Stanford Computational Antitrust

ARTICLE

Discussing The Legitimacy of Digital Market Surveillance

Catalina Goanta* & Jerry Spanakis**

Abstract. Legal compliance is increasingly becoming digital, and that is a fact. In shaping its digital future, in the past years, the European Union has been proposing one legal reform after another, such as the Digital Services Act package or the AI Act. A common thread in these developments is the policy reflection on not only how to update or make new rules for digital markets but also how to enforce them effectively. This has already been reflected in earlier instruments such as the Consumer Protection Cooperation Regulation or the Digital Market Surveillance Regulation. Although necessary for checking legal compliance, resulting digital enforcement practices need fast innovations from an interdisciplinary scientific space, (e.g., law/computer science/behavioral sciences) which is in its infancy. The pursuit of developing "tools" that can monitor market actors or detect harmful behaviors requires, at a minimum, clear legal interpretations, the translation of these interpretations into computer science tasks, and the ranking of harms affecting consumer behavior. This gap and the surrounding pace at which demands for filling it increases, create some interesting questions relating to the ethical and legitimacy limits of digital market surveillance. In this position paper, we firstly explore definitional frameworks for surveillance on digital markets and digital enforcement and subsequently propose a practical taxonomy for the types of digital compliance activities which may be undertaken by designated authorities in the European Union as a result of recent enforcement regulation, particularly in relation to consumer protection and competition authorities. In this section, we look at the new CPC Regulation and address some of the issues relating to its application to the digital economy. In the third section, we critically reflect upon the dangers of privatizing legal enforcement and briefly address some potential solutions. The fourth section concludes.

* **Catalina Goanta** is an Associate Professor in Private Law and Technology at Utrecht University and the Principal Investigator of HUMANads, a multidisciplinary Starting Grant funded by the European Research Council focused on the fairness of native advertising in the content creation economy.

** **Gerasimos (Jerry) Spanakis** is an assistant professor in machine learning and data mining at Maastricht University. Jerry currently serves in the editorial board of Data Mining and Knowledge Discovery Journal and has been in the program committee of many leading conferences and workshops in machine learning and natural language processing (ACL, ECMLPKDD, NLLP etc.)

I. Introduction

Legal compliance is increasingly becoming digital, and that is a fact. In shaping its digital future,[1] in the past years, the European Union has been proposing one legal reform after another, such as the Digital Services Act (hereinafter "DSA") package[2] or the AI Act.[3] A common thread in these developments is the policy reflection not only on how to update or make new rules for digital markets but also on how to enforce them effectively. This has already been reflected in earlier instruments such as the Consumer Protection Cooperation ("CPC") Regulation[4] or the Digital Market Surveillance Regulation.[5] As indicated in the preamble of the latter, "[i]n the age of constant development of digital technologies, new solutions that could contribute to the effective market surveillance within the Union should be explored."[6]

But what exactly is market surveillance in the digital age? Companies collecting the digital footprints of citizens and consumers led to the much-feared phenomenon of surveillance capitalism, the "looming threat of private power, subject to much analysis and heavy criticism."[7] States reducing the privacy of their citizens on a wide array of public interest grounds (e.g., combating crime) has led to state surveillance, which has been equally feared and criticized. For instance, the deployment of technologies for citizen surveillance, such as facial recognition, has led to considerable pushback from a vast range of regulatory stakeholders.[8] However, the surveillance of companies in order to prevent, for example, the proliferation of dangerous products that could affect consumers at large has traditionally been generally accepted as a necessity in the enforcement of effective consumer protection, at least in European legal doctrine and administrative practice.[9] In the past, this activity has been undertaken by national authorities

---

[1] *See Shaping Europe's Digital Future* (Feb. 2020), https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf. *See also Commission White Paper on Artificial Intelligence – A European approach to excellence and trust*, COM(2020) 65 final (19 February 2020) (https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf).

