological expertise

Another way to harness technology, even in the absence of in-house expertise, is to outsource the development of the tools. In Poland for example, the Office of Competition and Consumer Protection (UOKIK) used an open challenge process[46] to choose the provider that developed their ARBUZ tool. This is not a traditional tendering process and it is not common for public bodies to make use of it. This method can enable a relatively quick deployment of tools without having to increase the authority's headcount and thus long term overheads. It can also help bypass some staff recruitment hurdles. At least initially, it can be a good way to test out the potential for the use of technology without making staff investments and also increase staff awareness and buy-in for tech tools without disrupting teams' operations. The Open Challenge bidding process used by the UOKIK, as we understand it, is not a straightforward tendering process. It is designed to stimulate innovation and tap into the best expertise available, leading to selecting the best contractor on the basis of their real competences rather than experience of market position.[47] The authority is planning to use the same process for the development of their second tool concerning AI detection of dark patterns).[48]

However, outsourcing does require a level of commitment, funds and some expertise to ensure the product developed is up to the task, and thus it is by no means an easier way to develop the use of technology in agencies.[49] It will still require at least a small number of staff who, while not technologists themselves, will be able to interface successfully with providers to ensure that the best product is developed. External providers are unlikely to have consumer enforcement knowledge and will therefore depend heavily on staff to communicate needs in developing their technical product.

To overcome this, collaborative efforts between private and public sector actors to develop and deploy EnfTech tools could be an option, via a process known as 'pre-commercial procurement'[50]. This process is comparable to a blend of research and development and procurement, in that it involves using external, mostly private sector expertise to work directly with public sector stakeholders to better understand current challenges of agencies and

[46] Polish Public Procurement Law defines a competition as a public promise, in which the contracting authority promises a prize for the performance and transfer of the right to a competition work selected by the competition jury through a public announcement. The author/authors of selected competition entries may receive financial or material prizes, or they may be invited to negotiate a contract on a single-source basis.

[47] Conversation around public tech procurement practices with Jared Wright, Senior Policy Analyst, Tony Blair Institute for Global Change, June 2023.

[48] Briefing on 'Detecting and combating dark patterns with Artificial Intelligence' EU-Funded project May 2023 - April 2026 UOKIK Project 101102223.

[49] For some useful advice (although much is UK specific) see HM Government, The Digital, Data and Technology Playbook (June 2023) https://www.gov.uk/government/publications/the-digital-data-and-technology-playbook/the-digital-data-and-technology-playbook accessed 30 June 2023.

[50] Pre-commercial procurement is described by the European Commission as a process that enables public procurers to compare alternative potential digital solution approaches from the private sector, and filter which are most appropriate to address the public need. https://digital-strategy.ec.europa.eu/en/policies/pre-commercial-procurement accessed 27 November 2023.

developing novel solutions to address it. It is a useful approach for crafting appropriate solutions to niche or complex problems involving multiple stakeholders.

Several agencies have also been making use of third-party software irrespective of having technical staff and the relevant expertise in house. For example in Australia, the Scamwatch team at the Competition and Consumer Commission (ACCC) has used Netcraft to combat scams.[51] The EU eLab also uses a mix of open source and commercial products to aid enforcement and is now moving into developing its own bespoke tools.[52] In Colombia, the Oficina de Tecnologia e Informática (OTI) hosted withn the Superintendencia de Industria y Commercio (SIC) uses some externally sourced forensic tools and has also developed some in-house tools, notably for data searches in competition law interventions[53] and to assist with the imposition of consumer law sanctions.

### iii. Single v dual remit agency use of technological expertise

Our research spanned both single remit (only dealing with consumer law) and dual-remit agencies (charged with competition and consumer law enforcement or another combination of areas). Agencies with dual remits may be ideally placed to make use of cross-fertilisation and accelerate the pace of deployment of EnfTech capitalising on the advances already made in competition law. For example, the agencies below have now deployed tools in the field of both competition and consumer law enforcement: FTC (USA)*[54], CMA (UK)*, ACM (Netherlands)*, ACCC (Australia)*, SIC (Colombia)*. All have already developed many initiatives harnessing technology in both fields.

Many dual agencies are also involved in initiatives in the field of competition law, notably the Computational Antitrust project at the Codex Centre of the University of Stanford (USA), which lists named representatives circulating information, attending workshops and contributing to the annual report from 65 competition agencies around the world.[55] Of those 65 agencies, 21% have a clear dual remit and are also responsible for consumer law enforcement (14 agencies) and an additional two agencies have some discreet consumer enforcement powers although they mostly focus on competition.[56] As the CodeX project develops, the agencies involved will have acquired important knowledge that can be of benefit to their consumer law teams.

[51] https://www.scamwatch.gov.au/system/files/Targeting%20scams%20report%202022.pdf 8, accessed 29 June 2023. https://www.netcraft.com/ which provides cybercrime disruption services and notifies web hosts of irregular content/ and websites being hosted, relying on them exercising their contractual rights (contained in terms of service) to shut down fraudulent websites. This is an interesting dimension in that it does not rely on regulatory powers but instead on contract law to get results and yet in this example, its operation was commissioned by a public enforcement agency.

[52] Margarita Tuch, presentation "EU eLab: digital solutions for consumer protection" at 'Introducing EnfTech: a technological approach to consumer law enforcement 20 April 2023' by Margarita Tuch, Legal and Policy Officer, DG JUST, Consumer Enforcement and Redress, European Commission

[53] OECD, Latin American and Caribbean Competition Forum 2020: Digital Evidence Gathering in Cartel Investigations - Contribution from Colombia (DF/COMP/LACF (2020) 8) 5, para 13 https://one.oecd.org/document/DAF/COMP/LACF(2020)8/en/pdf accessed 30 June 2023.

[54] The * denotes an enforcement authority part of the CODEX project regarding Computational antitrust.

[55] For an up-to-date list of agencies, see <https://law.stanford.edu/codex-the-stanford-center-for-legal-informatics/computational-antitrust-agencie> accessed 12 October 2023.

[56] This is for example the case of Japan and Curacao.

There is already some evidence that dual remit agencies might have fared better so far, as a result of synergy between agencies with dual remit involved in the Computational Antitrust project and those who are active with the deployment of EnfTech in consumer protection featured in this present report.

Single remit agencies, especially if small and not already well resourced, may have a harder task in rolling out technology because they may have more limited opportunities for cross-fertilisation. They will thus need to be engaged in networking and learning from other agencies in order to strengthen their effectiveness in EnfTech adoption. Single remit agencies can make important gains by making investments and/or grouping resources together with other agencies, either in other fields at national level[57] and/or with other consumer enforcement agencies across borders.

For example, In the EU, the EU eLab[58] assists the consumer enforcement agencies of all member states.

> *The eLab is a "digital toolbox" which has been live since 2022 for national consumer authorities who want to conduct online investigations into mass scale breaches of EU consumer law.[59] It was developed within the Consumer Protection Cooperation network (or CPC), a network of member states' public consumer protection enforcers brought together to tackle cross-border issues. The eLab provides national authorities with access to a mix of tools from simple VPNs to avoid detection when investigating sites, to bespoke solutions.*

SIC, the Colombian authority, has also offered assistance and access to expertise for countries interested in emulating their sanction tool, thus contributing to processes of collaboration and information exchange taking shape.

## B. Adoption at international level

At international level, the International Consumer Protection Enforcement Network (ICPEN) has been versed in running common sweeps for many years. Members are now discussing use of more sophisticated technology at recent meetings. The Polish Presidency of ICPEN in 2023 is well placed to support those discussions as the Polish enforcement authority UOKIK has recently started to use AI in enforcement.[60] Notably, the Presidency held the 2023 ICPEN conference in Warsaw, including a panel on AI and consumer protection showcasing some examples of EnfTech in action. ICPEN members have agreed to further common work.

[57] Note for example, the Digital Regulation Cooperation Forum in the UK or the joint work in the Netherlands between the Dutch Data Protection Authority, the Authority for Financial Markets and the Media Authority.

[58] Margarita Tuch (European Commission), EU eLab: digital solutions for consumer protection, conference presentation at 'Introducing EnfTech: a technological approach to consumer law enforcement (20 April 2023) https://www.enftech.org/s/DG-JUST-eLab.pdf> accessed 26 April 2023.

[59] Consumer Protection Cooperation Network (CPC), Single Market Scoreboard, https://single-market-scoreboard.ec.europa.eu/governance-tools/consumer-protection-cooperation-network-cpc_en accessed 30 May 2023.

[60] https://icpen.org/ accessed 11 July 2023.

At UNCTAD, EnfTech has been discussed since 2022. The keynote address for the annual meeting of the UNCTAD Intergovernmental Group of Experts on Consumer Protection (IGE) 2022 delivered by Prof. Christine Riefa was entitled 'For a technological approach to consumer law enforcement and policy making in the Digital Age'.[61] The EnfTech project, directed by Christine Riefa and Liz Coll (authors of this report) was launched in 2023, with a joint event with the UNCTAD Consumer Policy Branch Secretariat and interim results were presented at the 14th Research Partnership Platform in July 2023.[62] The Working Group on consumer protection in e-commerce at UNCTAD also expressed an interest in exchanging information and following the progress of the EnfTech project as awareness of the potential of technology and expertise in agencies develop. The work programme of this working group for 2023-2024 will feature the use of AI in consumer protection. In many respects, the present report will support dissemination and best practice exchanges. UOKIK has also organised panels at both the UN Internet Governance Forum since 2021 discussing the use of AI in consumer enforcement[63] and is preparing a white paper for use of AI in consumer enforcement for 2024. In addition, in its report on Technology and the Future of Online Dispute Resolution (ODR) - platforms for consumer protection agencies, UNCTAD acknowledged the promise of technology in enhancing dispute resolution in e-commerce and reflected on the way forward.[64]

The OECD has also been giving thoughts to the use of technology, and, notably paired up with the computational anti-trust project in the release of their 2022 report. The OECD has also been involved with the UN IGF 2023[65] and is working on several initiatives of relevance to consumer law enforcement. Particularly noteworthy are an AI observatory[66] and a project on the consistency of terminology and understanding of the risks posed by AI, the AI Incidents Monitor (AIM).[67] This is particularly relevant as there is a lack of common language and response where AI problems pose risk to consumers. The AIM project is currently experimenting with the use of AI to categorise with neuro linguistic programming or NLP the data collected online about AI incidents (from reputable news channels). The OECD is also looking more specifically into the

[61] First in the report, Christine Riefa and others, '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' (2022) https://unctad.org/system/files/information-document/ccpb_WG_e-commerce_cross-Border_Riefa_en.pdf accessed 11 July 2023; and C Riefa, For a technological approach to consumer law and policy making in the digital age, Keynote, UNCTAD Intergovernmental Group of Expert on Consumer Protection (18 July 2022) https://unctad.org/system/files/non-official-document/ccpb_IGECON2022_present_financial_keynote_riefa_digital_en_0.pdf accessed 11 July 2023.

[62] Launch event: *Introducing EnfTech: A technological approach to consumer law enforcement* held online on 20th April 2023, www.enftech.org and https://unctad.org/meeting/introducing-enftech-technological-approach-consumer-law-enforcement, both accessed 11 July 2023. Interim report presentation: Liz Coll, Christine Riefa, EnfTech: the transformative potential of technology in consumer law enforcement, presentation at the fourteenth meeting of UNCTAD's research partnership platform (5 July 2023) https://unctad.org/meeting/fourteenth-meeting-unctad-research-partnership-platform, slides available here: https://unctad.org/system/files/non-official-document/ccpb_RPP_pres_Riefa_ppts_en.pdf, accessed 1 december 2023.

[63] Session #82 AI Technology - a source of empowerment in consumer protection, https://www.intgovforum.org/en/content/igf-2023-open-forum-82-ai-technology-a-source-of-empowerment-in-consumer-protection accessed 23 October 2023.

[64] UNCTAD (2023) https://unctad.org/system/files/official-document/tcsditcinf2023d5_en.pdf, accessed 1 December 2023.

[65] See ftn 61.

[66] See full details, https://oecd.ai/en/ accessed 23 October 2023.

[67] https://oecd.ai/en/incidents-methodology accessed 23 October 2023.

use of AI by members’ consumer authorities (but has not yet published on this specialised issue).

# 3. The EnfTech Generational Framework

Our review of technology use cases in consumer law enforcement (in part 4) shows disparities between the types and level of sophistication of technologies used by agencies in their enforcement efforts. Such disparities are often explained by divergence in the legal frameworks which underpin the existence of the enforcement agencies as well as their pre-existing institutional and/or technical capacity (explored in part 2).

Disparities are also explained by the fact that technologies may not all need to be at the same level of sophistication or maturity to yield good results. Some somewhat simple tools may be deployed to good effect for enforcement tasks, while other tasks may require the deployment of AI tools or Big Data infrastructure (or other equally sophisticated resources). In this part of the report, we seek to provide a methodology for unpicking the technological maturity of EnfTech tools. This methodology is what is referred to as the EnfTech generational framework. The EnfTech generational framework is based on Di Castri's work from 2019[68] in relation to supervisory technology. Di Castri introduced a typology of generations of technologies that are used for analysis and insight in financial supervisory technology, taking as an initial starting point the way in which regulatory data is made available.

The rationale for wanting to organise technical maturity in generations includes assisting enforcement agencies in:

- Understanding where each tool may sit and what technological infrastructure they may require;
- Making sense of a fast developing landscape of useful technologies;
- Mapping out the route and milestones necessary to improve an enforcement agency's technical capacity;
- Making identification of peer institutions and those institutions working with tools at a higher level of sophistication easier and thus facilitating exchange of best practices and learning at all levels of advancement.

In addition, the EnfTech generational framework enables an inclusive approach, recognising that between regions and countries there are vastly varying levels of ICT capacity, investment and spend amongst consumer authorities. Therefore, classifying the generations in use shows where technology can have value regardless of the resource and technological maturity of the authority.

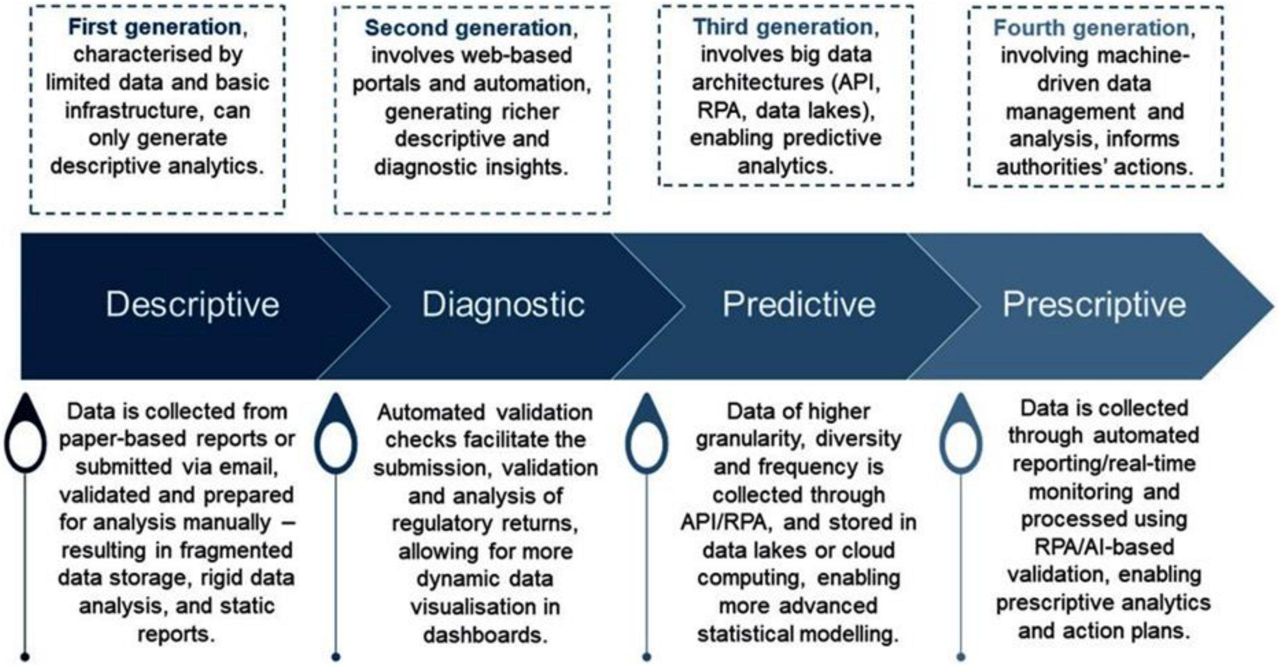
In this part of the report we first review Di Castri's model of generations of technology (A) before describing the adaptations necessary to use the model in relation to EnfTech (B) and our methodology for situating the EnfTech case studies contained in part 4 in the generational framework (C).

[68] Simone di Castri and others, 'The Suptech Generations' [2019] SSRN Electronic Journal <https://www.ssrn.com/abstract=4232667> accessed 27 September 2023.

## A. Di Castri's Generations of technology for analysis and insight

Di Castri's typology[69] is made out of four parts that look at the different stages of technological maturity, taking as its starting point the availability, format and channel of data available to an authority. The four generations cover a continuum of data analytic capabilities: descriptive, diagnostic, predictive and prescriptive.

*Figure 2: The SupTech Generations*


First generation, characterised by limited data and basic infrastructure, can only generate descriptive analytics.
Second generation, involves web-based portals and automation, generating richer descriptive and diagnostic insights.
Third generation, involves big data architectures (API, RPA, data lakes), enabling predictive analytics.
Fourth generation, involving machine-driven data management and analysis, informs authorities' actions.
Descriptive
Diagnostic
Predictive
Prescriptive
Data is collected from paper-based reports or submitted via email, validated and prepared for analysis manually – resulting in fragmented data storage, rigid data analysis, and static reports.
Automated validation checks facilitate the submission, validation and analysis of regulatory returns, allowing for more dynamic data visualisation in dashboards.
Data of higher granularity, diversity and frequency is collected through API/RPA, and stored in data lakes or cloud computing, enabling more advanced statistical modelling.
Data is collected through automated reporting/real-time monitoring and processed using RPA/AI-based validation, enabling prescriptive analytics and action plans.

**Source**: Simone di Castri and others, 'The Suptech Generations', 2019. *API and RPA and other technical acronyms are defined in Annex 1 of this report.

The first generation covers data sources and tools that can provide descriptive capabilities. The descriptive tools will be characterised by limited data and basic infrastructures and will only deliver descriptive analytics. The data may be collected from paper-based reports or emails and involve heavy manual processing.

Second generation tools (performing a diagnostic function) will involve web-based portals and some automated process for pulling in data or receiving it from entities who 'push' data to the portal.[70] In this generation, richer diagnostic insights (in terms of not just describing what is happening but why it is) are available and which can be visualised in more accessible and engaging ways through, for example, data dashboards.

[69] Simone di Castri and others, 'The Suptech Generations' [2019] SSRN Electronic Journal <https://www.ssrn.com/abstract=4232667> accessed 27 September 2023.

[70] See under heading 'Automated data reporting' in Annex 1 'Technologies and data: terms in use' for more detail.

The third generation involves the use of big data architectures and full automation, for example through receiving automated reports via APIs[71]. Big data refers to data sets that are simply too large to be managed by a human or by simple computing technology.[72] In this generation, descriptive, diagnostic and predictive functions become possible.

The fourth generation involves big data architecture with the addition of AI- enabled data analysis which enhances automated reporting to the extent that it may become possible to monitor data in real time. By layering more advanced AI technologies on top of the big data sets, tools are able to develop their own way of learning about patterns, enabling it to predict what will happen to a much more detailed level, and potentially prescribe anticipatory action. This fourth generation is a significant shift as it is the first indication we have of a move away from assistive and partial automation of tasks towards fully machine-enabled delivery of decisions.