[2] *Commission Proposal for a Regulation on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*, COM(2020) 825 final (15 December 2020) (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0825&from=en). *See also* Caroline Cauffman & Catalina Goanta, *A New Order: The Digital Services Act and Consumer Protection*, 12 EUR. J. RISK REGUL. 758 (2021).

[3] *Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts*, COM(2021) 206 final (21 April 2021) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206).

[4] Commission Regulation 2017/2394 of the European Parliament and of the Council of 12 December 2017 on Cooperation Between National Authorities Responsible for the Enforcement of Consumer Protection Laws and Repealing Regulation (EC) No 2006/2004 [2017] OJ L 345.

[5] Regulation 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 [2019] O.J. (L 169).

[6] Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on Market Surveillance and Compliance of Products and Amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 [2019] OJ L 169, pmbl. 31.

[7] *See* Amy Kapczynski, *The Law of Informational Capitalism,* 129 YALE L.J. 1460 (2020). *See also* Shoshana Zuboff, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (PublicAffairs, 2019); Julie E. Cohen, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATION CAPITALISM (Oxford University Press, 2019).

[8] *See* Monika Zalnieriute, *Burning Bridges: The Automated Facial Recognition Technology and Public Space Surveillance in the Modern State,* 22 COLUM. SCI. & TECH. L. REV. 284 (2021); Evan Selinger & Woodrow Hartzog, *The Inconsentability of Facial Surveillance,* 66 LOY. L. REV. 101 (2019); Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment,* 105 MINN. L. REV. 1105 (2021).

[9] *See, e.g.,* Laszlo Szegedi, *EU-Level Market Surveillance and Regulation by EU Agencies in Light of the Reshaped Meroni Doctrine*, 2014 EUR. NETWORKS L. & REG. Q. 298 (2014); Trudo Lemmens & Shannon Gibson, *Decreasing the Data Deficit: Improving Post-Market Surveillance in Pharmaceutical Regulation*,

endowed with investigation powers, like exchanges and securities commissions.[10] However, in more recent years, as digitalization drives the re-design of technical infrastructure around government activities, new forms of privatization have become embedded in this process. As legal compliance demands for complex techno-legal architectures, the expertise and resources pertaining to public administration no longer suffice to meet these demands. In addition, the complexities posed by digital markets dwarf a lot of the existing avenues for the detection of bad business behavior, such as consumer complaints. The Cambridge Analytica incident is a perfect example in this regard. As the tech giant was funneling data to third parties through its Graph API (including through the so-called "Extended Permissions," which gave developers access to Messenger data), it was telling consumers a whole different story.[11] How are then consumers supposed to understand the intricacies of secondary data brokerage markets fueled by data products created by social media platforms such as Facebook, when disparities exist between what is written in general terms, what is communicated to consumers, and what is done in practice?

Although necessary for checking legal compliance, resulting digital enforcement practices need fast innovations from an interdisciplinary scientific space, (e.g., law/computer science/behavioral sciences) which is in its infancy. The pursuit of developing "tools" that can monitor market actors or detect harmful behaviors requires, at a minimum, clear legal interpretations, the translation of these interpretations into computer science tasks, and the ranking of harms affecting consumer behavior. This gap and the surrounding pace at which demands for filling it increases, create some interesting questions relating to the ethical and legitimacy limits of digital market surveillance.

In this position paper, we firstly explore definitional frameworks for surveillance on digital markets and digital enforcement and subsequently propose a practical taxonomy for the types of digital compliance activities which may be undertaken by designated authorities in the European Union as a result of recent enforcement regulation, particularly in relation to consumer protection and competition authorities. In this section, we look at the new CPC Regulation and address some of the issues relating to its application to the digital economy. In the third section, we critically reflect upon the dangers of privatizing legal enforcement and briefly address some potential solutions. The fourth section concludes.

II. The legitimacy of legal compliance

A – **Market surveillance v. digital enforcement**

In the European Union, market surveillance is nothing new, and it needs to be understood in light of the history of European integration through the Internal

59 MCGILL L. J. 943 (2014); Barend Van Leeuwen, *PIP Breast Implants, the EU's New Approach for Goods and Market Surveillance by Notified Bodies*, 5 EUR. J. RISK. REGUL. 338 (2014).