Di Castri's classification is based on the deployment of supervisory technology (SupTech), not on the use of enforcement technology in a consumer law context. There are therefore two key adaptations required (as detailed below, in part 3 section B) to account for differences between SupTech and EnfTech.

## B. Adapting the Di Castri model to optimise the deployment of EnfTech for consumer protection

The Di Castri model needs two main adaptations to optimise it to the deployment of EnfTech in consumer protection. One adaptation is (i) to better reflect the data sources available to consumer protection agencies . The other key change to the established model is (ii) to allow the ability to envisage how more sophisticated technology can also lead to a transformation of enforcement with the possibility of automated sanctioning of wrongdoing . This would go beyond the partial or assistive automation of Di Castri's fourth generation. Both of these adaptations are given more attention below.

### i. Data sources

A notable difference when applying and extending Di Castri's four generational framework to consumer protection authorities' tasks is the availability of data to consumer protection bodies.

In many respects, the Di Castri model starts from the assumption that data is available. In later generations, although the volume, variety and quality of the data improves as does the method by which it is transferred to the authority, data remains a critical building block of a technological approach to supervision and enforcement.

It is perhaps no surprise that the development of SupTech began in financial supervision where the availability of structured data is common. While not every authority will have the same

[71] An API or application programme interface enables two different computing systems to communicate and share data, see under heading 'Appliance Programming Interface (API)' in Annex 1 'Technologies and data: terms in use' for more detail.

[72] See heading 'Big Data' in Annex 1 'Technologies and data: terms in use' for more detail.

quantity or quality of data, financial markets are globally interconnected and as such systemic risks are managed via international institutions like the IMF, and related reporting obligations via instruments such as BASEL III.[73] For example, in the EU, a financial services institution is required by its relevant national financial supervisor to regularly submit[74] reports on a wide range of transactions.

This is not the case in consumer protection in non-regulated industries, where the availability of structured, mandated data is uncommon. There will seldom be a requirement for traders that fall within the remit of an authority to provide any data on their activities, nor for courts to report on their finding of infringements for example.[75]

As seen in the financial sector, other authorities can and do impose reporting requirements on the companies they regulate. Some of those agencies may have consumer protection remits. But generally, there are no such obligations on companies operating in consumer retail or service markets which encompasses a vast amount of digital provision via apps, websites, platforms, e-commerce etc. This lack of a regular, formalised route to obtaining data means that consumer enforcement agencies would not hold as much data as other authorities and thus may have to rely on alternative sources.[76]

Thus we find that the enforcement of general consumer protection laws has a data deficit that needs to be factored in, to address the assumption that data is available, which is a key cornerstone of the Di Castri model. Enforcement technology relies in the first instance on organising and structuring data[77] in the most effective way, leaving consumer law enforcement at a different starting point.

Consumer authorities are more likely to make use of unstructured data[78] than structured data (as would be the case for supervisory authorities in financial services). For example, a consumer authority may hold data from market studies they have carried out or judgements taken in cases they have led (see for example, the Polish Consumer Agency's AI tool included in the case study section). Some may also have data on consumer complaints, if they make provision for direct consumer complaints reporting. In some cases, complaints capturing systems also act in conjunction with a dispute resolution system, for example, the Philippine's DTI Consumer

[73] The Basel Framework is the full set of standards of the Basel Committee on Banking Supervision (BCBS), the primary global standard setter for the prudential regulation of banks https://www.bis.org/basel_framework/index.htm

[74] For example under rules created alongside the Market in Financial Instruments Directive (MiFID II DIRECTIVE 2014/65/EU), regulated entities providing investment services and activities must report on any transactions related to financial instruments traded on regulated markets.
EUR-Lex - 32014L0065 - EN - EUR-Lex (europa.eu) retrieved 26 April 2023

[75] Note however that in product safety in particular there may be some additional obligations, such as registering with authorities if selling a particular type of product which may make data analysis and tracking easier (see for example Energy Safety Victoria case study in Part 5, section A, number 5)

[76] See 'Technologies and data: terms in use' below

[77] As shown in Part 2 Institutional Framework, technology strategies and teams grew out of or continue to be based in data science units.

[78] Structured data is data that can be easily categorised and searched, for example product IDs, bar codes, phone numbers or dates. Unstructured data includes emails, text, videos or photos etc which are harder to organise and search. See under heading 'Big Data'' in Annex 1 'Technologies and data: terms in use' for more detail.

Complaints Assistance and Resolution System (DTI CARe System), which is a web-based portal for consumer complaints and associated redress.[79]

In addition, the amount of data available for consumer authorities to work with will vary between them. According to Professor Kovacic, the older the agency, the higher the likelihood of having a large data collection available on which to build.[80]

For those agencies that either do not collect consumer complaints data or where the volume of complaints is not sufficient to draw detailed inferences, they may want to seek access to data on complaints collected by other bodies such as consumer associations. Consumer organisations are indeed often the recipient of consumer complaints and thus their data could be an important source of complaints data or be used to identify trends on consumer experiences. For example, the UK's Citizens Advice (which has statutory duties as a watchdog for consumer issues including energy, post and communications) can derive close to real-time insights into the problems people are experiencing. This is captured either through the webpages they visit on their website (eg 'help paying for energy'), or through the logging of problems via call centres or walk-in advice services.[81] In the EU, the CICLE project (on Cooperation Improving Consumer Law Enforcement) is another example of a direct attempt to tackle the challenge of improving the management of the flow of complaints data received by consumer associations from consumers to enforcement agencies (see part 4, section B, number 1).

Agencies could also experiment with identifying data from social media commentary and complaints via Social Media audits. For example, the Bank of Ireland has used social media monitoring since 2013 to gather real-time insights about consumer experiences with financial services providers (FSPs) and emerging consumer issues.[82]

These data sources can form valuable data sets on which enforcement tools can be trained to make links between key complaint words and the likelihood of an infringement having taken place.[83]

[79] "Philippines' Technological Approaches to Consumer Law Enforcement" presented at 'Introducing EnfTech: a technological approach to consumer law enforcement 20 April 2023' by Ruth Castelo, Undersecretary for Consumers Affairs, DTI, The Philippines

[80] Bill Kovacic, Professor of Law and Policy, George Washington speaking at CMA Data, Technology and ANalytics Conference, June 2022 https://www.youtube.com/watch?v=q6cJ43v3AcY&list=PLJREEEp2I-xckXWl5O-_BELnqA0tf1bu-&index=4 accessed 27 September 2023.

[81] This has led them to claim that their data can show up imminent peaks in problems before they hit policy makers' agendas. For example, their data from autumn 2021 showed a peak in inquiries about referrals to food banks, advice on evictions, problems paying for heating etc which was an indication of the cost of living crisis, identified much earlier than other government or civil society groups had realised. See for example: 'Our new cost-of-living dashboard: the crisis we're seeing unfold' https://wearecitizensadvice.org.uk/our-new-cost-of-living-dashboard-the-crisis-were-seeing-unfold-aac74fb98713 accessed 21 July 2023 ; see also Public Dashboard Shares Ground-up Insights to Inform Government Response, Data.org Public Dashboard Shares Ground-up Insights to Inform Government Response accessed 21 July 2023.

[82] Consumer Protection Bulletin Social Media Monitoring, May 2017, Central Bank of Ireland Social Media Monitoring Consumer Protection Bulletin - May 2017 (centralbank.ie) <accessed 12 October 2023> and Market Monitoring Country Case, Social media monitoring using supervisory technology, CGAP Central Bank of Ireland (cgap.org) accessed 12 October 2023.

[83] A related use of data that has risen in popularity in the era of opening up government data and information, is the publication of regulators' data on companies' infringements. This is one task that the FTC's consumer sentinel

Other data collection methods are revealed through the consideration of consumer protection enforcement case studies shown in part 4.

### ii. The transformative potential of a fifth EnfTech generation

The second key change to Di Castri's established model is to extend its use to allow for conceptualising a more transformative use of technology in enforcement, and one better suited to the pace and scale of harm in digital consumer markets.

Earlier reference has been made to the transformative potential of advanced EnfTech to act as a continual monitor of consumer market activity and to signal warnings to companies about to commit an infringement or apply a corrective remedy near-instantaneously.[84] Technology that is predictive and prescriptive will no doubt vastly assist consumer enforcement authorities. For the future of enforcement in consumer protection, the move from the fourth generation to a fifth 'proactive' generation could be a game changer.

A proactive generation (as shown in figure 2 below) would be one where technology can perform the tasks of understanding what is happening, why it is happening, what is likely to happen next as well as identify and execute an enforcement action automatically. Because consumer law infringements such as use of unfair terms, or use of dark patterns are replicated exponentially, having the technology to match the likely volume of infringement and dispense from time consuming enforcement officers' review will be vital for giving authorities a quicker route to enforcement in digital markets.

This vision may seem ambitious and somewhat distant in comparison with the current state of consumer protection enforcement, but it is not illusory. This type of automatically executed remedy already exists in areas such as copyright infringements on content platforms, and is already in use by marketplace platforms to detect counterfeit goods.[85] There is capacity for extending its use (with appropriate governance and supervision) for consumer protection tasks ex-post monitoring, or to use it for ex-ante protection to prevent problems reaching the market in the first place.

In this sense, as signalled in Part 1, section D, the deployment of fifth generation EnfTech offers an opportunity to change the enforcement infrastructure and approach from a reactive and ex-post function to proactive and ex-ante protection measures. Generation five technologies could well be able to create a much more suitable enforcement infrastructure for digital consumer markets than has been the case to date.

Instead of the current system, we might imagine something more akin to road traffic enforcement where there are clear expectations on all participants, full infrastructure of warnings, monitoring and sanctions and high levels of compliance in place.[86] This report does

performs (see case study Part 4, Section B, number 12). This can be seen as way upholding consumer protection through the use of simply publishing data on companies with the purpose of naming/shaming those that perform worst.

[84] As set out in Part 1 The Need for Enforcement Technology in Consumer Law enforcement.

[85] See Part 5 Case Studies: EnfTech for consumer protection B. Learning from private and other institutional settings.

[86] Thank you to Anne-Jel Hoelen, Senior Legal Counsel, Authority for Consumers and Markets, Netherlands for this useful analogy.

not delve into this fifth generation, but any development efforts ought to reflect on how this goal may be achieved and we offer some ideas for cross-fertilisation in part 5 of this report.

*Figure 3: Five Generations of EnfTech*

The table uses Generational headings to describe the potential methods of data capture available to consumer protection authorities **('Data source and capture')**, a description of the analytical capabilities that are made possible by that data ('**Potential data analytics'**), with examples of what this might look like in practice ('**Examples'**).

| | **1. Descriptive** | **2. Diagnostic** | **3. Predictive** | **4. Prescriptive** | **5. Proactive** |
|---|---|---|---|---|---|
| **Data source and capture** | Limited data, manual entry, paper records, fragmented storage, basic infrastructure<br>Basic complaints interface, or mystery shopping results | Some automation of data entry and data collection via web portals, checking and validating data<br>Devices and open-source software to collect unstructured data | Big data architecture, more diverse and frequent feeds, APIs, more automation and validation of data collection<br>More sophisticated, possibly bespoke software to capture unstructured data eg images | Big data architecture real time flow of data, advanced AI-enabled collection, monitoring and validation of data<br>Plus sophisticated software to capture unstructured data or new forms of structured data eg digital product IDs | Big data architecture, real time flow of data, AI-enabled collection, monitoring and validation of data<br>Plus sophisticated software to capture unstructured data or new forms of structured data eg digital product IDs |
| **Potential data analytics** | Basic analysis of what patterns and problems occur<br>Mostly manual or basic computing | Richer analysis of what patterns and problems occur in more detail, and why<br>Some automation of analysis and statistical methods in use | What and why problems occur in more detail, and what could happen next<br>Predictive analytics through algorithmic analysis and some AI / Machine learning | What, why, what next in more detail plus proposing anticipatory action<br>Prescriptive analytics through advanced AI / Machine learning | What, why, what next in more detail, identifying and executing an action<br>Prescriptive analytics through advanced AI /Machine learning plus execution |
| **Examples** | *Complaints or results of sweeps compiled on databases.*<br>*Structuring databases to flag infringements*<br>*Static reports* | *Analysis of complaints to understand timing, business/ product type, sector, factors causing problems.*<br>*Dynamic reports and visualisation of data* | *Automated scrapes of consumer websites*<br>*AI-enabled or automated detection of unfair contract terms*<br>*Predicting where bad practice is likely to occur* | *Warning of impending infringement*<br>*Proposal for an appropriate and effective level of sanction* | *Executing action, eg remedy, sanctions, correction, preventative measure*<br>*Algorithmic enforcement - as seen in IP protection* |

**Source**: Liz Coll, adapting Di Castri's SupTech Generations model, 2022. Technical terms are defined in Annex 1

## C. Methodology for compiling and situating case studies in the EnfTech generational framework

In this part we described the methodology we have used to compile the case studies presented in part 4 and 5 of this report (i), as well as how we decided to assign each technology to a particular generation (ii).

### i. Methodology for data collection

In this report we have conducted an initial review of tools used by a variety of agencies, with a specific focus on those applied in consumer law enforcement.

The bulk of our work concerns EnfTech tools used by generalist consumer agencies which are presented in part 4 (but we have also highlighted tools in connected spheres that may have a useful application in consumer law seeking to look for cross-fertilisation potential across a range of SupTech, RegTech as well as tools used in consumer product safety in part 5).

There is no established body of information on the different technological approaches used by consumer protection agencies to carry out their enforcement functions. In addition, where technological approaches are in development, information is rarely publicly available. In a few cases, the agencies have recognised the value in their approach and the benefits of sharing it more widely and so have written up or presented detailed case studies of their work. Others have shared the results of applying enforcement technology, but have not given detailed information on why, how and what methods and techniques they used.

A challenge to research in this area is sourcing information on EnfTech at a detailed enough level to deliver insights. The research rests essentially on desk research and publicly available information, but was able to also benefit from existing knowledge and information gathered for the write up of *'Cross-border Enforcement of Consumer Law: Looking to the Future'* report in 2022.[87] Our knowledge was further enriched through the participation of Professor Riefa in the UNCTAD working group on consumer protection in e-commerce, as well as involvement in academic and legal conferences.[88]

More importantly the EnfTech research greatly benefitted from the event co-organised with UNCTAD on 20 April 2023, Introducing EnfTech: A technological approach to consumer law enforcement[89] which put the use of technology in consumer protection in the spotlight.

[87] Christine Riefa and others, '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' (2022).

[88] Including the International Congress on Sanctioning Dosimetry in Consumer Protection organised by the Deputy Superintendent for Consumer Protection (SIC Colombia), (27-28 June 2023); the Conference on Private Law and New Technologies organised by TELOS at King's College London (20-21 April 2023); the biennial Modern Studies in Commercial Law Conference on Embedding Innovative Technologies into Commercial Law: Challenges and Opportunities (University of Reading, 27-28 September 2023).

[89] https://unctad.org/meeting/introducing-enftech-technological-approach-consumer-law-enforcement

Identifying case studies and finding out more about them also relied on leveraging existing networks.We are grateful to everyone who generously gave their time to enable this work (for a full list see Acknowledgements).

The compilation of use cases cannot be described as systematic or exhaustive and will mean we have inevitably overlooked some examples. We invite any contributions to grow this unique body of case studies and contribute to the collective knowledge of the role of technology in consumer enforcement Information about new initiatives can be sent to info@enftech.org to be featured in future editions of this report.

### ii. Methodology for data comparison and analysis

The analysis of EnfTech tools relies on the adapted generational framework described above and illustrated in Figure 2. Generational categories contain a description of two things: firstly, progressively more advanced methods for capturing data sources, and secondly, the data analytical techniques these data sources then make possible.

Data source
enables
Potential analytics

For example, the prescriptive generation which can show why an event occurred and prescribe an action requires a big data source coupled with an AI-enabled learning technique. However, it does not necessarily correlate that a tool making use of a particular data source or method of capture will be using the same method of data analysis that the source makes possible. It is possible that some may use a data source classed within one generation but carry out analysis using data analysis techniques and outcomes classed within another generation.

Therefore, the task of assigning a generational category to an EnfTech tool is not straightforward, as some tools fit with elements of a category but not with all. For example, the Colombian Authority's sanction calculator tool uses manually inputted data on previous sanction decisions, putting it in the Generation 1 category, but applies statistical analysis to the data to suggest an appropriate level of sanction for new cases, which is a data analytical function within Generation 2.

Given this uncertainty, the classification of each tool required making decisions on how best to represent the generations of technology. We considered two things: firstly, what purpose we wanted the classification and presentation of case studies to serve and secondly, what information was available on which to make a decision about a classification.

As set out in part 3, the rationale for presenting case studies organised by generation of technical maturity included: assisting agencies by making sense of the landscape of useful technologies; facilitating exchange of best practice by helping identify peer institutions including those at a further level of advancement; understanding the capability of tools that they or others use. Given the breadth of other information and categories provided in the case studies to a primarily non-expert audience, we preferred to keep the presentation as simple as possible, opting for a single generational classification rather than differentiating between data type and source and analytical functions.

In terms of available information, our research did not include in-depth interviews with all of the organisations making use of the tools. Therefore, the analysis rests sometimes on a limited amount of consistently comparable information available on the data capture and data analysis features of each tool and the degree to which these could be understood as cutting across different generations. It was also not always possible to accurately deduce which generation the predominant element of the tool belongs to from the available information.

We therefore chose to identify the highest level of technology in use within any tool as its overall classification score. This is a practical response as such identification is relatively simple, despite the limited information.

We found that using the highest-level generation approach was the best way to compare and classify the range of tools within the limits of the available information. However, we fully acknowledge that this method may mis-represent the technological advancement of some of the tools we present. We also acknowledge that other methods for classification are available and that the current classification is a work in progress and may evolve over time, as underlying technology changes or as more information becomes publicly available about each case study. For all its imperfections, this classification methodology does lead to identifying some useful insights into the state of the EnfTech as it is currently being rolled out by consumer enforcement agencies (see Part 4, section C).

The remainder of this report turns to looking at use cases and classifying them as per the generational framework and methodology described above. The cases identified enable authorities at all generational levels of development to map out the route travelled and think about how to move between generations as well as how to develop tools matching the task at hand.

There are currently no examples of a proactive, fifth generation tool being used in consumer enforcement, but when considering the tools classified in Generation 3 or 4, it is apparent that some have the potential to be developed further to incorporate automating the execution of a remedy or sanction. For example, the Polish Consumer and Competition Agency’s AI tool to spot unfair contract clauses currently highlights potential cases to be studied by a human officer. If the tool continues to learn from the decisions made by humans, it could in theory begin to make those decisions itself.

This raises the question of 'correlation over causation' which is a well known phenomena in any statistical analysis.[90] Correlation describes the level of association or relationship between two events, which does not necessarily mean that one event is causing the other. Causation is harder to establish as it needs a more in depth understanding of the relationships between events. Where correlation is high, it can lead to other factors being ignored.

If an EnfTech tool is learning only from correlations and not causations, there is a risk that the wrong conclusions and decisions may be made and that the system continues to 'learn' and base further decisions on these.

[90] Rohrer JM. Thinking Clearly About Correlations and Causation: Graphical Causal Models for Observational Data 1 (2018) 1 *Advances in Methods and Practices in Psychological Science* 27-42, doi:10.1177/2515245917745629 accessed 28 August 2023.

# 4. Case Studies: EnfTech for consumer protection

This part focuses on live use cases specific to consumer enforcement. It first reviews the methodology used to select those cases (A), the cases themselves offering some overview of their functionalities (B) and finishes with some analysis of the salient features and trends we identified (C).

## A. Methodology for the selection of case studies

In the course of the project, we identified over 40 instances of technology currently actively involved in the regulation of consumer markets (such as finance, data protection and product safety). This section contains a compilation of 18 examples of the use of EnfTech specifically concerned with the enforcement task of consumer protection agencies or delivered in the consumer protection functions of dual competition/consumer protection authorities.[91] Part 5 of this report (on cross-fertilisation) will also deal with a number of other relevant examples in related fields that could have an application in consumer enforcement, although not specifically designed for it.

The 18 case studies found in consumer enforcement cover 7 different consumer authorities, 4 continents and span 3 generations of technology. The list of use cases is by no means exhaustive, and it is our understanding that new use cases are being worked on, but are not yet at the stage where they can be made public. We are aware of others but did not have access to sufficient information to feature them in the report at the time of publication.[92] We would welcome any information to include in future editions of this report about case studies we have not featured.

In any event, this compilation is the first of its kind in consumer law enforcement and will give the reader greater understanding of the type of technologies in use for particular enforcement tasks or goals. In its current format, the case studies are tagged according to the following features:

- **Generation:** the generation of analysis and insight technology to which the tool belongs, based on the most mature generation incorporated into the tool. The generation number refers to the generation in the adapted Di Castri's classification contained in Figure 2, pp.25.
- **Location:** The country or region from where the example originates.

[91] A dataset of cases and classifications is available on request

[92] This is for example the case of Korea where the agency uses AI in the context of consumer safety with an injury surveillance system (which searches online for products that were recalled using text and images to detect where products are still being sold) and a chatbot to facilitate consumer reporting (using the data to analyse the reporting and detect trends and dangerous products).

- **Sector:** denoting if the tool is used in the private or public sectors (note, the consumer protection EnfTech case studies are all from public authorities).
- **Organisation:** the type of organisation using the tool, in terms of consumer protection enforcement, this shows the institutional frameworks of the authority.
- **Consumer field:** indication of the area of consumer protection that the tool is predominantly concerned with, including a secondary and tertiary field if appropriate.
- **Data collection and analysis involved:** where known, the main task/s carried out by the tool is shown.
- **Technology field:** where known, the type of technology in use is included, starting with a top level field and if known, a secondary field and tertiary field if appropriate. A glossary of technologies referred to here is available in Annex 1 of this report.

## B. Case Studies

### i. Contents

17. Superintendence of Industry and Commerce (SIC), Colombia - Integrated Sanction System
18. Australian Competition and Consumer Commission (ACCC) and the Australia Securities and Investment Commission (AISC) - Scamwatch takedown trial

## ii. EnfTech use cases

Details of EnfTech use cases in Consumer Protection Authorities and in consumer protection function of dual Competition/Consumer Protection Authorities:

### 1. EU Consumer Protection Cooperation Network (CPC) – live complaints from consumer organisations to enforcement alerts

The CICLE project is part funded by the EU Consumer's Programme and consumer organisations OCU in Spain and Altroconsumo in Italy. CICLE aims to feed regular information to consumer protection enforcement authorities to fill in the gap of EU market surveillance and promote cooperation between consumer organisations and the authorities in the Consumer Protection Cooperation network under Regulation (EU) 2017/2394.

It maximises the potential of consumer complaints by improving the consumer-facing platform interface, and at the back end, creating a common framework of sectoral classifications. Complaints can be much more easily classified and mapped and eventually, there will be new capacity for a live tracking tool to generate alerts to authorities and detect trends relating to product types or companies. A further iteration of the platform in the next phase of the project from 2023 onwards will include an AI based tool that will automate the classification of complaints and cases and more quickly detect cross-border problems.

Gen 2 | EU | Public | Consumer Protection Agency Network| Cross-sector consumer complaints | web portal data collection | automated data analysis | real time

### 2. UOKiK, Poland - ARBUZ – AI-powered assistant detecting abusive contract clauses

UOKiK, like other national consumer protection authorities in the EU, is obliged to ensure that contracts used in everyday consumer transactions such as financial services or online subscriptions do not contain provisions detrimental to the interests of consumers.

The usual way to investigate whether such terms exist has been through the legal teams at UOKiK investigating external complaints of clauses which potentially infringe consumers' rights. In response, they carry out the time-consuming tasks of reading, analysing and assessing and so must read, analyse and assess standard contracts to identify abusive clauses.

To speed up and streamline this process and support staff in the initial review of contracts, the UOKiK held an open competition to create an artificial intelligence tool to perform the assessment task. The programme they selected is called ARBUZ - which in Polish means 'watermelon' and is a word similar to 'abusive'.

The ARBUZ system uses a class of AI solutions that come from deep learning, called ‘Transformer deep neural networks’. The system was trained on a valuable database that included a register of court judgements that officially recognised clauses as violating consumer interests. Since 2016, it has been the remit of UOKiK to recognise such clauses (with the business having the right to appeal to court), and so the database also included a large number of clauses that the UOKiK found to be abusive.

To add value to this information, the register was manually annotated by around 50 of UOKiK’s legal officers over the course of several months. They tagged the entries with the relevant industry, keywords and the passage from the judgement which stated why the clause was deemed to be unfair.

The input of experienced, legal staff gave ARBUZ the knowledge required to attempt automated analysis. The detailed annotation meant that when abusive clauses are identified, they are accompanied with a justification for the assessment given.

Employees dealing with the detection of prohibited clauses can now log in to ARBUZ and use it to support their daily tasks. As a first step in surveillance, it is equipped with a ‘crawler’ that allows a search of internet domains to assess whether they contain standard contracts.

ARBUZ can also be fed with contracts received along with consumer complaints or obtained from other sources, for example, submitted by the investigated company at the request of UOKiK.

Based on the forms uploaded to the system, ARBUZ reviews the contract selected by an employee of UOKIK. Using the slider, the sensitivity with which the analysis is to be performed can be set - e.g. 5, 10 or 20 illegal provisions are to be found. The system compares the contract with the clauses identified as abusive in the database.

Visually, the newly identified potentially unfair clause is highlighted, next to a second, more detailed screen showing how likely they are to be unfair, according to the system. This is shown by values in percentages based on a comparison of how similar they are to provisions formerly assessed as abusive. This is not just a simple comparison, ARBUZ uses intelligent algorithms to recognize the meaning of complex sentences written in legal language.

UOKiK sees ARBUZ as working at the level of an intelligent assistant - more than just a simple tool but not yet set up to make independent decisions. UOKiK staff either accept or reject its proposal which is an important stage in ‘supervised learning’ as it learns to better refine results. Management oversight is critical and tools have been built-in to allow directors to check and if necessary override incorrect judgements by officers, which reduces the risk of the program going in the wrong direction.

Gen 3 | Poland | Public | Consumer protection agency / dual agency | Consumer contracts | Unfair contract terms | AI | Deep learning | Transformer deep neural networks | Web crawler

### 3. UOKiK, Poland - Detecting and combating dark patterns with Artificial Intelligence

UOKiK is embarking on a project funded by the EU to develop a methodology for conducting proceedings on dark patterns and delivering a Proof of Concept for an AI-powered tool to detect dark patterns.

The project will take a holistic approach to the identification of dark patterns (sometimes known as deceptive design) for the purposes of enforcement, aiming to fully understand the design, occurrence and effects of dark patterns on consumer experiences. This will involve: a sweep to screen consumer facing websites and identify those with the highest incidences of dark patterns; a consumer survey about the experience of dark patterns; and neuromarketing tests to examine the neurobiological human reactions that occur when exposed to dark patterns.

All of these results will inform the next stage which will be the development of an AI-powered dark patterns detector.

Gen 3 | Poland | Public | Consumer protection agency / dual agency | e-commerce | dark patterns | Automated data capture and analysis | AI

### 4. Authority for Consumers and Markets (ACM), Netherlands – Scanning spoken marketing

Enforcement agencies also need to detect wrongdoing in offline environments, for example monitoring whether unfair commercial practices occur in telemarketing phone calls. The Authority for Consumers and Markets, Netherlands is exploring the use of AI in analysing the content of recorded interactions during phone calls to consumers. In the past, the agency had to rely on analysing a small sample of conversations, the use of AI makes analysis much more efficient as it can pick up on particular phrases and terminology.

The efficiencies gained enabled many thousands of phone calls to be surveyed for compliance with the law. The ACM is also applying this type of voice scanning technology to spot where online gamers who broadcast (so called ‘gamefluencers’) may be breaching laws on unfair commercial practices.

Gen 3 | Netherlands | Public | Consumer protection agency / dual agency | offline commerce | telemarketing | Automated data capture and analysis | AI

### 5. Authority for Consumers and Markets (ACM) Netherlands – Misleading reference pricing spotting tool

The ACM has also developed its own tool to spot infringements around reference pricing (when presented as a discount, the price at which an item is offered, should be the lowest price in use by the trader in the previous 30 days). The tool is designed to detect discounted prices that do not comply with the rule. The tool can scan hundreds of products in a given period of time to create a picture of prices being displayed multiple times a day. This creates thousands of data points which can be analysed by the tool to flag price reduction that may be misleading.

Gen 3 | Netherlands | Public | Consumer protection agency / dual agency | e-commerce | misleading pricing | Automated data capture and analysis | AI

### 6. Authority for Consumers and Markets (ACM), Netherlands – Fake countdown timer spotter

Building on their work with spotting potential reference price infringements, ACM have also developed a tool to detect misleading countdown timers. These timers are an example of a deceptive design (or dark) pattern where platforms or retailers give the impression that a limited period of time is available for a particular offer. This creates pressure to make a purchase by creating the illusion of scarcity. The use of timers in itself is not prohibited under Dutch law. However the timers must relate to a genuine limited sales period.

The ACM have built a tool in-house which is able to recognize the patterns that indicate a countdown timer is likely to be on a website, thus being able to scan many hundreds of websites for potential infringements. Launched in June 2023, the automated detection process identified 41 misleading countdown timers on retail websites across a wide array of sectors[93]. Prohibited practices included: countdown timers that would simply restart after countdown ended or offers that would remain unchanged after the countdown timer ended.

Gen 3 | Netherlands | Public | Consumer protection agency / dual agency | e-commerce | misleading pricing | Automated data capture and analysis | AI

### 7. Authority for Consumers and Markets (ACM) Netherlands – Network investigation tool

The Dutch Authority for Consumers and Markets is in the final stages of developing an interactive data visualisation and analysis tool, which can produce overviews of corporate structures and digital footprints in relation to violations of consumer law. The tool works by

[93] ACM confronts online stores using misleading countdown timers with their practices (27 June 2023) https://www.acm.nl/en/publications/acm-confronts-online-stores-using-misleading-countdown-timers-their-practices, accessed 1 December 2023.

importing static information, for example, information acquired through formal information requests, and APIs which connect to external databases to provide dynamic information. The tool allows investigators to quickly find hidden companies, websites and individuals that are related to consumer law violations.

Gen 3 | Netherlands | Public | Consumer protection agency / dual agency | consumer law violations | Automated data capture + static data import and analysis | AI

### 8. Authority for Consumers and Markets (ACM) Netherlands – Web scraping tool

The Authority for Consumers and Markets has developed an accessible web scraper[94] which non-technical and technical officials will find easy to use. It can be used for large-scale investigations that require the securing of digital evidence. It comes with a front-end dashboard which can be directed to make complex scrapes as required. It can process multiple domains at the same time and can be set to recurring scrapes and scrapes on exact moments in time, adding timestamps and hash values to the evidence.

Gen 3 | Netherlands | Public | Consumer protection agency / dual agency | consumer law violations | Automated data capture and analysis | Web scraping | AI

### 9. EU eLab - Mystery shopping environment

The EU eLab provides authorities with a toolbox to fully mimic consumer behaviour without being identified. This avoids the possibility that they would be blocked or even shown a different experience online.

The investigator sees exactly what a consumer would see, so they can replicate a typical consumer journey and experience all the deceptive or dark patterns that the consumer is subject to which may be unlawful as they unduly influence a consumers' choices. A screen recording tool enables authorities to collect this evidence.

Gen 2 | EU | Public | Consumer Protection Agency Network | online user experience|
Automated data capture* | VPN | Screen recording

*data analysis not known

[94] Web scraping refers to the gathering and copying of specific data from websites and is most commonly carried out by an automated process for example a web crawler (see Annex 1).

### 10. EU eLab - Investigating website provenance tools

The EU eLab works with specialised software providers and data brokers to connect to companies and individuals who are running or investing in websites carrying out potentially infringing practices.

These are publicly available/open source tools that open up access to data held in, for example, domain name registries or national company registries to give a risk score for particular people or companies. More sophisticated tools can uncover deeper links between entities, or between influencers and brands and advertisers. Depending on the jurisdiction, these findings could be accepted as evidence in court or would be a first stage in identifying bad practice which would then be verified and further evidenced by officers.

Gen 2 | EU | Public | Consumer Protection Agency Network | e-commerce | fraud | Automated data capture* | Website provenance

*data analysis not known

### 11. EU eLab - Price Reduction Tool: detecting misleading discount announcements

The eLab has begun to develop bespoke tools for specific tasks, the first one to be tested, tackled the challenge of misleading price reductions. In 2022, the CPC network carried out the first automated sweep on misleading price reduction announcements. The tool created in eLab for this purpose uses AI and webscraping techniques to flag such discounts on a user-friendly graphic interface, and provides evidence (in this case Black Friday[95]).

The EU has strict rules on promotional prices covered by Article 6(a) of the EU Price Indication Directive, which states that any advertised price reduction must indicate the prior price of the goods, and that this reference price must be the lowest price that the goods have been sold at over a 30 day period. Artificial price reduction might occur if the goods haven't previously been on sale at a higher price over the 30 day period, or at a price that reflects the discount being promoted to consumers.

CPC Authorities staff can use this to catch a much wider range of potential infringements than sampling or complaints would allow, although the decision on whether it is an infringement still remains with the inspector.

Gen 2 | EU | Public | Consumer Protection Agency Network | e-commerce | dark patterns | Automated data capture* | Web scraping | AI

*data analysis not known

[95] European Commission, Sweeps on Black Friday Sales (2022), https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/sweeps_en#ref-2022---sweep-on-black-friday-sales, accessed 27 November 2023

## 12. EU elab - Fake Review Detector (in development)

The eLab is currently developing a tool to more quickly detect fake reviews en masse. Fake reviews are a growing problem in online retail markets. Large quantities of fake or misleading reviews can skew results and make comparison of quality and value difficult for consumers. Investigations have revealed a thriving market in fake reviews, showing reviews can either be generated by machines, or written by people for goods or cash. Around 30% of fake online reviews come from review farms and/or users who have no experience with the product.

The tool uses natural language processing which can flag whether the review was computer generated or written by a person that has, in fact, not used the product or service. The purpose of the tool is to flag when a retailer or a platform has a high number of suspicious reviews, which may mean that the trader needs to step up its measures to ensure that consumers only see the genuine reviews.

Gen 3 | EU | Public | Consumer Protection Agency Network | e-commerce | fake reviews | Automated data capture and analysis | AI | NLP | Text analysis

## 13. Competition and Markets Authority (CMA), UK – web scraping for detecting infringements and compliance

The UK CMA has built a data analytics platform (in Amazon Web Services or AWS) which uses an implementation of JupyterHub to sort and analyse large amounts of data relating to both competition and consumer protection issues[96].

The CMA has used the technique of web scraping[97] to monitor and detect a range of consumer law infringements on websites. Machine learning with human oversight and checks is employed to analyse the data and assess where there is a problem. The DaTA unit (see Annex 2) has used analysed data collected via web scraping to look for patterns in online reviews that suggest fake or misleading practice. The unit also built their own tool to look at price data and detect where there is suspicion of retailers and manufacturers keeping prices at a fixed level.

Web scraping has also been used to check that companies are adhering to remedies or guidance stipulated by the CMA as a result of market investigations. For example, following an investigation into payday lending, lenders were required to put a link to a price comparison website on their site[98]. The CMA created code to scrape lenders' websites to check they were compliant. In a similar vein, the check on adequately disclosing commercial relationships for social media endorsements, used scraping to automatically check compliance with guidance.[99]

[96] 'The journey so far' in CMA blog (28 May 2019) https://competitionandmarkets.blog.gov.uk/2019/05/28/the-cma-data-unit-were-growing/, accessed 24 July 2023.
[97] See footnote 87 and Annex 1.
[98] See CMA PayDay Lending Marking investigation (2015) https://www.gov.uk/cma-cases/payday-lending-market-investigation#final-order, accessed 30 November 2023.
[99] See https://www.gov.uk/cma-cases/social-media-endorsements

Gen 3 | UK | Public | Consumer protection agency / dual agency | Cross-sector consumer complaints | Covid related | Automated data capture and analysis | Web scraping | AI | NLP

### 14. Competition and Markets Authority (CMA), UK – Covid Taskforce complaints data pipeline

The Covid pandemic and subsequent impact on business practices and consumers led to a large and sudden increase in consumer complaints to the CMA. A webform was launched to collect complaints using a free text box in which consumers could describe problems such as cancellations of travel or price spikes for essential health products. The free text boxes were analysed for content and key components such as name of company, sector, type of issue using machine learning. Machine learning was employed to clean the data, infer their content (using natural language processing techniques[100]) which could then be analysed.

This live pipeline of data enabled the authority to track and prioritise issues over time. It also led to the launch of consumer enforcement cases[101] and to track whether the enforcement intervention had decreased the number of complaints in that sector or company.

Gen 3 | UK | Public | Consumer protection agency / dual agency | e-commerce | loans | Automated data capture and analysis | Web scraping | AI | NLP

### 15. Federal Trade Commission, USA - Consumer Sentinel Network database

The FTC's Consumer Sentinel Network is a free access tool that holds data on millions of consumer complaints. This data can be analysed to show macro trends in complaints, and be interrogated to show details of complaints. For example, in the case of reported fraud, an upward spike in ID theft and online fraud was clearly seen in 2020 over the course of the early pandemic lockdowns. Users can click through this data to find details such as the contact method used or type of scam in play. International comparisons can also be made to assess the levels and types of fraud in other countries.

This data is used by FTC investigators, attorneys, economists and data analysts to aid enforcement. They can mine the information to identify law violations, targets for investigation and to find potential witnesses. Users can also request alerts based on particular issues or targets they are following.

Externally, the Consumer Sentinel also provides for greater awareness of what consumers should be on the lookout for. For example, the latest release of data via a consumer-facing

[100] See Annex 1 for terms and techniques.

[101] See https://www.gov.uk/government/news/latest-update-from-cma-covid-19-taskforce

dashboard showed that bank impersonation is the most reported text-message scam, followed by ‘free gift’ scams, fake delivery notifications and fake job offers.

Gen 2 | USA | Public | Joint consumer protection, data protection and competition agency | Cross-sector consumer complaints | general | Analysis of data collected via web platform | Open data

### 16. Federal Trade Commission, USA - Tech Labs investigative equipment and software

The FTC has a tech lab resource which its staff including investigators and attorneys can access to conduct work in support of the commission’s goals. The resources includes hardware such as mobiles, laptops, tables, wearables, monitors and cameras plus software applications. These tools are isolated from the FTC network so users are not identifiable.

They allow staff to collect and analyse digital content, including the content that a regular consumer user would see (such as images) and go on to  sign up and purchase goods to view contract terms or payment processes. They also enable staff to collect background information such as code, network traffic, data flows between devices and other usage data.

Gen 2 | USA | Public | Joint consumer protection, data protection and competition agency | online user experience | general | Automated data capture* | VPN | Code recording tools

*data analysis not known

### 17. Superintendence of Industry and Commerce (SIC), Colombia - Integrated Sanction System

SIC, the Colombian consumer protection authority is in the finishing phases of development of a tool to aid in the application of administrative sanctions. The *Sistema Integrado de Calculo y Application de Sanciones* tool supports officers to calculate and record sanctions, a task which involves the consideration of a large number of variables.