[10] Douglas Cumming & Sofia Johan, *Global Market Surveillance*, 10 AM. L. & ECON. REV. 454 (2008).

[11] *See, e.g.,* Cătălina Goanta & Stephan Mulders, *'Move Fast and Break Things': Unfair Commercial Practices and Consent on Social Media,* 8 EUCML 136 (2019). *See also* Iraklis Symeonidis, Pagona Tsormpatzoudi & Bart Preneel, *Collateral Damage of Facebook Apps: An Enhanced Privacy Scoring Model*, 2015 EPRINT IACR (2015).

Market by virtue of the free flow of goods across borders.[12] A healthy Internal Market has been considered to need a rather high degree of harmonization of technical standards in the name of public trust, which is said to include health, safety, and environmental and consumer protection.[13] In 2008, the European Union adopted a generous package of legal measures which were, on the one hand, aimed at improving the free movement of goods, while on the other hand strengthening market surveillance to ensure the smooth flowing of goods. This package included three specific measures:[14]

(i) Regulation (EC) No. 764/2008 of the European Parliament and of the Council of 9 July 2008 Laying Down Procedures Relating to the Application of Certain National Technical Rules to Products Lawfully Marketed in Another Member State and Repealing Decision No. 3052/95/EC;
(ii) Regulation (EC) No. 765/2008 of the European Parliament and of the Council of 9 July 2008 Setting Out the Requirements for Accreditation and Market Surveillance Relating to the Marketing of Products and Repealing Regulation (EEC) No. 339/93; and
(iii) Decision No. 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a Common Framework for the Marketing of Products, and Repealing Council Decision 93/465/EEC.

In this context, market surveillance has been mainly focused on product safety.[15] As a regulatory activity, market surveillance consisted of monitoring and detecting products available on the market that were unsafe, and the removal of which was necessary to minimize consumer harm.[16] By ensuring that some companies would not get away with selling and profiting off dangerous products, this type of regulation would also be beneficial to business.

More recently, the Market Surveillance Regulation of 2019 re-affirmed the fact that market surveillance is a long-standing characteristic of effective consumer protection in the European Union.[17] According to this newer Regulation, "market surveillance" is defined as "the activities carried out and measures taken by market surveillance authorities to ensure that products comply with the requirements set out in the applicable Union harmonization legislation and to ensure the protection of the public interest covered by that legislation."[18] These developments are equally acknowledged in the technology-centric regulatory proposals pursued by the

[12] *See* Lukasz Gorywoda, *The New European Legislative Framework for the Marketing of Goods*, 16 COLUM. J. EUR. L. 161 (2010). *See also* Michael Veale & Frederik Zuiderveen Borgesius, *Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach*, 22 COMPUT. L. REV. INT'L 97 (2021).
[13] *Id.* at Gorywoda, *supra* note 11, at 163.
[14] Gorywoda, *supra* note 11, at 162.
[15] *See also* Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety, 2001 O.J. (L 11); Geraint Howells, *Towards an Even Safer Europe for Consumers*, 3 J. EUR. CONSUMER & MKT. L. 1 (2014); Luis Gonzalez Vaque, *The Proposed EU Consumer Product Safety Regulation and Its Potential Conflict with Food Legislation*, 9 EUR. FOOD & FEED L. REV. 161 (2014). However, market surveillance can also be relevant for other industries, such as securities. *See* for instance James M Bartos, *US Market Regulation and Global Offerings with a US Tranche*, 6 INT'L FIN. L. REV. 16 (1987).
[16] Gorywoda, *supra* note 11, at 167. *See also* Christopher Hodges, EUROPEAN REGULATION OF CONSUMER PRODUCT SAFETY 156 (Oxford University Press 2005).
[17] Regulation 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 [2019] O.J. (L 169).
[18] Article 3(3) of Regulation 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 [2019] O.J. (L 169).