To start, the relevant variables, including the size of the company at fault, its financial health and capacity to pay the fines, the type of wrongdoing and its severity, the impact on consumers (and the type of consumers who were victims of the wrongdoing), are documented. An investigating officer can also document other relevant factors such as: additional aggravating or mitigating factors, such as whether the agency is dealing with a repeat offender or a small business on a first offence. The tool also enables officers to weight the different factors included in the calculation. Once all the relevant fields and weightings are input, the tool calculates an appropriate level of fine. This calculation is not the final decision, instead, it is a suggested proportionate figure that can be used by an officer alongside their judgement as part of the process to set a fine.

As well as reducing discretionary margins and lessening the burden in decision-making, the tool will help ensure sanctions are more proportionate and thus make them easier to defend on appeal, adding legal certainty and reducing costs for the authority.

The more the tool is used, the more data will be captured and stored (in accessible excel cvc files). Such a database can then be a foundation for more functionality. In time the tool could be expanded to assess if the level of fines issued is effective as a dissuasive tool, through comparing the number of fines at particular levels with the amount of re-offending businesses. As well as the analysis of past practices, the tool could be developed to make predictions for an appropriate, proportionate and dissuasive fine. At present the tool requires human input to populate fields and to make the final decision by applying discretion. This discretion, currently based on the experience of legal officers, could to some extent be 'taught' to a tool once it has enough data so that it can, not only make a more refined prognosis, but also make predictions.

Gen 2 | Colombia | Public | Consumer protection agency / dual agency | Sanction setting | Manual data capture and statistical analysis | Excel

### 18. Australian Competition and Consumer Commission (ACCC) and the Australian Securities and Investment Commission (AISC) - Scamwatch takedown trial

The Australian Competition and Consumer Commission and the Australian Securities and Investment Commission are working together on detecting scams and disrupting their progress. Part of their work involves trialling the application of existing private enforcement software tools used for cyberattack and malicious website scanning and takedown of consumer facing scams.

Netcraft provides an automated detection service that it uses to discover fraud, potential cyberattacks and scams. The software can detect features common to potential scam activity such as fraudulent domains.

Machine learning techniques are then applied to this data to confirm whether the data patterns give a positive indication of a live threat. If confirmed, the software 'disrupts' the process by blocking sites, and issuing notices to web hosts who can then investigate and take down fraudulent sites. During the 21 day trial, the ACCC referred 1,757 web addresses to be analysed by Netcraft of which 381 were found to be malicious, and were subsequently removed.

Gen 3 | Australia | Public | Consumer protection agency / dual agency / financial supervisor | Fraud | online scams | Automated data capture and analysis | AI | Machine learning

## C. Main findings from the case studies

Mapping the case studies against generations shows that there are gains to be made at any stage. For example, the EU Consumer Protection Cooperation Network co-funded a project to organise and structure consumer complaints received via various web platforms data in a systematic way across borders in the single market. This immediately improved the ability to spot patterns and communicate them to a regional authority, with enforcement action initiated against two companies within six months of the initial pilot being developed.[102]

There's a lot happening across a wide range of authorities. While fewer examples were found in agencies from developing and transitional economies, there are technological tools such as ODR platforms, complaints submitted via mobile texts, and apps provided by authorities for use by consumers, (for example to check websites for privacy protection), which come from non-OECD countries. This activity suggests that consumer protection authorities in all parts of the world have started to recognise the value of technology, but at present more tailored research would be helpful to discover where technology might be applied to the task of enforcement as well as the task of consumer communication and advice in developing countries or what work is currently underway for agencies to proceed.

Our snapshot survey reveals that most authorities are at the diagnostic/ predictive/ stage. A lot of the activity remains in detection. Nevertheless, this first wave has proved valuable in assisting staff in their enforcement tasks and freeing up some valuable investigative time normally spent by officers. The survey of case studies also reveals that there is an increased appetite amongst the agencies that have been making progress in harnessing some features of AI and moving through the generations of technology to increase their capacity. This rapid move may of course be driven by a range of factors (which we did not study) including existing agency structures facilitating prompt adoption for example where there is a strong team of technologists in post already or where staff numbers may allow some redeployment on infrastructure projects. In other cases, the adoption of new technological solutions may be driven simply by the urgent needs of the agency.

In many cases we did have to rely on the agency's own description of tools, many including 'AI-powered' or simply 'AI'. In the absence of further information on these, it was difficult to ascertain the particular type of AI used, or whether the agency may have in fact been using data science or algorithmic interrogation techniques which do not strictly fall under the definition of artificial intelligence (but would fall under the definition of EnfTech in any event). We went on face value. From this standpoint, we identified that AI use is accelerating. In 2020, only 6 consumer authorities were identified as using technology in enforcement and AI was not heavily

[102] The CICLE pilot launched in May 2022 led to two coordinated enforcement actions based on data analysis of consumer complaints- one against Samsung for misleading and aggressive conduct around a phone recycling plan, one against Citroen for anomalies in its AdBlue anti-pollution system which resulted in costly repairs for consumers CICLE digital consumer complaints tool delivers fast and timely enforcement | Euroconsumers accessed 20 July 2023

featured, with other tools, such as data analysis, being preferred.[103] However, in a short time, the proportion of agencies using AI has jumped from about 40% of use cases[104] to just over 66% (12 out of the 18 case studies) at the most recent count (as described in this version of the report).

However, it is not possible to extrapolate from this figure how widespread the use of AI may really be because our study focussed on a sample of authorities that were identified in the literature as 'leading' in the adoption of a technological approach to consumer enforcement.[105] As a result, this figure is necessarily skewed. Many more agencies will have no EnfTech programme at all and will be far from being able to even think of AI as a credible and widespread tool.

Consumer protection agencies appear to be on their own individual and time intensive learning journeys. More co-ordination of technology-based supervision and enforcement solutions by authorities would help ensure that best practices are not limited to one jurisdiction and avoid the costly duplication of development work. It will also ensure that failures in one agency are used as learning opportunities in another. For EnfTech to succeed there will be many programmes that will be likely not to be as viable or successful as first hoped. Avoiding duplication of mistakes would be as important as sharing best practices on what is effective. More recently, the OECD, ICPEN, and UNCTAD have been working on technological approaches to enforcement and thus, it may be possible to envisage further work in this area leading to a more 'standardised' approach. There are indeed many gaps in the common understanding of best practices and how the use of AI in enforcement for example should be framed. Here, some work towards an international set of guidelines ought to be a very valuable addition to the nascent literature on the use of technology in consumer enforcement.

Furthermore, experimenting with tools that start to step into the fifth generation to test out the use case for execution of enforcement remedies would also be welcome, but at present the technology and data streams available may not yet allow a reliable transition for enforcement agencies.

[103] Stefan Hunt, The technology led transformation of competition and consumer agencies: The CMA's experience, discussion paper (14 June 2022).

[104] New use cases were added and use cases that were not classed as AI have now moved to using AI as an underlying technology. We are not able to verify the understanding that each agency has of what AI is and thus is it possible that some tools may not technically be classed as such. We however calculated the most recent percentage based on the descriptions officially published by authorities regarding the technology they are using.

[105] In two main sources: Stefan Hunt, The technology led transformation of competition and consumer agencies: The CMA's experience, discussion paper (14 June 2022) and Stephanie Nguyen, A Century of Technological Evolution at the Federal Trade Commission (https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/02/century-technological-evolution-federal-trade-commission accessed 3 July 2023).

# 5. Developing EnfTech: potential for cross-fertilisation

Whilst researching EnfTech examples specific to consumer protection authorities, the research also uncovered many other use cases with particular resonance for consumer protection tasks. They were identified in two different realms: (A) in public authorities, and (B) in private or other institutional settings. These selections are presented here, separate from the specific EnfTech collected for consumer protection case studies. However, the types of tools in use are helpful in suggesting what other approaches and technologies Consumer Protection Authorities could adapt or make use of for their own work. This is particularly relevant because some of the EnfTech solutions that can be used for cross-fertilisation purposes are ahead in the generational framework described above in part 3 and can thus help inform where consumer law enforcement could move forward.

## A. Learning from other public authorities' work

A selection of EnfTech use cases in public authorities with relevance to consumer protection is available below:

1. Energy Safety Victoria, Australia - electrical safety sweep
2. Superintendence of Industry and Commerce (SIC), Columbia - Sabueso pricing monitor
3. CNIL, France – CookieViz software to identify non-compliant cookie usage
4. Bangko Sentral ng Pilipinas/Central Bank of Philippines – BOB: BSP Online Buddy Chatbot and Processing Utility for Consumer Complaints
5. Australia Securities and Investment Commission (AISC), Australia: Financial promotions tool trial
6. Monetary Authority of Singapore (MAS), Singapore - Anticipating misconduct
7. Advertising standards agency (ASA) UK – Tracking non-disclosed influencer ads

Each case study features a description of the tool as it is currently used as well as an analysis of how the tool can come to assist consumer enforcement agencies below the purple keywords description.

### 1. Energy Safety Victoria, Australia - electrical safety sweep

Energy Safety Victoria is the state's energy safety regulator. Its responsibilities include maintaining a registry of authorised electrical product providers who need to demonstrate that their goods have passed the appropriate electrical safety checks before being put on the market.

They designed an AI tool that can identify where electrical products are being sold online via visual and text recognition. Once identified, the seller is matched against the registry to check if they are authorised to sell the product to consumers. The tool can also be used in stores by inspectors, who scan the product information and the supplier linking back to the registry to check credentials of the seller.

Gen 3 | Australia | Public | State energy safety regulator | Product safety | electrical product safety | Automated data capture and comparison | AI | Machine learning | Data comparison

**Learning for consumer protection authorities:** the tool solves a problem that is common to all forms of consumer protection enforcement - identifying products of a particular type for inspection. Where a large amount of products are available in online and offline marketplaces, it can be difficult to identify categories for inspection. This tool uses visual and text recognition to find the products most likely to be in a particular category, in this case electrical goods, which can then be checked back against the official register of providers to see if they are certified to sell electrical products and thus meet state safety requirements. Of course, this tool to speed up product safety surveillance works as there is a registry of products to cross reference against. For the many consumer products for which this will not be the case, the technology that can quickly scan and identify goods for monitoring is nevertheless useful.

## 2. Superintendence of Industry and Commerce (SIC), Columbia - Sabueso pricing monitor

The competition arm of Colombia’s competition and consumer protection authority have developed a tool for surveying pricing patterns in e-commerce markets. The tool is known as ‘Sabueso’ (which means bloodhound in Spanish) and carries out the resource-intensive task of collecting publicly available information on goods and prices.

The data collection is automated by the tool, resulting in a user-friendly presentation of pricing data. Machine learning programmes are trained on visuals of products shown on websites to identify when a product is the same, regardless of its name or description. This helps in investigations to recognise possible anti-competitive practices such as price fixing.

Gen 3 | Colombia | Public | Consumer protection agency / dual agency | e-commerce | price fixing | Automated data capture and analysis | AI | Machine learning

**Learning for consumer protection authorities:** similarly to the Energy Safety Victoria scanner, Sabueso’s machine learning tool takes on the task of capturing and analysing publicly available information on goods and prices for items sold online. Its design means it can help with a key challenge of online retail platform sales - that of the same product being sold under different brands or descriptions, where smart analysis of unstructured data is required.

## 3. CNIL, France – CookieViz software to identify non-compliant cookie usage

France's Data Protection Authority known as the Commission Nationale de l'Informatique et des Libertés (CNIL) includes a digital innovation laboratory known as the Laboratoire d'Innovation Numérique de la CNIL (LINC).[106] LINC has developed a piece of software called 'CookieViz' which as the name suggests, makes cookies stored by third party domains visible by analysing the interactions between a browser and remote sites and servers.[107] Third party cookies are the non-essential cookies which are mostly used to collect data about people's browsing behaviour which can then be packaged and sold on for marketing or advertising purposes. Under European data protection rules, consent must be obtained from website users if they wish their online browsing behaviours to be captured by these cookies.

Once the third party cookies are made visible, further analysis can be carried out to find out whether the proper consent as required by law has been obtained. On the basis of these results, the CNIL was able to send a letter to the highest viewed websites in France which were not obtaining adequate consent to advise them to change their practice.

LINC has made the CookieViz software source code openly available so other developers can work with it and enhance its functionality.

Gen 2 | France | Public | Data protection agency | data protection | cookie use | Automated data capture and analysis | Open source

**Learning for consumer protection authorities:** the CookieViz tool is a good example of bringing transparency and accountability to company's online practices. This example is also interesting as it has the potential to move into Generation 5 - that of direct execution of a warning letter to a company where non-compliance with GDPR is discovered. If this feature were to be developed, it would start to mirror the activity found in the private enforcement of copyright infringement where takedown notices are issues automatically with minimal or no human intervention on discovering content in breach of copyright on platforms (see case study 5 on Algorithmic enforcement of copyright breaches in the next section).

[106] https://linc.cnil.fr/propos-de-linc,accessed 19 July 2023.

[107] Goring,CookieViz 2:3: Une nouvelle version plus sécurisée, plus stable et une mise en avant du rôle des intermédiares, https://linc.cnil.fr/cookieviz-23-une-nouvelle-version-plus-securisee-plus-stable-et-une-mise-en-avant-du-role-des, accessed 6 October 2023.

## 4. Bangko Sentral ng Pilipinas/Central Bank of Philippines – BOB: BSP Online Buddy Chatbot and Processing Utility for Consumer Complaints

The Philippines' Central Bank rolled out a consumer complaints chatbot in 2017-18 which enables consumers to submit complaints through their mobile devices via an app or via SMS. BOB which stands for the BSP Online Buddy can receive complaints and respond to them using machine learning and NLP (natural language processing)[108].

As well as providing an easier interface for consumers who are comfortable with online interactions, BOB's back-end system can classify, store and analyse the complaints. In this way, consumers are generating a dataset which the Bank can interrogate to understand more about consumer experiences and to detect potential market misconduct.

Gen 3 | Philippines | Public | Central bank | consumer complaints | general | Automated data capture and analysis | AI | NLP

**Learning for consumer protection authorities:** this type of tool could be of use in any authority or organisation that collates consumer complaints, although caution would be needed to ensure that there are alternative channels of communications if consumers are not comfortable or able to interact with a Chatbot. The use of natural language approaches to understand, respond and process human language is becoming more common, this tool also shows the value in having an additional system that runs analyses on the complaints to aid enforcement activity.

## 5. Australia Securities and Investment Commission (AISC), Australia: Financial promotions tool trial

In response to a rise in financial promotions targeting vulnerable consumers during the Covid-19 pandemic, the ASIC trialled the use of artificial intelligence and machine learning tools to monitor financial promotions on a mass scale. The tools were designed to identify promotions and adverts for products like credit, insurance and wealth management that were potentially in breach of the law, and then to put these forward for human review. In a three month trial the tool scanned around 1.7 million webpages, identifying 1,950 potential risk cases for review. The trial showed the potential efficiency of automated web scraping and analysis of promotions as compared to the task being done solely by human staff.[109]

Gen 3 | Australia | Public | Financial supervisor | Fraud | malicious promotions | Automated data capture and analysis | AI | web scraping

[108] Di Castri, Simone and Grasser, Matt and Kulenkampff, Arend, A Chatbot Application and Complaints Management System for the Bangko Sentral ng Pilipinas (BSP). R2A Project Retrospective and Lessons Learned (May 8, 2020). Available at SSRN: https://ssrn.com/abstract=3596268 or http://dx.doi.org/10.2139/ssrn.3596268

[109] ASIC's regtech initiatives 2019–20 Report 685, January 2021 https://download.asic.gov.au/media/5937756/rep685-published-20-january-2021.pdf <accessed 12 October 2023>

**Learning for consumer protection authorities:** this example shows again the value that technological tools can bring for speeding up monitoring of markets. This can be particularly useful for online markets where tracking information can be difficult and the production of content is fast moving. It can also be useful for agencies where staff are stretched as it can transfer some time previously spent on the identification of wrongdoing to be invested in investigating problematic behaviours, potentially increasing the rate at which intervention can take place.

## 6. Monetary Authority of Singapore (MAS), Singapore - Anticipating misconduct

The Monetary Authority of Singapore (MAS) uses existing reports of misconduct by financial adviser representatives working at insurers, banks, and financial advice firms to develop a series of predictive factors for identifying those most likely to sell unsuitable life insurance or investment products to consumers.

The model affirmed supervisors' intuition that factors such as misconduct history and previous work experience of the representatives are statistically significant in predicting future misconduct. Using the model, MAS is able to identify representatives and transaction samples for scrutiny during onsite inspections.[110]

Gen 3 | Singapore | Public | Financial supervisor | Misconduct | mis-selling | Automated analysis of data** | | statistical analysis predictive modelling

*data collection not known

**Learning for consumer protection:** of interest here is the capability of tools to anticipate potentially harmful activity before it occurs. Technologies supporting enforcement agencies protecting consumers, from companies likely to use pressure selling tactics or with a track record of using deceptive design patterns will be essential if the shift to an ex-ante, proactive approach to market supervision is to become a reality.

## 7. Advertising standards agency (ASA) UK – Tracking non-disclosed influencer ads

The ASA first used AI technology for its monitoring work in 2021. The ASA has to analyse a very large volume of digital content from advertisers and social media influencers who are paid to endorse or promote products. They used a machine learning tool that could scan and

[110] Case study featured in Appendix 1 of The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions: Market developments and financial stability implications (fsb.org)

categorise images and text in influencers' social media posts and assess the likelihood of them being advertisements.

The next step was to see if it was appropriately disclosed as an ad as required by the Committees of Advertising Practice code, a self-regulatory code with a compliance function that 'names and shames' those breaking the rules. Enforcement action can be taken against persistent offenders with a referral to Trading Standards Services and the Competition and Markets Authority who have responsibility for upholding regulations on unfair trading[111]. According to their 2021 annual report, almost 20,000 Instagram Stories were captured and analysed each month.

As well as identifying infringements, they were able to analyse which of the non-disclosed adverts might fall into high-risk categories, for example, those aimed at children. They could also analyse those companies partnering with influencers who might be driving bad practice, with the ability to refer these to statutory enforcement authorities. Subsequent work by the agency has tracked scams in online display advertising and potentially misleading green claims made by energy companies. The Agency is now growing its Data Science team to support and complement this work.

Gen 3 | UK | Public | Advertising regulator | Misleading advertisements | influencers | Automated data capture and analysis | AI | Machine learning | Data comparison

**Learning for consumer protection:** the agency focuses on advertisements but the methods employed to track infringements of their code are applicable to other online platforms or any type of monitoring and detection that requires reviewing a mix of unstructured data such as images and text.

## B. Learning from private and other institutional settings

A selection of EnfTech in private or other institutional and academic settings with relevance to consumer protection is available below. Those solutions could be taken as a demonstration of what is possible in terms of detection, and/or industry collaboration in enforcement, with industry, exercising responsibility for detecting and eradicating bad practices, thus saving enforcement agencies time and resources.

1. Austria Institute of Technology - Fake Online Shops spotter
2. Amazon AI fake review detector
3. Alibaba counterfeit goods spotter
4. Digital product identities

[111] CMA OFCOM, ASA, Regulatory roles in tackling hidden advertising, Regulatory landscape: Social media endorsements (publishing.service.gov.uk), accessed 1 December 2023.

5. Algorithmic enforcement of copyright breaches
6. Detection of Generative AI created synthetic content
7. Identification of unfair contract clauses and non-compliant privacy terms
8. Web crawler for dark patterns

Each case study gives a description of how the tool is currently used and a reflection on how it could be applied for consumer protection tasks, either in its entirety or by using selected particular components.

## 1. Austria Institute of Technology - Fake Online Shops

Fake online shops tend to cut and copy code between them, so a tool has been developed by the Austria Institute of Technology that can compare the programming codes behind suspicious shops, detect similarities, and give a high or low risk score to potentially fake shops. The tool is called 'MAL2' (MAchine Learning detection of MALicious content)[112] which flags suspicious shops whose code is similar to that of other fake shops. The tool then analyses the code using more than 22,000 assessment factors and determines the level of risk (from low to high) risk or high risk[113]. The tool was tested between July 2020 and January 2021, evaluating around 17,500 websites, with results compared against expert human analysis. The tool matched detection in 90% of cases, making it a reliable tool for detecting fake websites.

Gen 3 | Austria | Private | Research institute | e-commerce | fraud | Automated data capture and analysis | AI | Machine learning

**Learning for consumer protection enforcement:** the tool is in fact deployed to enable consumers to avoid the sites altogether. A plugin into a browser can detect and disable the site for the consumer equipped with the plug-in but it could also be adapted for enforcement purposes.

## 2. Amazon - AI fake review detector

In June 2023, Amazon responded to various regulator and consumer organisation complaints about the number of fake reviews on their platform. In an announcement covering a range of actions, they also indicated that they already invest significant resources, including machine learning tools which proactively stop fake reviews. The machine learning models "analyze thousands of data points to detect risk, including relations to other accounts, sign-in activity,

[112] https://www.ait.ac.at/en/news-events/single-view/detail/6860?cHash=250795314de77d44fa029af1a1310da2

[113] According to the open source information available on GitHub, the project uses Deep Neural Networks and Unsupervised Learning to advance cybercrime prevention, <https://github.com/mal2-project/fake-shop-detection_models>; This is confirmed by the Austrian Research Promotion Agency which funded the project, <projekte.ffg.at/project/3044975> both accessed 25 April 2023.

review history, and other indications of unusual behavior”.[114] They claim to have blocked over 200 million reviews suspected to be fake in 2022.

There are also consumer facing tools run by third parties which can help people identify fake reviews. For example, ReviewMeta[115] works by enabling online shoppers to paste the Amazon product URL into their browsers to see an analysis of the reviews. It analyses patterns in reviews, including the language, and details of the review poster and presents consumers with an adjusted review score, based on the removal of those reviews that it suspects of being fake.

Gen 3 | International | Private | Platform | e-commerce | fake reviews | Automated data capture and analysis | AI | Machine learning | Text analysis

**Learning for consumer protection**: of interest here is the development and roll out of tools doing the same or similar job. For example, The EnfTech in consumer protection section gave the example of the EU elab’s Fake Review Detector (Part 4, Section A, 1) which, based on the information available, appears to also use AI to detect the likelihood of fakes. An obvious learning point for Consumer Protection authorities could be to establish when it is most appropriate to make use of existing tools such as third-party run fake review scanners and when building bespoke tools is the best option.

### 3. Alibaba - counterfeit goods spotter

Alibaba Group has a monitoring tool to tackle online counterfeiting and piracy. It uses fake product identification modelling, image recognition, semantic recognition and product information databases to identify products and real-time interception systems to serve take down notices. Further, by tracing the movement of funds and finance, it can identify counterfeiters and the factories producing the goods.[116]

Gen 4 | International | Private | Platform | e-commerce | counterfeit goods | Automated data capture and analysis | AI | Machine learning | Data comparison | Realtime interception

**Learning for consumer protection:** As with the Energy Safe Victoria tool and Sabueso tool of the Colombian authority, product identification modelling will be helpful in filtering categories of products for inspection. Interesting here too is the ability of the tool to track and trace back to the source of the problem, as far as a physical location. This use could extend to fake reviews, fake products or unsafe products in consumer markets.

[114] Blog post by Dharmesh Mehta, Vice President, Worldwide Selling Partner Services, 13 June 2023, accessed 19 July 2023 3 steps Amazon is taking to stop fake reviews (aboutamazon.com)
[115] How it Works - ReviewMeta Blog – accessed 19 July 2023
[116] Mostert, F and Lambert, J, Study on IP Enforcement Measures, Especially Anti-Piracy Measures in the Digital Environment (July 23, 2019). WIPO/ACE/14/7, 2019, Available at SSRN: https://ssrn.com/abstract=3538676 <accessed 12 October 2023>

## 4. Digital product identities

Other innovations include companies developing individual digital identities for consumer products, enabling them to be part of 'product cloud' which organises the world's ecosystem of product lifecycle data[117]. An active digital identity is given to every product at serialised item, stock keeping unit or batch level. These are currently used to identify which branded products are genuine or counterfeit.

Gen 3 | International | Private | Multiple | e-commerce | counterfeit goods | Automated data capture and analysis | IoT | AI | Data comparison

**Learning for consumer protection:** Digital identities could in theory be given to any product to enable greater transparency and tracking of a product throughout its lifecycle to check for compliance. For example the EU's new proposals on Digital Product Passports[118] are designed to open up data on its component parts to enhance opportunities for repairability, durability and recycling. With the right infrastructure, in future claims made by companies about their green credentials such as durability could be checked back against the data on the actual product to ensure they could be verified. Digital identities provide the traceability that surveillance tools rely on (for example, Energy Safety Victoria's tool makes use of a registration scheme in order to check back on providers). In the absence of formal registration schemes, digital product identities could have the potential to provide some of that capacity and enable broader surveillance of consumer products.

## 5. Algorithmic enforcement of copyright breaches

Online content platforms use automated search and takedown tools to remove material that breaches copyright. Copyright owners use robots to issue huge volumes of takedown requests to platform intermediaries, and the platforms use algorithms to filter, block, and disable access to allegedly infringing content automatically, with minimal or no human intervention[119].

This approach is embedded in the design of all major intermediary systems since the adoption of the Digital Millennium Copyright Act (DCMA) in 1998. However, the law enforcement and adjudication role played by private online intermediaries is subject to little transparency or accountability for how decisions are made, and redress is challenging.[120]

[117] See for example: https://evrythng.com/

[118] Public Hearing of the European Commission Committee on the Internal Market and Consumer Protection "Digital product passports: enhancing transparency and consumer information in the internal market" <https://www.europarl.europa.eu/committees/en/digital-product-passports-enhancing-tran/product-details/20220510CHE10181 accessed 12 October 2023>

[119] Accountability in Algorithmic Copyright Enforcement, Maayan Pere & Niva Elkin-Koren,,19 STAN.TECH. L.REV. 473 (2016)

[120] As above Perel/ Elkin-Koren

Gen 5 | International | Private | Platform | e-commerce | IP infringement | Automated data capture and analysis | AI | Machine learning | Data comparison

**Learning for consumer protection:** despite the challenges of accountability and transparency, the long standing use of algorithmic enforcement of copyright on content platforms offers a useful view of the extent to which large-scale, platform based enforcement can be carried out. The EnfTech in consumer protection in section B shared the example of ACCC/AISC's Scamwatch trial, which has much in common with this approach. The software that they applied for public enforcement purposes was in use for private enforcement. When the software spotted a potential risk, it blocked the site and issued notices to web hosts who then investigated and took down fraudulent sites. This shows the potential to copy across elements of established private enforcement to public use, or for authorities to require platforms to be more accountable for this type of monitoring for consumer facing harms.

## 6. Detection of Generative AI created synthetic content

The rise in content generated by AI that is convincing enough to pass as real has raised serious concerns. Fake reviews, fake news, deep fake videos and ever more convincing scams are just a few of the harms that could occur as plausible looking content is transmitted in greater amounts. Developers are responding to the need to be able to verify the provenance of content and identify whether it was created by an AI or not.

For example, digital watermarks make tiny adjustments to the word pattern of an AI-generated text which create a 'fingerprint' that can identify how it was produced. Google's DeepMind has already launched a beta version of such a watermarking tool for images[121]. There's also software to help prevent adaptation by an AI system, for example, MIT have released 'Photoguard'[122] which makes invisible changes to a photo that then prevent it being modified by an AI system.

International | Private | Multiple | pan-digital | Misinformation/Disinformation | Automated data capture and analysis | AI | Machine learning | Data comparison

**Learning for consumer protection:** These types of technology, although in their infancy, could eventually be used by enforcers to monitor content to check its provenance, or to carry out audits on whether companies or platforms are correctly labelling AI generated content as such.

[121] https://www.deepmind.com/blog/identifying-ai-generated-images-with-synthid (accessed 6 September 2009)

[122] https://www.technologyreview.com/2023/07/26/1076764/this-new-tool-could-protect-your-pictures-from-ai-manipulation/ (accessed 6 September 2023)

## 7. uTerms - identification of unfair contract clauses and non-compliant privacy terms

An academic team have a developed a prototype called 'uTerms'[123] that reads and highlights potentially unfair terms to automate the time-consuming processes of reading, reviewing and judging the likelihood of unfairness of clauses. Based on training data from 20 online service terms, partially automating the initial stage frees up the time of lawyers and consumer organisations who can then focus on analysis and initiating proceedings where appropriate[124]. Members of the uTerm team were also involved in developing a tool called CLAUDETTE[125] which used the same approach to evaluate whether companies' privacy policies were compliant with the EU General Data Protection Regulation.[126] The European consumer organisation BEUC was also involved in assessing the potential of the tools for practical application.

Gen 3 | EU | Private | Academic partnership | contractual clauses | Unfair terms | Automated data capture and analysis | AI | Machine learning

**Learning for consumer protection:** These tools were developed specifically for consumer protection and data protection uses, as part of an interdisciplinary research project which involved academics from the fields of law and software engineering as well as civil society. The value of linking up different disciplines and sectors when developing EnfTech is clear here.

## 8. Princeton University - Web crawler for dark patterns

An academic team at Princeton University has developed software that can automatically identify dark patterns on a large set of consumer facing e-commerce websites. They demonstrated how software could be used to detect which websites are using techniques that might for example push users towards disclosing more personal information or spending more money than they would otherwise do. Of the 11,000 shopping websites, they detected 1,818 instances of a dark pattern, of which 183 were found to constitute deceptive practice.[127]

Gen 3 | USA | Private | Academic partnership | e-commerce | dark patterns | Automated data capture and analysis | AI | Machine learning

[123] The software can be downloaded at: http://uterms.software

[124] Micklitz, HW., Pałka, P. & Panagis, Y. The Empire Strikes Back: Digital Control of Unfair Terms of Online Services. *Journal of Consumer Policy* 40, 367–388 (2017). https://doi.org/10.1007/s10603-017-9353-0, accessed 12 October 2023

[125] Claudette stands for automated 'CLAUse DETectEr' and a demo an be found at http://claudette.eui.eu/demo/ <accessed 12 October 2023>

[126] Contissa, G, Docter, K, Lagioia, F, Lippi, M, Micklitz, H-W, Pałka, P, Sartor, G and Torroni, P 'Claudette Meets GDPR: Automating the Evaluation of Privacy Policies Using Artificial Intelligence' (July 2, 2018). Available at http://dx.doi.org/10.2139/ssrn.3208596 <accessed 12 October 2023>

[127] Mathur, A, Acar, G, Friedman, MJ, Lucherini, E, Mayer, J, Chetty, M and Narayanan, A. 2019. Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. Proc. ACM Hum.-Comput. Interact. 3, CSCW, Article 81 (November 2019), 32 pages. https://doi.org/10.1145/3359183 <accessed 12 October 2023>

**Learning for consumer protection:** As was the case for the Amazon AI fake review detector earlier in this section, this demonstrated a new approach to detection of dark patterns, with a methodology that could be used by consumer protection stakeholders including regulatory agencies to track dark patterns.

## C. Main findings from the public authorities and private institutions' case studies

Consumer protection agencies are somewhat behind the curve. The data, both from other agencies' use of technology in supervision, regulation and enforcement, and from industry and further afield shows that some use of technology already exists beyond generation 3. It has been embedded for some time notably in financial services and in intellectual property. Most actors in this section on cross-fertilisation have developed and rolled out more sophisticated tools. Whereas we had found use of AI up to Generation 3 in 66% of consumer agencies featured (with the caveat that the sample is not fully representative but ought to give a good sense of the direction of travel), our cross fertilisation sample shows that AI is used much more, although here again the size of the sample makes it difficult to conclude beyond noticing a trend. AI is used in 87% of cross-fertilisation case studies (13 out of 15), with 66% at Gen 3 and 94% at Gen 3 or above (with one case in Gen 4 and one case in Gen 5 as the highest). This reveals a practice gap, which can be explained by a lag in pre-existing expertise and availability of data in consumer agencies.

Many of the techniques consumer agencies are piloting have been tested and rolled out in other sectors and so there is an opportunity for the field of consumer protection to apply the most appropriate learning from other sectors, both public authorities and the B2B tools in use by companies.

Learning could come in the form of advice from other authorities on how to champion EnfTech within an organisation, or the best way to set up a data and technology unit. As publicly funded authorities, they are likely to face similar resource, time and institutional challenges. Learning could also be more direct, for example by using code developed in academic or enforcement settings and applying it to consumer protection tasks.

Looking beyond public authorities and into private uses of enforcement can give a different view - tools to protect their platforms have been widely in use where brands stand to lose out financially such as in counterfeiting and copyright infringement, or where criminal activity causes immense harm to vulnerable people such as CSAI (child sexual abuse image detection).[128] The private sector has driven the honing of fast, automated surveillance and the

[128] For example, the Internet Watch Foundation 'IntelliGrade' tool was designed in response to the proliferation of illegal images of child sexual abuse online. The tool enables our analysts to accurately grade images and videos, and create a unique #hash (a type of digital fingerprint) that is compatible with child sexual abuse laws and classifications in the UK, US, Canada, Australia, New Zealand and the Interpol Baseline standard. Once an image has a unique fingerprint it can be removed everywhere, even if images have been edited. IntelliGrade from the Internet Watch Foundation | IWF

development of innovations such as Digital Product IDs which are only now being legislated for. Whilst the end goal will be different, the technology will work for both private and public interests.

# 6. Key challenges in the roll-out of EnfTech

Using EnfTech in enforcement practice does bring many benefits notably in terms of augmenting institutional capacity response and streamlining operations. However, the use of technology in enforcement also does come with pitfalls. The research work conducted for this report did not investigate pitfalls specifically. The below is thus only an overview of the pitfalls identified and is by no means exhaustive. We identified two main categories of risks: Generic risks that relate to the roll out of EnfTech in general and some risks that may vary according to the technology being deployed. We note that the two categories under which we have organised and highlighted the problems that enforcers may face are not hermetically sealed and that problems tend to link into one another. It is therefore perhaps more useful to think of a 'web of problems' to ensure connections are made and implications are drawn where necessary when reflecting on how to roll out EnfTech.

Before proceeding with unpicking those risks, it is worthwhile noting that while this report seeks to promote the adoption of EnfTech, we would be concerned if technology were limited to simply placating the deficiencies of the legacy systems of enforcement. It may indeed be tempting to seek efficiencies through technology, digitising clunky processes, but we suspect that results would be  largely disappointing. Therefore, rolling out EnfTech ought to be an opportunity to reflect on more transformative options. Although consumer agencies may not always be able to influence the legal frameworks available to them nor the allocation of budgets, they may need to carry out such broader reforms in due course. In this process however, 'perfect should not be the enemy of the good' and some tech fixes to enforcement mechanisms may be a way forward for many consumer agencies pending more thorough reforms.

## A. Generic Risks of using EnfTech

Changing the way enforcement works to make it more effective does come with a number of challenges. The list below is not exhaustive but reflects the problems agencies can face and that we came across in our research. This list of problems offers a good starting point to reflect on how to ensure the effectiveness of the roll out of EnfTech, and avoid or minimise errors, learning from the experience of others and from a large field of academic research.

### i. The choosing the right tech for the right task problem

This report offers a framework to map out what technologies are available and reflect on already successful applications in a consumer law enforcement set up. It does not dwell on how to select the right technology. This is the remit of technologists. What the research shows is that sometimes, the job of enforcing law can be done well with some low key technology. There is no need to reach for AI at every turn. This is encouraging as it makes EnfTech accessible to a large number of agencies even if they do not have many resources. It also enables agencies to start small while they build up capacity and understanding. But choosing technology well is a first and essential phase. Agencies will therefore need to have a clear vision and understanding of their goals and how they can get there, which will include some good understanding of the technologies available and how they can be harnessed to solve consumer enforcement problems. This will include some time reflecting on:

- what tasks need to be performed: is a given option the best technology to use to perform this task? Or can something lower tech do the job just as well?
- who will be charged with overseeing the development as well as utilisation of the tool?
- how does the data need to be collected?
- what evidence needs to be kept?
- what resources does the agency already have?
- what experience of this type of task already exists and how successful have they been?
- cost-effectiveness;
- likely time reallocation during development phases, etc.

### ii. The privatisation problem

Where agencies are not able to staff or resource technical solutions, they may try to use external providers as well as rely on 'off-the-shelf' technical solutions. Relying on an externally developed system can be a way to cut through some obstacles to the roll out of EnfTech. Indeed, it can ensure an authority develops a viable tool where it lacks in-house expertise or where the development of a particular tool would not be economically viable. Some public agencies which normally need to adhere to strict rules may find that 'procurement, building, testing and implementing technology solutions may take longer than it would in a private enterprise.'[129] However, going down the procurement route also brings some challenges which are not unique to consumer enforcement authorities. Outsourcing may not be the panacea. For example, the novelty of technology driven applications as well as unfamiliarity on both sides of the system – the supervisory agencies' procurement offices and technology vendors[130], may make delivery arduous. But relying on external, proprietary systems is more likely where AI is the tool of choice as agencies could lack the budgets (and technical capacity) to develop and train AI systems from the ground up.[131] There some issues pertaining to training data or even accessing it in the first place may perpetuate already established asymmetries. Indeed, the amount of data and

[129] Dirk Broeders and Jermy Prenio, 'Innovative Technology in Financial Supervision (Suptech) - the Experience of Early Users' (Financial Stability Institute 2018) FSI Insights on Policy Implementation n9 22.

[130] Dirk Broeders and Jermy Prenio, 'Innovative Technology in Financial Supervision (Suptech) - the Experience of Early Users' (Financial Stability Institute 2018) FSI Insights on Policy Implementation n9 22

[131] Catalina Goanta and Jerry Spanakis, 'Discussing The Legitimacy of Digital Market Surveillance' [2022] Stanford Journal of Computational Antitrust 44.

computing power required to build effective AI models is often held by or is only accessible to a small number of very large multinational companies, meaning they have an entrenched advantage in training and developing the technology[132] which may well lead to authorities having to rely on their tools in order to deploy effective enforcement. Goanta and Spanakis therefore warn of public authorities remaining tech users rather than becoming tech makers.[133] There may be the potential for the public enforcement function to become dependent on privately provided expertise, with public responsibility and oversight neutralised by the lack of in-house knowledge.

### iii. The arms race problem

Much of the technology deployed to break or circumvent consumer law rules is also technology needed to enforce legislation. There is therefore a risk that the subjects of enforcement have the ability to 'game the system' and avoid detection. This could be done for example, by the use of self-destructing encrypted data making evidencing practices almost impossible.[134] Cao and others also found that the increase in the use of AI has led to a change in the way firms prepare filings, making them friendlier to machine parsing and processing. But with this also comes the avoidance of 'words that are perceived as negative by computational algorithms, as compared to those deemed negative only by dictionaries meant for human readers'.[135] This manipulation of data is problematic in an enforcement context. Enforcement authorities may have legal obligations of transparency[136] meaning that the tools they use in enforcement may have to be shared with business or at the very least some elements of their enforcement strategy may need to be public. When it is the case, there is a risk that companies can gain prior knowledge and use this knowledge to adapt their technological responses. Meanwhile, enforcement agencies may also not have direct access to the data they wish to audit to find evidence of wrongdoing, compounding the asymmetry between firms and enforcers.