Commission earlier this year. For instance, the AI Act states that "[m]arket surveillance authorities would also control the market and investigate compliance with the obligations and requirements for all high-risk AI systems already placed on the market. Market surveillance authorities would have all powers under Regulation (EU) 2019/1020 on market surveillance."[19]

Digital enforcement is a term with a broader meaning, ranging from the enforcement of rules initially intended for the offline world in the online sphere[20] to private enforcement mechanisms facilitated by technology.[21] These two approaches pertain to two different narratives. First is the narrative that "all the enforcement mechanisms that are available in the analog environment need to be available in the digital environment as well."[22] The second narrative revolves around native, technology-driven possibilities to enforce rules by virtue of their embedding in the architectures providing access to goods or services via the Internet or even the dark web.[23]

Especially when looking at the role of public authorities in digital markets, there is a noticeable trend towards digital enforcement needs. For instance, in 2019, the Canadian Competition Bureau appointed a "Chief Digital Enforcement Officer, who will help the Bureau monitor the digital landscape, identify and evaluate new investigative techniques, and boost its digital intelligence-gathering capabilities."[24] This may be a sign of what was referred to earlier as the "machine state," namely the paradigm shift according to which the "inherent characteristics of technology will become inherent within the digitization of law."[25]

Given these developments, it can be argued that market surveillance as a product safety activity is increasingly becoming a type of digital enforcement. In the European context, it must be noted that surveillance for the purpose of making sure children do not choke on toys, or that batteries do not explode and hurt consumers has been generally seen as a responsibility of public authorities tasked with the protection of both consumers and the market ecosystem. From this perspective, there is a history of legitimacy for market surveillance, together with a well-carved need for such effective accountability mechanisms.

---

[19] Section 5.2.6. of Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence.

[20] Margot E Kaminski, *An Overview and the Evolution of the Anti-Counterfeiting Trade Agreement*, 21 ALB. L.J SCI. & TECH. 385 (2011); Margot Kaminski, *Positive Proposals for Treatment of Online Intermediaries* 28 AM. U INT'L L. REV. 203 (2012); Hilary H. Lane, *The Realities of the Anti-Counterfeiting Trade Agreement*, 21 TUL. J INT'L & COMP. L. 183 (2012).

[21] Mark Verstraete, *The Stakes of Smart Contracts,* 50 LOY. U. CHI. L.J 743 (2019). *See also* Andrea Ottolia and Dan Wielsch, *Mapping the Information Environment: Legal Aspects of Modularization and Digitalization,* 6 YALE J.L & TECH. 174 (2003-2004).

[22] Steven Metalitz, *Session I: Keynote Panel, Describing the Legal Landscape*, 40 COLUM. J.L & ARTS 319, 321 (2017). *See also* Eldar Haber, *The Wiretapping of Things* 53 U.C. DAVIS L. REV 733, 737 (2019).

[23] Catalina Goanta, *The Private Governance of Identity on the Silk Road*, FRONTIERS IN BLOCKCHAIN (Apr. 7, 2020) https://www.frontiersin.org/articles/s10.3389/fbloc.2020.00004/full.

[24] *George McDonald Joins the Competition Bureau As New Chief Digital Enforcement Officer,* COMPETITION BUREAU CANADA, https://www.canada.ca/en/competition-bureau/news/2019/07/george-mcdonald-joins-the-competition-bureau-as-new-chief-digital-enforcement-officer.html

[25] James G. H. Griffin, *The Future of Technological Law: The Machine State,* 28 INT'L REV. L. COMPUT. & TECH 299 (2014).