### iv. The skills capacity problem

The successful deployment of EnfTech does require a modicum of technological expertise. The institutional research conducted did highlight the fact that some agencies were actively

[132] See for example, UK Government Office for Science, Large-scale computing: the case for greater UK coordination A review of the UK's large-scale computing ecosystem and the interdependency of hardware, software and skills, September 2021 UK_Computing_report_-_Final_20.09.21.pdf (publishing.service.gov.uk)
OECD, Measuring compute capacity: a critical step to capturing AI's full economic potential, February 2022 https://oecd.ai/en/wonk/ai-compute-capacity; N Ahmed, M Wahed,
[2010.15581] The De-democratization of AI: Deep Learning and the Compute Divide in Artificial Intelligence Research (arxiv.org)

[133] Catalina Goanta and Jerry Spanakis, 'Discussing The Legitimacy of Digital Market Surveillance' [2022] Stanford Journal of Computational Antitrust 53.

[134] Sean S Cao and others, 'How to Talk When a Machine Is Listening: Corporate Disclosure in the Age of AI' [2020] SSRN Electronic Journal <https://www.ssrn.com/abstract=3683802> accessed 22 March 2023.

[135] Sean S Cao and others, 'How to Talk When a Machine Is Listening: Corporate Disclosure in the Age of AI' [2020] 35, SSRN Electronic Journal <https://www.ssrn.com/abstract=3683802> accessed 22 March 2023.

[136] For an example in the EU under the DSA and DMA, see Edelson, Graef, Lancieri, Access to data and algorithms: for an effective DMA and DSA implementation (CERRE, March 2023) CERRE https://cerre.eu/wp-content/uploads/2023/03/CERRE-Access-to-Data-Algorithms.pdf accessed 05 October 2023.

recruiting technologists (in different specialisations). Attracting talent to the public sector may be a first challenge. Pay tends to be lower than in the private sector. And talent may not be drawn to the public sector as it will not traditionally be regarded as cutting edge. However, the CMA in the UK reports that recruitment has been on the whole a positive experience by:

- conducting large employee searches (advertising different roles at the same time);
- emphasising the societal benefits that come with being a part of regulating big tech in advertising jobs;
- emphasising the information gathering powers the agency has and thus the ability to work with data no other entity has access to, making it attractive and exciting work for technologists.[137]

However, hiring staff with the right mix of expertise is a challenge and the CMA has found that there is only a thin labour market for the skills required to make a good enforcement agency technologist.[138] Technologists normally want to use their core skills. They tend to have limited interest in or ability for qualitative (as opposed to quantitative) work or regulatory work as well as managerial roles. Thus multi-disciplinary teams may also be required. Indeed, the CMA investigating Facebook and Google's advertising quickly discovered that data scientists and engineers were not keen to embed into the case load as this was mostly qualitative work with which they were unfamiliar. They preferred to remain working with data and coding.[139] This does pose some challenge for retention as enforcement agencies cannot necessarily offer much career progression at this stage of development of their teams.[140]

For agencies that will need, or prefer to outsource, staffing is also a relevant issue because in-house staff need to have sufficient knowledge and a good working relationship with the developers to shape tech tools fit for purpose. There would therefore need to be some investment made in skilling up some existing staff or recruiting new staff able to interface with the technologists used in deployment. Consultants offering their services will also require some upskilling because there is at present no company that seems to specialise in EnfTech and thus, it is likely that no external company can be relied upon to fully understand the needs of consumer law enforcers (although some may be servicing SupTech or RegTech).

### v. The agency culture change problem

The roll out of new tools is often met with resistance. Staff may worry that the arrival of technology makes them redundant or may do so in future. Staff may struggle to understand the process or the tool that is available to them. With any new technology roll out, there is indeed a learning curve and often difficulties linked to the adoption of tech tools that may not always be intuitive to use.

[137] Hunt (ftn 43) 37.
[138] Hunt (ftn 43) 38.
[139] Hunt (ftn 43) 37.
[140] Hunt (ftn 43) 38.

### vi. The legal challenge problem

Not all legal systems may allow for evidence to be gathered by a machine[141] or even for detection to take place other than by the intervention of an enforcement officer. To a large extent, the use of IT in enforcement is now well established and use of first and second generation EnfTech tools are unlikely to lead to too many problems. But the rolling out of EnfTech may open agencies to some legal challenges that agencies need to factor in when developing their EnfTech strategies. This being said, it is possible to use technology and continue to have human oversight in order to minimise the risks of a legal challenge. However, the more an agency is willing to travel towards the 3rd and 4th generation of EnfTech, the more likely it is that challenges will follow.

Where authorities are going down the path of AI many potential issues may come to the fore and increase the likelihood of legal challenge unless the development and review as well as operation of the AI is well thought out. Indeed, there could be many factors that make AI-assisted decisions easy to question in court.

Thinking of legal challenge risks should not deter agencies but help them strategize how to ensure their efforts are not annihilated by procedural oversights in the bid to adopt new technologies.

Legal challenges may focus on a range of issues, including exposure to violation of data privacy laws for example in the collecting of data from social media sites to investigate consumer issues; or using proprietary data through APIs. One key challenge for enforcement agencies is indeed to have access to back end data in order to detect any violation or assess their scale.

Ensuring all the relevant and correct legal permissions for using data for the purpose of enforcement will need to form part of the agency's strategy.[142] On this aspect, regulation may be required to avoid any bottlenecks in enforcement with companies refusing to share data which may be used in assessing their behaviour.

For example, in the EU, the Digital Services Act and Digital Market Act include a range of obligations (a total of 54 algorithmic and data sharing obligations across the DMA and DSA) to enable data access and transparency for a variety of objectives, including verifying legal compliance, to increasing market contestability, to enabling a better understanding of how algorithms and advertising systems impact our societies.[143] These include obligations specifically designed to give regulators access to the data which establishes and in some cases expands the powers to require access to private data for investigations or other public

[141] See Paul W. Grimm, Maura R. Grossman, Gordon V. Cormack, Artificial Intelligence as Evidence (2021) 19 Nw. J. Tech. & Intell. Prop. 9, https://scholarlycommons.law.northwestern.edu/njtip/vol19/iss1/2/ accessed 10 October 2023.

[142] Dirk Broeders and Jermy Prenio, Innovative technology in financial supervision (suptech) – the experience of early users, FSI Insights on policy implementation, Bank for International Settlements, July 2018.

[143] Edelson, Graef, Lancieri, Access to data and algorithms: for an effective DMA and DSA implementation (CERRE, March 2023) https://cerre.eu/wp-content/uploads/2023/03/CERRE-Access-to-Data-Algorithms.pdf accessed 05 October 2023.

purposes.[144] In Australia, the ACCC also has powers to request algorithms code for investigative purposes[145] and through this power were able to uncover wrongdoing in a range of cases.[146]

## B. Specific risks in the deployment of EnfTech based on AI

Artificial Intelligence is one of the most discussed technologies in recent years. It is relatively well established in SupTech and RegTech and rapidly expanding. Enforcement agencies have also started to experiment with it. Its use will bring specific risks, many of which are discussed in relation to AI generally: ethics, social and security risks as well as its impact on the environment[147] which we are not addressing in this report. Instead we focus on the problems we uncovered in our specific study of the use of AI in enforcement of consumer rights. The key issues highlighted below include (in no particular order) problems related to: 'hype', data quality and quantity, opacity, the risk of discrimination and the temptation to go first to 'low hanging fruit'. Those problems are raised in relation to the use of AI but some may also be thought of as generic.[148]

### i. The hype problem

One important risk pertains to responding to the hype generated around AI without a solid and well thought out strategy to roll it out. The building and deployment of an AI detection system may be extremely costly and protracted if the authority in question does not have adequate funds, datasets or expertise to tap into or even reliable electricity supply. Its return on investment may equally be poor if it is devoid of useful data to work from or its training and deployment is not well thought out. In those situations, and in line with the generational framework above (part 3), resources may be better invested in earlier forms of technology, with a view to feed data and acquired expertise to a future project. At this stage of EnfTech development, it is essential to see past the hype, to focus on how to build effective resources to assist in enforcement tasks.

[144] Edelson, Graef, Lancieri, Access to data and algorithms: for an effective DMA and DSA implementation (CERRE, March 2023) https://cerre.eu/wp-content/uploads/2023/03/CERRE-Access-to-Data-Algorithms.pdf accessed 05 October 2023.

[145] Competition and Consumer Act 2010, section 155.

[146] See for eg, ACCC v iSelect [2020] FCA 1523 concerning false claims concerning best electricity deals; ACCC v Trivago N. V. [2020] FCA 16 for misleading consumers on hotel rooms rates; ACCC v Uber B.V. [2022] FCA 1466 for misleading representation about taxi fares and cancellation fees.

[147] The sum of the machinery and energy required to run AI-enabled technology is growing and in many respects this report encourages this trend. But such use does have an environmental footprint across a broad lifecycle, which at today's date is not easily quantified or quantifiable according to the OECD but will require some careful planning to make is sustainable (see OECD, 'Measuring the Environmental Impacts of Artificial Intelligence Compute and Applications: The AI Footprint', vol 341 (2022) OECD Digital Economy Papers 341 35 <https://www.oecd-ilibrary.org/science-and-technology/measuring-the-environmental-impacts-of-artificial-intelligence-compute-and-applications_7babf571-en> accessed 9 March 2023.

[148] Eg: low hanging fruit. It is possible that some agencies will remain in a generation of technology they know well and do well to get results and demonstrate efficiency, where in fact being more ambitious and moving up the generations may be more beneficial.

Interestingly, even at those consumer agencies that could be deemed to be leading the way into a technological approach to consumer enforcement, AI is not always the tool of choice. Instead AI appears to be part of a menu, a selection of technologies. As our case studies attest, solutions in consumer enforcement can be delivered through a range of tech tools, including automated processes driven by algorithms, while some tasks may require statistical techniques from data science. Besides, AI is a generic term and often remains a misnomer because the many AI solutions that at today's date are performant are limited to repetitive tasks with clearly defined outcomes and thus cannot be relied upon to solve all enforcement woes. However, there is room for AI to take on more analytical roles and help in the shaping of consumer enforcement in a different direction notably with machine learning and neural networks able to crunch huge amounts of data, sniff out complex patterns and deal with statistical issues, enabling prediction as well as detection.[149]

### ii. The data quality and quantity problem

AI can accomplish some very useful tasks, but it has limitations. One key issue with AI is its appetite for data. AI cannot function without data. We have already discussed how consumer enforcement agencies do have data but may lack the sufficient volumes of meaningful data needed to train and develop AI tools (see part 3, section B). However, data does not simply need to be abundant. It also needs to be of good quality and much resources do in fact go into data preparation and cleaning[150] although some preparation can now also be done with the use of AI itself. Without clean data, many more risks await. For example, this may include wrong results (AI is only as good as the data it is fed) or worse, discrimination if the data is skewed.

### iii. The opacity problem

Opacity in AI is rooted in the technology itself as well as a range of other factors. Some strands of AI are not programmed by a human to execute specific code. The system is simply programmed to teach itself a course of action out of the available data. This means that the role of the human programmer is minimised. While machine Learning can significantly augment human capabilities, detecting patterns and making meaningful correlations from data to help enforcers make decisions, it also arrives at conclusions without its programmer being truly able to explain how a decision was made.[151] It is the ability to adapt without human intervention (as

[149] C Riefa, L Coll, The use of AI in the Enforcement Technology (EnfTech) toolbox: is AI a friend or a foe? in Larry Di Matteo, Cristina Poncibo, Geraint Howells, *AI and Consumers* (Cambridge University Press, forthcoming 2024).

[150] Cleaning data occupies 80% of the time spent by data scientists and is the least enjoyable part of their job, according to: Gil Press, 'Cleaning Big Data: Most Time-Consuming, Least Enjoyable Data Science Task, Survey Says' (*Forbes*, 23 March 2016) <https://www.forbes.com/sites/gilpress/2016/03/23/data-preparation-most-time-consuming-least-enjoyable-data-science-task-survey-says/> accessed 9 March 2023.

[151] Alessio Azzutti, Wolf-Georg Ringe and H Siegfried Stiehl, 'Machine Learning, Market Manipulation and Collusion on Capital Markets: Why the "Black Box" Matters' [2021] SSRN Electronic Journal <https://www.ssrn.com/abstract=3788872> accessed 16 March 2023.

the AI learns from the data) which makes it 'qualitatively different from previous technological advancements'.[152]

This opacity also called the 'black box' problem creates a real challenge in an enforcement context. It makes the process of enforcement rather difficult as many AI used by companies may not be 'explainable' and thus it may make the detection of wrongdoing more complex for enforcement agencies. Opacity may also derive or be compounded by other factors, such as a bi-product of a lack of specialised skills or because of concealment activities by firms being investigated.[153] This can be controlled in part by adequate staffing strategies whereby staff have expertise in unpicking and interrogating how AI systems are used (often the by-product of having the right skills to develop AI in the first place).

Conversely, agencies that employ AI to assist them in their tasks may find that basing decisions on unseeable and unknowable factors leaves an enforcement authority with blind spots on how to improve enforcement mechanisms and unable to easily identify potential issues with the underlying data or the way the AI interprets the data. It also may leave the authority open to challenge and so undermine the process of enforcement. Enforcement authorities may be accountable for the proper functioning of AI systems and for respecting some key principles in its use of AI.[154] The question of liability is not yet settled, but it is likely to follow the 'AI creator', commensurate with role, context as well as state of the art. It would thus be the AI creator's responsibility to design, install, and monitor processes that include documenting AI system decisions, conducting or allowing auditing, and providing adequate response to risks and redress mechanisms where justified.[155]

### iv. The potential discrimination problem

The risk of discrimination in the use of AI is more or less omnipresent.[156] Consumer protection authorities will thus need to be alert to bias and ensure that skewed algorithms and discrimination in enforcement is guarded against. Discrimination may be as a result of poor quality data or narrow and/or incomplete data sets. Discrimination in enforcement may for

[152] Commission Staff Working Document, Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (AI Act) and Amending certain Union Legislative Acts SWD/2021/84 final.
[153] Jenna Burrell, 'How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms' (2016) 3 Big Data & Society <https://journals.sagepub.com/doi/epub/10.1177/2053951715622512> accessed 16 March 2023.
[154] Such as for example, OECD, 'Recommendation of the Council on Artificial Intelligence' (2022).
[155] OECD, 'Recommendation of the Council on Artificial Intelligence' (2022) 7.
[156] For example a well documented risk is that of correlation over causation according to which an AI tool may find correlation and assume causation where they may not in fact be a connection. On this issue, see for eg, Rohrer JM. Thinking Clearly About Correlations and Causation: Graphical Causal Models for Observational Data. *Advances in Methods and Practices in Psychological Science*. 2018;1(1):27-42. doi:10.1177/2515245917745629; *"On one hand, algorithms may single out borrowers who are already disadvantaged as bad credit risks, thereby exacerbating existing inequality. On the other hand, lenders may be able to provide loans to disadvantaged people if (and only if) they can accurately price credit risk. This could particularly impact borrowers who are on low incomes, and who are less likely to get approved for credit. These borrowers often seek out alternative providers such as payday lenders, and end up paying much higher interest rates".* See Fuster, Andreas and Goldsmith-Pinkham, Paul S. and Ramadorai, Tarun and Walther, Ansgar, Predictably Unequal? The Effects of Machine Learning on Credit Markets (June 21, 2021). Journal of Finance, Forthcoming, <https://ssrn.com/abstract=3072038 or http://dx.doi.org/10.2139/ssrn.3072038> accessed 03 May 2023.

example manifest itself by the recurrent flagging of particular types of companies or practices for investigations which may omit a larger market view and thus skew enforcement efforts.

Similarly, relying on consumer complaints data to prioritise enforcement could carry bias, because most complaints may be put forward by a particular type of consumer or may be as a result of particular campaigns, and thus  are unlikely to represent the experiences of all consumers, for example those who face certain disadvantages.[157] Hence missing infringements that may be worthy of intervention and misrepresent  the understanding enforcers have of the markets they oversee. The discrimination problem links back to data quality as a key problem in enforcement using AI.Avoiding these risks will involve monitoring the way the AI system develops in terms of data quality and testing/ training protocols. Authorities would also need to rely on the judgement and experience of staff to understand and question why particular conclusions might be reached and reviewed periodically.

### v. The low-hanging fruit problem

Using AI well can be difficult. As AI gathers pace and enforcement authorities feel the need to modernise their enforcement techniques (linking back to the hype problem), there is a risk that only easy to do solutions will be developed leaving much consumer harm unchecked. This can also be linked to discrimination because there may also be bias if decisions about the activity that enforcers chose to prioritise is led by the availability of data and the ease of analysis and not by broader prioritisation criteria.[158]

There is also a risk that some companies or types of practice may be overrepresented in enforcement activity because developing AI solutions to combat those practices are easy to do rather than because they are causing the most harm.[159] This may cause a risk to the needs of under-represented or vulnerable groups of consumers who may find their problems de-prioritised for lack of meaningful data to feed the AI or because they are not the most efficient issue for enforcers to address as they may require more capacity in the AI solution to have a more nuanced and granular approach.

[157] see for eg, A survey of UK consumers by UK consumer ministry BEIS in 2022 found that younger consumers (especially aged 18-39) and consumers in difficult  financial situations were consistently more likely to experience detriment and yet would not to take actions and suffer the most negative consequences compared to other groups.See Consumer Protection Study 2022 “Understanding the impacts and resolution of consumer problems” BEIS Research Paper Number 2022/005 accessed at 26 April 2023 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1068864/consumer-protection-study-2022.pdf

[158] C Riefa, L Coll, The use of AI in the Enforcement Technology (EnfTech) toolbox: is AI a friend or a foe? in Larry Di Matteo, Cristina Poncibo, Geraint Howells, *AI and Consumers* (Cambridge University Press, forthcoming 2024).

[159] Dries Cuijpers, comments at EnfTech event “Potential biases towards specific topics and ‘simple’ violations” Using Tech in Consumer Enforcement, ACM’s experiences, Dries Cuijpers, ACM, Netherlands presentation at ‘Introducing EnfTech: a technological approach to consumer law enforcement 20 April 2023’ by Dries Cuijpers, Senior Enforcement Officer, Authority for Consumers and Markets, Netherlands, https://static1.squarespace.com/static/638646cea1515c69b8f572cb/t/64478512565ae2428ba15ecd/1682408723189/ACM_NL_Dries+Cuijpers.pdf accessed 05 October 2023.

# 7. Conclusion: the EnfTech way forward

Businesses engaged in the delivery of digital services and products, consumer facing platforms and e-commerce have embraced technology (from cookies to machine learning and AI) to track, predict and influence consumer behaviour and choice. So far however, national enforcement agencies have remained timid towards incorporating technologies in their daily work to monitor and detect wrongdoing. Fighting the excesses of technology with yet more technology may seem counterintuitive. Yet, 'tooling up' no longer appears an option or a useful add-on. It is quickly becoming an essential aspect of enforcement in today's largely digitised consumer markets.

EnfTech has the potential to change the way consumer law is enforced. While enforcement agencies are by and large proactive in their enforcement approach, they are limited in their capacity to act. This necessarily leaves some harm unchecked meaning that enforcement often appears reactive (with interventions being rolled out after the harm is experienced by consumers) or altogether lacking. The use of EnfTech in enforcement can boost the efforts of agencies. It can enhance their capacity to act, enabling them to sanction wrongdoing in real time (in the same way a speed camera would issue a fine). EnfTech could also assist with moving enforcement to a largely proactive practice with intervention happening before the harm is even experienced.

With the right technology in place, enforcement agencies can make important gains. They can streamline their operations and be able to focus their human capital where it is most needed. Swifter discovery of infringements can in the short to medium term contribute to enhancing deterrence, and lead to significant reductions in infringements in the long term. This is particularly the case where EnfTech can work in tandem with technology deployed in other spheres, notably with RegTech, ensuring that companies compliance-check their activities before/ or as close as possible to when their products or services reach the market. A collaborative approach may indeed be the ultimate way to ensure consumers are treated fairly.

This report explored novel means of combating wrongdoing through a technology-assisted approach, adding valuable understanding of current activity and of the different types of technologies in use for particular enforcement tasks or goals. An important added value is the listing and documenting of real use cases of technology in consumer enforcement (18 use cases) alongside an inventory of case studies from other disciplines and actors that could be adapted for consumer enforcement. This includes 7 case studies in public authorities' in related fields and 8 case studies from private and other institutional settings.

The study is aimed primarily at newcomers to the field of EnfTech, but agencies at all levels of developments may regard the findings of use. The research revealed that while the use of technology in consumer law enforcement is still in its infancy, it is, however, developing at a fast pace, in a small, yet significant number of agencies. The set up employed by those consumer agencies varies and there is no 'one size fits all' model to accommodate the roll out of EnfTech.

All agencies studied in this report have employed different models (in-house or outsourced or a mix of both), but all have managed to make gains, sometimes with very simple or readily available off-the-shelf technology. EnfTech tools therefore are not reserved to big agencies with sizeable budgets and can be rolled out in all types and sizes of agencies and at every stage of technological development.

The technologies employed by enforcers indeed are varied, although AI has occupied much of the discussions and attention in the most recent past. The report assesses current use cases by reference to the EnfTech Generational framework which charts five successive generations of technology. Generation 1 rests on fairly basic tech, with data collected from paper based reports or emails and involves heavy manual processing and only performs descriptive tasks. As the use of technology develops and moves through the generations, the input of data becomes automated and the insights gained from this data are increasingly diagnostic (Generation 2) then evolve to rely on full automation and big data and can, at this stage, help with predictive analysis (Generation 3). Our data shows that currently the highest generation of tools used by enforcement agencies and covered in this report is Generation 3.

The data also points to the acceleration of the use of AI in consumer enforcement. However this result needs to be put into context. Our survey sample is small and focuses on agencies that are already ahead of the game and thus would have had the ability and experience to progress through the generations at a faster pace. Nevertheless their experience will be invaluable to any newcomers to the field. Another important gain would be to develop and agree a more standardised approach to the use of AI in consumer enforcement to also facilitate cross-border enforcement.

Advances in technology will make possible the use of tools feeding on big data architectures and offer real-time monitoring with more advanced AI techniques (Generation 4) than the ones that are currently being rolled out. Generation 5 would cover technology that builds on existing generations and moves away from assistive and partial automation of tasks towards fully machine-enabled delivery of decisions. Our study of use cases in related fields as well as in industry revealed a gap with consumer enforcement practice. Our cross-fertilisation case studies feature use of technology in generations 3, 4 and 5. They are thus more advanced and confirm the trend for reliance on more AI tools.

Perhaps the primary obstacle to consumer enforcement agencies engaging with generations 3, 4 and 5 is the availability of data, followed by the lack of an appropriate legal framework.

For AI to lend a hand it needs a lot of good quality structured and unstructured data. Because of historical set up, most consumer agencies will not yet have all the required data sets and will need to develop strategies to build them and/or acquire them. There may even be a need to mandate by law that private entities respond to demand for data during investigations. In spite of these difficulties, we have seen quick uptake of AI amongst agencies already active in EnfTech.

Our study found evidence that AI can be a very useful technology to deploy, but it is not the only one, nor is it always going to be the solution to all enforcement problems. Approaching it therefore requires caution and a lot of learning. However, if deployed correctly, AI shows promise in improving consumer enforcement. In the foreseeable future, human intervention in the deployment of AI will no doubt remain indispensable. However, as technology develops, human time, skills and judgement can progressively be freed up to focus on more intricate (and interesting) parts of the job, while machines can take over the most repetitive and time consuming tasks.

But to get to this stage requires some management buy-in and resources being deployed to prepare the ground for a technological roll out in agencies. EnfTech will require growing more than just technological capability, it will need confidence and capacity across the organisation for example from legal teams and procurement units.

All EnfTech roll out carries with it some challenges and agencies will also need to work through a list of problems (some general issues, others very much technology specific). For example, agencies will need to grapple with choosing the most appropriate technology to fulfil their needs, and choose whether outsourcing to privately provided expertise is the best route or if they are able to attract and retain the right level of skills in-house and foster a culture that embraces the change to EnfTech. Agencies will need to reflect on the response companies will have to their upgraded enforcement tools and how they may seek to circumvent detection. On the legal side in particular, one important risk that comes with deployment of EnfTech is that of an absence of an appropriate legal framework. From this, it is likely that companies that are the target of investigations or sanctions may wish to explore the possibility of challenging the legality of decisions and enforcement processes if they cannot be fully accounted for and justified. If AI is the technique of choice, more specific risks await ranging from avoiding the hype and ensuring AI is able to deliver what is needed rather than what is easy to achieve, having the right data to feed it and avoiding any discrimination in the way the system is built and rolled out. While none of the problems that present themselves appear insurmountable, they need to be addressed in order to ensure that the use of technology is a legitimate and worthwhile addition to any consumer law enforcement strategy.

Fast forward a few years, EnfTech ought to be making its way into the work of all agencies, building data sets in the first instance, followed by skilling up to meet the demand of a technological approach to consumer law enforcement. To ensure agencies can effectively master technology they would also benefit from collaboration and the sharing of best practices, as well as sharing what did not work - to avoid repeating costly and time-consuming steps that did not deliver as planned. In that sphere, the latest developments in ICPEN, UNCTAD and the OECD are encouraging, giving time for dialogue and experimentation not just within national borders but also across borders.

How to proceed with EnfTech will depend on pre-existing institutional setups and local regulatory and enforcement cultures. These are inevitably influenced by the wider regulatory and enforcement environment, and we might consider how that could potentially encourage the sustainable and effective development of EnfTech. Designing EnfTech in a way that works across borders will be vital for protecting consumers active in today's global, digitalised markets. This requires improved international cooperation in areas like cross-border data flows, shared taxonomies, databases structure for recording issues and using shared approaches to turning law into code. Institutions such as OECD, ICPEN and UNCTAD are again critical here in that they can provide a venue for discussions around those themes to take place and lead to the adoption of key documentation.

Consumer authorities and other organisations who prioritise consumer protection can also be mindful of where new powers might unlock EnfTech. For example, they could work with those crafting new digital regulations to secure access to appropriate transaction data flows that can be used for the purposes of monitoring and enforcement.[160]

In addition to guidance on shared structures for data and monitoring, collaboration can also produce principles and guidance on the use of technology in enforcement, in the case of employing AI this might require describing the safeguards needed to make sure it is used in a way that produces robust and interpretable results.

EnfTech is an opportunity to change the enforcement infrastructure in consumer markets. It's not simply about tools but about a whole new organisational approach to enforcement - one that is ex ante and that incentivises fairness by design. If EnfTech can become a force to be reckoned with then consumers will gain - and that would be truly transformative.

[160] For example, proposed EU regulation on Digital Product Passports could enable the third-party verification of product data so a green claim can be immediately checked against information on a central database

# Annexes

## Annex 1 - Technologies and data: terms in use

The generational model developed in this report is useful for locating the range of technologies and data streams available for use in supervision and enforcement and appraise the potential of Enftech. It uses some technical language in the description and discussions of the different models. Similar language is also used in the case studies contained in this report. As written for non-technical experts, the report inevitably uses terminology that may be unfamiliar to the reader. This annex provides some brief definition of the main terminology used in the generational model and in the subsequent case studies. It is important to remember that an array of technologies are in evidence in EnfTech which work independently or alongside each other to support or deliver enforcement functions.

**Big data:** describes data sets that are simply too big to be managed by a human or by simple computing. These large datasets came about with the growth of data collection from the increase in online activity and digital footprints and more public and private bodies collecting and holding data.  Big data can be made up of structured or unstructured data, both types have grown in the last 20 years.

> **Structured data** can be easily categorised and searched, for example product IDs, bar codes, phone numbers or dates.
>
> **Unstructured data** includes emails, texts, videos or photos etc which are harder to organise and search.

**Algorithm**: an algorithm is a set of instructions that can perform a computation or carry out a task. They can carry instructions as simple as ‘if-this-then-that’ (eg product recommended on a website because a similar purchase was made) or be more elaborate and based on a complex set of mathematical equations, rules and calculations. Algorithms also power many other compliance and enforcement functions for example, the automated processing of reporting reminders or to update and inform entities of new activity. Algorithms have traditionally been written by a human programmer.

**Data Science**: is an interdisciplinary field concerned with extracting information from data. Data science investigates, develops and uses scientific methods, processes, and systems to extract knowledge and insights from data. Techniques might include more traditional statistical analysis or more advanced techniques such as artificial intelligence approaches like machine learning.[161]

**Artificial Intelligence (AI):** is a broad discipline which has been around since the 1950s. It describes a collection of advanced software technologies and applications that allow machines

[161] Hunt, S, 2017: From Maps to Apps: the Power of Machine Learning and Artificial Intelligence for Regulators from-maps-to-apps.pdf (fca.org.uk) accessed 20 July 2023

to simulate different aspects of human intelligence, most critically learning and decision-making. The type of AI attracting attention and scrutiny today is a particular type called Machine Learning which has become so prevalent that the terms AI and machine learning tend to be used interchangeably.

**Machine Learning i**nvolves vast amounts of data being fed into a 'learning algorithm' that can find patterns and rules within it and then use those rules to make predictions. This differs from other types of algorithms which are not programmed to learn, but only to carry out a task (see **Algorithm**). Machine learning at the scale we recognise today only became practically possible with the availability of **Big Data**. Types of machine learning:

**Supervised machine learning** is the most common type of machine learning. Models are trained to learn from labelled data sets and to map relationships between data. For example an algorithm would be trained to spot the words 'lottery' or 'you've won' in emails and classify them as either spam or not spam. Supervised machine learning algorithms can be tasked to learn from past events and predict new ones.

**Unsupervised machine learning** involves the programme looking for patterns in unlabelled data. Unsupervised machine learning is powerful as it can find patterns in data that may not have been identified before, because a human programmer may not have considered them or been able to consider them due to the large volume of information to analyse.

**Reinforcement machine learning** uses trial and error to train a model by rewarding the most optimal way to complete a task. In this way, it learns over a series of attempts which actions are best. For example, a warehouse robot might be trained with reinforcement learning to find the most efficient way to navigate around the warehouse, gaining rewards for shorter time taken.[162]

**Deep learning systems** and **Neural Networks** are closely related types of machine learning that use more advanced techniques to teach themselves to deduce and reason in ways that mimic the multi-layered neural networks of the human brain. Neural networks have now reached notoriety with deep learning being used in Natural Language Processing as part of large language models like OpenAI's ChatGPT, Google's Bard and Meta's LLaMA. Deep learning such as this brings specific challenges because the algorithms required to crunch huge amounts of data, sniff out complex patterns and deal with statistical issues often become opaque and hard to interpret or explain.

**Natural Language Processing** gives the machine the ability to read, understand/ interpret human language. This branch of machine learning is what chatbots or our voice assistants rely on to converse with humans. The mainstream release of large language models and

[162] Those rewards are coded in 'rewards' - a signal that the machine knows what it has done is positive and their learning needs to continue that way. As opposed to being signalled that it is negative. See Leslie, David, Burr, Christopher , Aitken, Mhairi, Cowls, Josh, Katell, Michael and Briggs, Morgan, Artificial intelligence, human rights, democracy, and the rule of law: a primer (April 2, 2021) 8, available at SSRN: https://ssrn.com/abstract=3817999 or http://dx.doi.org/10.2139/ssrn.3817999, accessed 3 August 2023.

other AI systems capable of generating music, images or videos has brought a new category of AI into common discourse – these models are known collectively as **Generative AI.**

**Web scraping:** Web scraping is a term for gathering and copying of specific data from websites. Most commonly carried out by an automated process for example a web crawler, web scraping can collect data at a volume that can form a dataset for statistical analysis including machine learning analysis.

**Appliance Programming Interface (API):** facilitates communication between the software of two different computers or systems. This can enable companies to open up data and functionality within their application to external third parties. In enforcement terms, an API could be opened up and shared between a platform and an agency inspecting content on the platform.[163]

**Automated data reporting**: the automatic gathering of data from different platforms and integrating of reporting or transactional data into a regulatory system. This could involve two types of technology. Push technologies where pre-defined data is being delivered from the regulated entity to the regulator, and pull technologies where the authority can draw data from the regulated entity as required. Both require standardised formats for data, and APIs to allow submission and communications between entities.[164]

**Related advanced technologies:** other advanced technologies or processes such as **robotics, IoT** or **blockchain** are often employed to work with AI systems, but they are not the same thing. These advanced technologies can interoperate with AI systems but do not rely on them to function.

[163] One such use case for enforcing compliance is explored in Catalina Goanta, Thales Bertaglia, and Adriana Iamnitchi, The Case for a Legal Compliance API for the Enforcement of the EU's Digital Services Act on Social Media Platforms, In 2022 ACM Conference on Fairness, Accountability, and Transparency (FAccT '22), June 21–24, 2022, Seoul, Republic of Korea. ACM, New York, NY, USA, Article 111, 14 pages. https://doi.org/10.1145/3531146.3533190, accessed 03 August 2023.

[164] OECD, Business and Finance Outlook 2021: AI in Business and FInance, section 5, The use of SupTech to enhance market supervision and integrity, , https://www.oecd-ilibrary.org/sites/d478df4c-en/index.html?itemId=/content/component/d478df4c-en#back-endnotea5z6, accessed 03 August 2023.

# Annex 2 - Institutional Capacity for EnfTech

*Findings based on desk study, June-July 2023*

The below gives more details about the institutional capacity for EnfTech in a sample of consumer agencies. The agencies featured were selected because they were recognised in early and/or connected literature as leading the field.[165] That is not to say that best practice does not exist elsewhere.[166] Some background on institutional setups helps understand the various models available and evaluate what may best suit agencies new to the field as well as to benchmark progress. However, it is noted that institutional setups vary so much that it is not possible to infer from the below information what models may work best as this will likely come down to national preference and pre-existing structures.

Agencies in the USA, UK, Netherlands, Australia and Colombia have direct experience of technology assisting in consumer law enforcement. Agencies in France, Canada, Japan and Korea are mentioned in FTC documents as having embedded some tech in their practice[167] and there is evidence of interventions in competition law. However, we could not trace from official documents and desk research any consumer law interventions using technologists' contributions. Taiwan does not appear to have a specialised team, but there is a record of staff with a computer science background in the staff.

However, the fact that the tools and technologists are in post in either the same authority or a connected one[168] can lead to cross fertilisation to the consumer side. In this sense, we expect to find examples of EnfTech in consumer law soon as those countries would be uniquely set up to embrace technologies in consumer law enforcement having had experience in other fields, if they have not already done so.

## UNITED STATES

### **Federal Trade Commission (FTC)** www.ftc.gov

The FTC is directed by a number of commissioners working alongside its chair (currently Lina Khan) The FTC has 3 bureaus. Notably the Bureau for Competition and the Bureau for Consumer Protection, but there is also a bureau for economics. In addition to the Bureaus, a number of offices provide additional assistance and are very much the administrative backbone of the FTC.

[165] Most notably, Stefan Hunt, The technology led transformation of competition and consumer agencies: The CMA's experience, discussion paper (14 June 2022) referencing FTC, AdIC, CBC, ACCC, DG Comp, ACM and Stefanie NGuyen, A Century of Technological Evolution at the Federal Trade Commission (17 February 2023) referencing use in the UK, AUS, CAN, FR, Japan, Korea, Germany and Netherlands, https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/02/century-technological-evolution-federal-trade-commission accessed 3 July 2023; Also see 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' (2022),https://www.crossborderenforcement.com/

[166] In fact, in the case of SIC, EnfTech has been embedded since 2014, but had escaped notice and we came across interesting example of tech use almost by accident.

[167] See for example discussing best practices to justify the set-up of the Office of Technology at the FTC, https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/02/century-technological-evolution-federal-trade-commission accessed 30 June 2023.

[168] In France for eg, the institutions for competition and consumer enforcement are two different agencies.

There is for example, an office of the Executive Director, or an office of international affairs which notably supports cross border collaborations.

The FTC has had a Chief Technologist since 2011.[169]The Office of Technology (OT) was created in February 2023[170] to assist the Commission and support law enforcement investigations and actions; advise and engage FTC staff and the Commission on policy and research initiatives, engage with the public and relevant experts to understand trends and advance the Commission's work. The staff of the office is varied and includes software engineers, data scientists, artificial intelligence, machine learning experts. One of the goals of the office is to bolster wider specialisations and crossovers (promoting collaboration and coordination between technologists working at the agency and streamlining deployment of resources).[171]The team is centralised, uniting the expertise that sat in the specialised bureau of Competition (Technology Enforcement Division) and Consumer protection (OTECH - Office of Technology Research Investigation[172]) that now appear to have been disbanded.[173] OTECH was created in 2015 but remained dormant for a period of time (2018 to 2021) in the absence of a Chief Technologist in post.[174] It had a small staff of only a 'handful of employees' back in 2021, that had not been specifically recruited but shifted around from other departments.[175] The team is however growing with the recruitment of Technologists in Residence.[176] Technologists work across the agency, with attorneys and other staff to understand markets and business models. They help the FTC understand the technologies consumers interact with and keep pace with developments. They assist in asking for the right type of information and interpreting the information that may be provided to the Bureaus.[177]

Public information on The Bureau of Consumer Protection shows that currently this Bureau hosts 8 divisions in total specialising in different areas including one division of Enforcement and one Division of Litigation Technology and Analysis.[178] The Division of Enforcement litigates cases in civil and criminal courts. The Division of Litigation Technology and Analysis assists with

[169] https://www.ftc.gov/about-ftc/commissioners-staff/ftc-chief-technologists accessed 11 July 2023.

[170] https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-launches-new-office-technology-bolster-agencys-work accessed 24 June 2023.

[171] https://www.ftc.gov/about-ftc/bureaus-offices/office-technology accessed 23 June 2023.

[172] https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/our-divisions/office-technology-research-investigation accessed 30 June 2023.

[173] https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/02/century-technological-evolution-federal-trade-commission accessed 24 June 2023. Although note no announcements has been made and thus some uncertainty remains, as noted here: https://www.jdsupra.com/legalnews/ftc-s-new-office-of-technology-is-not-5157567/ accessed 29 June 2023.

[174] JK Wagner, The Federal Trade Commission and Consumer Protections for Mobile Health Apps 48(1 Suppl) (2020) J Law Med Ethics 103-114, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8329941/ accessed 11 July 2023.

[175] Consumer Reports et al, Letter to Majority and Minority leaders of the United States Senate and to Speaker and Minority Leader of the House of Representatives, in support of FTC Privacy funding (2021) https://advocacy.consumerreports.org/wp-content/uploads/2021/09/Group-letter-in-support-of-FTC-privacy-funding.pdf accessed 24 June 2023.

[176] https://www.ftc.gov/technologists accessed 30 June 2023.

[177] Stacy Procter, Counsel, International Consumer Protection, Federal Trade Commission, Office of International Affairs presentation at 'Introducing EnfTech: a technological approach to consumer law enforcement 20 April 2023' <accessed 12 October 2023>

[178] The others are: Privacy and identity protection, advertising practices, consumer & business education, marketing practices, consumer response and operations, financial practices. For more details, see https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/our-divisions accessed 23 June 2023.

the investigation and the litigation of consumer cases. This may include evaluating and/or managing tools to conduct the investigations. The Division is further subdivided into a number of units with different specialisations and including:

- digital forensic unit (identification, collection and analysis as well as keeping records for evidential purposes);

- e-discovery unit, which uses technological tools to process, organise, manage and produce electronically stored information[179];

- Tech lab which provides technical assistance in the use of innovative tools in investigation, and detection of unfair and deceptive activity and to secure relevant evidence of wrongdoing.