B – Administrative Powers under the New CPC Regulation

As goods circulating on the Single Market need to abide by product safety standards, Member States are responsible for the national enforcement of these standards. In addition, administrative cooperation has been facilitated through the creation of informal groups of market surveillance authorities such as Administrative Cooperation Groups (AdCos).[26] The CPC Regulation is a clear example of a framework that formalizes the coordination between national authorities while harmonizing the administrative powers of such institutions to protect consumers' economic interests. The CPC Regulation covers three categories of infringements (Art. 2):

- *intra-Union infringements*: "any act or omission contrary to Union laws that protect consumers' interests that has done, does or is likely to do harm to the collective interests of consumers residing in a Member State other than the Member State in which: (a) the act or omission originated or took place; (b) the trader responsible for the act or omission is established; or (c) evidence or assets of the trader pertaining to the act or omission are to be found" (Art. 3(2)).
- *widespread infringements*:
  - "any act or omission contrary to Union laws that protect consumers' interests that has done, does or is likely to do harm to the collective interests of consumers residing in at least two Member States other than the Member State in which: (i) the act or omission originated or took place; (ii) the trader responsible for the act or omission is established; or (iii) evidence or assets of the trader pertaining to the act or omission are to be found; or
  - any acts or omissions contrary to Union laws that protect consumers interests that have done, do or are likely to do harm to the collective interests of consumers and that have common features, including the same unlawful practice, the same interest being infringed and that are occurring concurrently, committed by the same trader, in at least three Member States" (Art. 3(3)).
- *widespread infringements with a Union dimension*: "a widespread infringement that has done, does or is likely to do harm to the collective interests of consumers in at least two-thirds of the Member States, accounting, together, for at least two-thirds of the population of the Union" (Art. 3(4)).

[26] EUROPEAN COMMISSION, *Administrative Cooperation Groups*, https://ec.europa.eu/growth/single-market/goods/building-blocks/market-surveillance/organisation/adcos_en (last visited Jan. 10, 2022). The European Commission acknowledges a total of 29 administrative cooperation groups in the following industry areas: equipment and protective systems intended for use in potentially explosive atmospheres; cableways; explosives for civil uses; medical devices; construction products; unmanned aircraft systems; eco-design; electromagnetic compatibility; energy labeling; fertilizers; gas appliances; lifts and safety components for lifts; low voltage; machinery; marine equipment; measuring instruments; noise; pressure equipment sector; cosmetics; personal protective equipment; pyrotechnics; recreational craft and personal watercraft; chemicals; radio equipment; restriction of the use of certain hazardous substances; textile labeling; safety of toys; transportable pressure equipment; and labeling of tires. See also Geraint Howells, *Product Safety—A Model for EU Legislation and Reform* in VARIETIES OF EUROPEAN ECONOMIC LAW AND REGULATION – LIBER AMICORUM FOR HANS MICKLITZ 525 (Kai Purnhagen & Peter Rott eds., 2014); Kenneth W. Abbott et al., *The contribution of trans-governmental networks of regulators to international regulatory co-operation*, (OECD Regulatory Policy Working Papers No. 10, 2018); Cristina Alén Cordero & José Luis Muñoz Sanz, *Measurement of machinery safety level: European framework for product control: Particular case: Spanish framework for market surveillance*, 47(10) SAFETY SCI. 1285 (2009).

For these three categories of infringements, The CPC gives national consumer (and competition) authorities two main categories of powers: investigation and enforcement. The investigation powers are the following:

- the power to access documents, data or information, "in any format" (Art. 9(3)(a));
- the power to require relevant information, data or documents from any public authority, body or agency within their Member State, once more "in any format" (Art. 9(3)(b));
- the power to undertake inspections on any premises, land or means of transport of traders, or request other authorities to do so in order to obtain information, data or documents (Art. 9(3)(c));
- the power to engage in mystery shopping "to purchase goods or services as test purchases, where necessary, under a cover identity" (Art. 9(3)(d)).[27]

As for enforcement powers, these are:

- the power to adopt interim measures (Art. 9(4)(a));
- the power to settle the cessation of infringements and additional remedies with traders (Art. 9(4)(b)-(c));
- the power to inform consumers about the possibility of seeking compensation (Art. 9(4)(d));
- the power to order in writing the cessation of infringements or to bring it about (Art. 9(4)(e)-(f));
- in case no other effective means are available for the cessation of the infringement (Art. 9(4)(g)):
  - the power to remove content or restrict access to an online interface, as well as to order the display of a consumer warning on that interface;
  - the power to order a hosting service provider to remove, disable or restrict access to an online interface;
  - the power to order the deletion of a domain name before domain registries and allow competent authorities to register it.
- the power to give "effective, proportionate and dissuasive" fines or periodic penalty payments (Art. 9(4)(h));
- the power to start investigations or proceedings on their own initiative (Art. 9(6)).