In addition a unit is charged with ensuring the Bureau of Consumer Protection's needs to fulfil its mission are catered for and the necessary technology to do so is available (technology planning).[180]

## UNITED KINGDOM

### Competition and Markets Authority (CMA)

https://www.gov.uk/government/organisations/competition-and-markets-authority

The CMA operates with a chief executive assisted by a Board, a Panel and some Committees.[181] The CMA deliver its mission through a number of units (some called Directorates, others offices) including corporate services, strategy, communications and advocacy and also more notably, an enforcement directorate (one of the directors being dedicated to consumer protection, alongside an executive director and 2 other directors - cartels and antitrust)[182]; a Markets and Mergers Directorate; the Legal Services/ Policy and International Directorate (with a director (out of 7) shared across cartels and consumer enforcement).

The CMA also has an Office of the Chief Economic Adviser which houses the Chief Data and Technology Insights Officer.[183] The team working for the Chief Data and Technology Office is known as the DaTA unit[184] (although it is not featured in any official organograms). The first impetus for the creation of a data and technology team at the CMA dates back to 2017. It was linked with the need to strengthen investigative capacity in 'big digital cases'.[185] The DaTA unit

[179] https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/our-divisions/division-litigation-technology-analysis accessed 23 June 2023

[180] https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/our-divisions/division-litigation-technology-analysis accessed 23 June 2023.

[181] https://www.gov.uk/government/organisations/competition-and-markets-authority/about/our-governance accessed 24 June 2023.

[182] https://www.gov.uk/government/publications/cma-structure/cma-structure-chart-as-at-march-2019 (updated 22 July 2022) accessed 24 June 2023.

[183] https://www.gov.uk/government/publications/cma-structure/cma-structure-chart-as-at-march-2019 (updated 22 July 2022) accessed 24 June 2023. Currently Karen Croxson, Chief Data & Technology Insights Officer, succeeding Stefan Hunt.

[184] Stefan Hunt, The technology led transformation of competition and consumer agencies: The CMA's experience, discussion paper (14 June 2022)

[185] Barney Thompson, UK Competition regulator builds new tech team (Financial Times, 13 November 2017).

had 15 staff as of May 2019 and the CMA was advertising for more recruits.[186] The number of staff is believed to be around 50 in 2023. The reason why the team sits with the economic team is because economists would typically lead on technology insights and data analysis.[187] Being embedded into an existing team reportedly worked well, saving on the overheads needed to establish a separate division or directorate and enabling it to complement the work of colleagues already part of case teams.[188] The team reporting to the Chief Technology and Insight Officer is organised in single skills and includes the digital forensics and e-discovery team, a data science team, a data engineering team, a digital technology and insights team, and finally a behavioural hub.[189] In 2022, the CMA fielded a speaker at Cross-border enforcement of consumer law: looking to the future, panel on the use of data and other technologies organised by the University of Reading.[190] The CMA also ran a conference on Data, Technology and Analytics[191] featuring experiences from other agencies.[192]

The CMA also has a Digital Market Unit. The Digital Markets Unit was created in 2021 to cater for competition enforcement needs (although some benefits will inevitably derive consumers).[193] At the time it was constituted it lacked a legislative basis to exercise its powers. The unit was nevertheless established on a non-statutory basis to prepare for the new regime (there is currently a Bill[194] in front of Parliament which will significantly enhance the enforcement powers of the CMA). In the interim, the Government published some terms of reference setting out its non-statutory role. Aside from work preparing for the new enforcement regime (including building a team with the right expertise and the preparation of draft guidance, supporting and advising the government on the establishment of the statutory regime) the DMU works with the Government to provide insights and shape interventions. It also has a role in gathering evidence on digital markets to assist with the use of current powers regarding harm to competition. The DMU is also tasked with engaging stakeholders nationally (notably with the Digital Regulation Cooperation Forum, which includes sectoral enforcers[195]]) and internationally.[196] As the Bill's

[186] *See* Stefan Hunt, *The CMA DaTA Unit – We're Growing!*, U.K. Competition and Markets Authority (May 28, 2019), https://competitionandmarkets.blog.gov.uk/2019/05/28/the-cma-data-unit-were-growing/, accessed 24 June 2023.

[187] Stefan Hunt, The technology led transformation of competition and consumer agencies: The CMA's experience, discussion paper (14 June 2022) 36.

[188] Stefan Hunt, The technology led transformation of competition and consumer agencies: The CMA's experience, discussion paper (14 June 2022) 36.

[189] Stefan Hunt, The technology led transformation of competition and consumer agencies: The CMA's experience, discussion paper (14 June 2022) 36.

[190] The conference programme is available: https://www.crossborderenforcement.com/copy-of-conference-17-03-22 accessed 11 July 2023. The online recording for the conference is available here: https://www.youtube.com/watch?v=DpPvjoamb2I&t=6066s accessed 11 July 2023.

[191] CMA Data, Technology and Analytics Conference 2022, bringing data, technology and analytics to competition and consumer protection (15-16 June 2023) https://cmadataconference.co.uk/ accessed 26 June 2023.

[192] Ibid.

[193] https://www.gov.uk/government/collections/digital-markets-unit accessed 11 July 2023.

[194] https://bills.parliament.uk/bills/3453 accessed 24 June 2023.

[195] https://www.gov.uk/government/publications/drcf-terms-of-reference accessed 24 June 2023. The Digital Regulation Cooperation Forum includes the CMA, the Information Commissioner's Office and Ofcom (the telecoms regulator). The Forum supports regulatory coordination in digital markets and cooperation on areas of mutual importance (see for more details, https://www.gov.uk/government/publications/digital-regulation-cooperation-forum accessed 1 July 2023).

[196] https://www.gov.uk/government/collections/digital-markets-unit accessed 11 July 2023.

adoption is approaching the DMU advertised for new roles[197] (a total of 20 new roles, ranging from principal digital market advisers to support officers).

NETHERLANDS

**Authority for Consumers & Markets (ACM)** https://www.acm.nl/en

The ACM has both a competition and consumer enforcement remit. It has oversight for general consumer law and some sectoral aspects (notably telecoms, having merged with the Post and Telecommunication Authority (OPTA) back in 2013. It is an independent regulatory body, directed by a Board of 3 (including the Chairman of the ACM).[198] Its work is structured around 3 main divisions: the Policy and Communications Department, The office of the Chief Economist (also housing the ACM Academy) and specialised departments which include the Consumer Department, the Competition Department, and Energy, Telecommunications, Transport and Postal, Healthcare as well as the Legal Department and Corporate Service Department.[199]

The ACM operates a Taskforce for Data and Algorithms (TDA) which employs data engineers, data scientists and visualisation experts and data governance experts. Their main tasks include the in-house development of tooling (vs. off the shelf solutions), monitoring and anticipating developments (e.g. voice analyses AI); supporting enforcement cases (advisory role) and processing large data sets.[200]

The ACM has joined forces with the Dutch Data Protection Authority, the Authority for Financial Markets and the Media Authority to work together to strengthen oversight of digital and online activities and seek to develop a coherent and coordinated strategy. The authorities will combine their expertise and knowledge and help each other in enforcement efforts.[201]

AUSTRALIA

**Australian Competition & Consumer Commission (ACCC)** https://www.accc.gov.au/

The ACCC is the regulator for competition, consumer, fair trading, and product safety. It also has a remit for national infrastructure. To deliver this vast portfolio, the ACCC is an independent statutory authority. It was established in 1995. The institution is organised with a Chair, (2 deputy chairs) and commissioners and associate members at its helm.[202] Its day to day activities are directed by the Chair and agency Head (currently Gina Cass-Gotlieb) and a chief executive officer. Thy oversee the work of a number of units including: Digital Transformation,

[197] https://competitionandmarkets.blog.gov.uk/2023/05/16/join-the-cmas-digital-markets-unit/ accessed 24 June 2024.
[198] https://www.acm.nl/en/about-acm/our-organization/board accessed 30 June 20223.
[199] https://www.acm.nl/en/about-acm/our-organization/organizational-structure accessed 30 June 2023.
[200] Using Tech in Consumer Enforcement, ACM's experiences presentation at 'Introducing EnfTech: a technological approach to consumer law enforcement 20 April 2023' by Dries Cuijpers, Senior Enforcement Officer, Authority for Consumers and Markets, Netherlands, https://static1.squarespace.com/static/638646cea1515c69b8f572cb/t/64478512565ae2428ba15ecd/1682408723189/ACM_NL_Dries+Cuijpers.pdf accessed 05 October 2023
[201] https://www.acm.nl/sites/default/files/documents/2021-acm-annual-report_0.pdf accessed 30 June 2023.
[202] https://www.accc.gov.au/about-us/accc-role-and-structure/organisation-structure accessed 30 June 2023.

Competition, Consumer Data Right, Consumer and Fair Trading, Consumer product Safety, Corporate[203], Infrastructure, Mergers, Exemptions and Digital and a number of Specialist advice and Services units including: General counsels and special counsels (incl. consumer law), Chief Economist, and Data and Intelligence.[204]

## COLOMBIA

**Superintendencia de industria y comercio (SIC)** https://www.sic.gov.co/

SIC is a public authority attached to the Ministry of Trade, Industry and Tourism of Colombia. It is organised into 6 divisions (Deputy Superintendence): Competition, Consumer Protection, Personal Data Protection, Industrial Property, Technical Regulation and Legal Metrology, and Judicial Affairs.[205] Each section is subdivided into Directorates. The Consumer Protection section hosts an investigative branch (direction of investigations). SIC uses different digital tools to support the detection and gathering of anti-competitive conducts and some of them have been developed in-house.[206] It has a specialised IT unit called the Officina de Tecnologia e Informática (OTI)[207] staffed by engineers and professionals with technical and specialised knowledge in computer forensic science.[208] The technical staff is versed with the applicable administrative procedures, and they follow rigorously documented for each data processing activity.[209] The unit uses some externally sourced forensic tools. It has also developed some in-house tools, notably for data searches in the Sabueso project (see Part 5, section A, number 2)[210] Within the Deputy Superintendence on Consumer Protection, a small team (including staff with a background in Science, Technology and Innovation) worked with the OTI to develop a tool that will help staff impose sanctions for wrong-doing and are working on other projects.

## CANADA

**Office of Consumer Affairs** (OCA)

https://ised-isde.canada.ca/site/office-consumer-affairs/en

[203] Note the existence of an Information Management and Technology Services Director in this unit. https://www.accc.gov.au/about-us/accc-role-and-structure/organisation-structure accessed 30 June 2023.

[204] Headed by Sharon Deano (acting) – information current at 30 June 2023, https://www.accc.gov.au/about-us/accc-role-and-structure/organisation-structure.

[205] https://www.sic.gov.co/en/about-us accessed 30 June 2023.

[206] OECD, Latin American and Caribbean Competition Forum 2020: Digital Evidence Gathering in Cartel Investigations - Contribution from Colombia (DF/COMP/LACF (2020) 8) 3, para 7 https://one.oecd.org/document/DAF/COMP/LACF(2020)8/en/pdf.

[207] https://www.sic.gov.co/organigrama-perfiles-directivos accessed 30 June 2023.

[208] OECD, Latin American and Caribbean Competition Forum 2020: Digital Evidence Gathering in Cartel Investigations - Contribution from Colombia (DF/COMP/LACF (2020) 8) 4, para 8 https://one.oecd.org/document/DAF/COMP/LACF(2020)8/en/pdf accessed 30 June 2023.

[209] OECD, Latin American and Caribbean Competition Forum 2020: Digital Evidence Gathering in Cartel Investigations - Contribution from Colombia (DF/COMP/LACF (2020) 8) 4, para 11 https://one.oecd.org/document/DAF/COMP/LACF(2020)8/en/pdf accessed 30 June 2023.

[210] OECD, Latin American and Caribbean Competition Forum 2020: Digital Evidence Gathering in Cartel Investigations - Contribution from Colombia (DF/COMP/LACF (2020) 8) 5, para 13 https://one.oecd.org/document/DAF/COMP/LACF(2020)8/en/pdf accessed 30 June 2023.

OCA promotes the interests and protection of Canadian consumers based on the premise that well-informed and confident consumers help stimulate competition and innovation in the Canadian marketplace. Canada being a Federal State, there are two layers of protection, one at Federal level and one at provincial/ territorial level. Much of the enforcement on general consumer protection falls to the provinces. Our study was not able to look into the work of the Provincial agencies.

Competition law comes under the remit of the **Competition Bureau Canada (CBC)** www.ised-isde.canada.ca. The Competition Bureau Canada is an independent law enforcement agency that protects and promotes competition for the benefit of Canadian consumers and businesses.[211] A Commissioner of Competition and its office oversee the work of a number of Branches: the Mergers and Monopolistic Practices Branch, the Cartel and Deceptive Marketing Practices Branch, the Competition Promotion Branch, and the Digital Enforcement and Intelligence Branch and the Corporate Services Branch.[212] The Digital Enforcement and Intelligence Branch is known by the acronym CANARI which stands for Competition through Analytics, Research and Intelligence. This branch is a centre of expertise on digital business practices and technologies. It provides some intelligence expertise (behavioural economics, enforcement) and supports the understanding of the way companies use technology and data in the marketplace as well as how the Bureau is able to use tech and data to enhance enforcement and promotion work.[213]

FRANCE

**Autorité de la Concurrence (AdlC)** https://www.autoritedelaconcurrence.fr/en.

This authority specialises in competition regulation. In France, consumer law matters fall under the remit of a distinct entity, the DGCCRF - la Direction Générale de la concurrence, de la consommation et de la répression des fraudes. The Conseil National de la Consommation is only a consultative body to the relevant ministry.[214] The Autorité de la Concurrence has a shared secretariat and 3 directorates (cabinet of the resident and European and international affairs; communication; legal). It also hosts investigative units (for eg, cartels; economics) and in particular there is a unit dedicated to the digital economy - le service de l'économie numérique (SEN).[215] The digital economy unit is tasked with developing new digital investigatory tools, notably based on algorithmic technologies, big data and artificial intelligence. It supports the

[211] https://ised-isde.canada.ca/site/competition-bureau-canada/en/how-we-foster-competition/our-organization/our-structure accessed 30 June 2023.
[212] https://ised-isde.canada.ca/site/competition-bureau-canada/en/how-we-foster-competition/our-organization/our-structure accessed 30 June 2023.
[213] https://ised-isde.canada.ca/site/competition-bureau-canada/en/how-we-foster-competition/our-organization/our-structure accessed 30 June 2023.
[214] https://www.economie.gouv.fr/cnc/presentation-conseil-national-consommation-cnc accessed 24 June 2023.
[215] https://www.autoritedelaconcurrence.fr/sites/default/files/20220622-decision-d-organisation.pdf accessed 24 June 2023.

work of all investigation and litigation units. It contributes to studies on digital matters and provides expertise to other projects of the Authority that require digital expertise.[216]

JAPAN

**Fair Trade Commission (JFTC)** https://www.jftc.go.jp/en/

In Japan, the Fair Trade Commission is charged with the regulation of competition. It is a separate entity that is charged with consumer protection, the Consumer Affairs Agency. The agency is under the direction of the Minister of State for Consumer affairs and food safety. The agency chart does not show a dedicated team of technologists assisting with consumer law enforcement[217] and we have not found evidence of use of tech in consumer enforcement. The Fair Trade Commission has started using technological tools in the enforcement of competition law[218] but it does not appear to have created a specific team to deliver this.[219]

KOREA

**Korea Consumer Agency (KCA)** https://www.kca.go.kr/eng/main.do

The Korea Consumer Agency is headed by a President with a Board of Directors and assisted by a Vice President and a team of Secretary.[220] The Vice President and President have as direct reports, the Chairman of the CDSC (Consumer Dispute Settlement Commission) and the Inspector general who is a non-standing member and who heads the Integrity Audit Office. The Vice President oversees a number of departments including PLanning & coordination, Safety Management, Public affairs and Consumer Policy. Besides, 2 executive directors report to the Vice President. They are the executive director of Consumer Safety Centre (https://www.ciss.go.kr/english/contents.do?key=596) and executive directive of the KCA. This later executive Director oversees the work of 3 departments and 2 regional offices (Seoul and Gyeonggi-Incheon-Gangwon). The departments are: Market research, Consumer education and consumer redress (which also houses reports for other regional offices). It is in the department of education that seats a Big Data Analytics & Public Disclosure Team and an Informatization Strategy Team.

In Korea there is also a **Korea Fair Trade Commission (KFTC)** https://www.ftc.go.kr/eng/index.do. The KFTC's main organisational components include a Committee (the decision making body) housing 9 commissioners and including a Chair and Vice Chair both recommended by the Prime Minister and appointed by the President. The work is

[216] Article 14, Décision du 22 Juin 2022 portant organisation de l'Autorité de la Concurrence (2022) https://www.autoritedelaconcurrence.fr/sites/default/files/20220622-decision-d-organisation.pdf accessed 24 June 2023.

[217] https://www.caa.go.jp/en/about_us/pdf/organization_chart_190701_0001.pdf accessed 26 June 2023.

[218] https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/02/century-technological-evolution-federal-trade-commission accessed 26 June 2023.

[219] https://www.jftc.go.jp/en/about_jftc/JFTC_OrganizationChart23.04.pdf accessed 26 June 2023.

[220] https://www.kca.go.kr/eng/sub.do?menukey=6021 accessed 03 October 2023.

supported by a Secretariat General for Policy.[221] The Institution hosts a general counsel, with separate directors for deliberation management in both consumer law and competition law, alongside directors for business trade, Litigation and a general unit. A number of Bureaux are also in place, notably a consumer policy bureau which houses a general consumer policy division, a consumer safety and education division, a consumer trade policy division and a specialised division in trade. There does not appear to be a specialised tech unit, although there is an e-commerce investigation Team housed in the Anti-Monopoly Investigation Bureau.[222]

## TAIWAN

### The Taiwan Fair Trade Commission (TFTC) www.ftc.gov.tw

The authority primarily has a competition law remit, but it holds some discreet consumer protection powers notably in the enforcement of fair trading laws and notably misleading and comparative advertising[223] and pyramid sales. The TFTC is governed by a Commissioner's meeting (with a Chairperson, a vice chair and Commissioners). The institution's day to day work is carried out in a number of departments: Planning, Service Industry Competition, Manufacturing Industry Competition, Fair Competition, Legal Affairs. The work is also supported by a number of administrative offices including the Information and Economic Analysis Office, a secretariat, an HR office, Civil Service Ethics, Budget, Accounting and Statistics office. The organisational chart for the TFTC shows that 3% of staff specialise in computer science and related department, hitting towards the existence of tech expertise in-house[224] although there appears not to be a specialised unit[225] and we have not been able to document use in consumer law.

[221] https://www.ftc.go.kr/eng/contents.do?key=496 accessed 30 June 2023.
[222] https://www.ftc.go.kr/eng/contents.do?key=496 accessed 30 June 2023.
[223] https://www.ftc.gov.tw/internet/english/doc/docList.aspx?uid=748 accessed 26 June 2023.
[224] https://www.ftc.gov.tw/internet/english/doc/docDetail.aspx?uid=198&docid=12193 accessed 30 June 2023.
[225] The TFTC needs to be set up to receive electronic form for complaints on misleading ad, see https://www.ftc.gov.tw/internet/english/doc/docDetail.aspx?uid=748&docid=15243, art 8.