C – The New CPC Regulation and Digital Markets

The CPC Regulation reform is an example of an enforcement framework that aims to increase the administrative options available to national authorities in effectively applying consumer protection rules. This is, among others, since the earlier version of the CPC Regulation was considered to lead to "ineffective enforcement in cases of cross-border infringements, including infringements in the digital environment."[28] Its application to the digital market is particularly

[27] *See also* Vanessa Mak & Kristin Nemeth, *The EU's Digital Agenda: New Proposals for Online and Offline Consumer Disputes, E-Commerce and Card, Internet and Mobile Payments*, 1 J. EUR. CONSUMER & MKT. L. 112 (2012); Mary Goodrich Nix and James R Ray, *Dissemblance in the Franchise Industry: The Art (and Ethics) of Deception*, 33 FRANCHISE L.J. 525 (2014).

[28] Claudia Massa, *New CPC Regulation and ECN+ Directive: The Powers of National Authorities in the Fields of Consumer Protection and Antitrust*, 4 MKT & COMPETITION L. REV. 113, 115 (2020). For a more

interesting to discuss, as consumer and competition authorities end up engaging in two categories of digital enforcement:

- *Monitoring activities*: this category entails market monitoring at scale, and in the past, it had included approaches such as "sweeps," consisting in the "screening (of) websites to identify breaches of consumer law in a given online market" and the adoption of further enforcement measures "in which national authorities ask traders to take corrective actions."[29] By engaging in monitoring activities, authorities focus on the market as a whole to better understand and measure the prevalence of consumer harm.
- *Investigation activities*: this category entails focusing on specific traders and doing in-depth investigative activities to ascertain if and to what extent consumer harms can be proven for authorities to take further enforcement measures such as injunctions, fines, etc.

To understand and measure harms on digital markets, particularly from a monitoring perspective, designated authorities need to have access to company data. This can be done in two ways. Firstly, companies may have to provide authorities with requested documents, information, or data, much like the obligation recently enshrined in Art. 31 of the DSA,[30] and secondly, authorities may proceed to collect documents, information, or data by themselves and even from other public authorities. As indicated above, under the new CPC Regulation, authorities may have access to any relevant documents, data, or information (Art. 9(3)(a)), and they may also "carry out necessary on-site inspections, including the power to enter any premises, land or means of transport that the trader concerned by the inspection uses for purposes related to his trade, business, craft or profession" (Art. 9(3)(d)). Although web scraping is not specifically referred to in the preamble or Art. 9, it can be interpreted to fall under any of these two provisions. It follows that authorities have broad, legitimate powers of collecting data from companies that participate in the digital economy.

On the one hand, these powers are necessary. The opacity of economic activity around data brokerage has long been signaled as a problem that existing regulatory

comprehensive overview of the history of the CPC Regulation see also Laurens van Kreij, *Towards a Comprehensive Framework for Understanding EU Enforcement Regimes*, 10 EUR. J. RISK REG. 439 (2019); Luis Gonzalez Vaque, *Possible Unfair Practices in the Marketing of Differentiated Food Products in the Single Market: The Concept of the Legitimate Expectations of Consumer*, 12 EUR. FOOD & FEED L. REV. 482 (2017); Carmen Appenzeller, *Towards a More Effective Regulation of Unfair Standard Contract Terms in Europe: Of Cartels, Watchdogs and a Gorilla in the Closet,* 6 J. EUR. CONSUMER & MKT. L. 60 (2017); Jules Stuyck, *The Transformation of Consumer Law in the EU in the Last 20 Years*, 20 MAASTRICHT J. EUR. & COMP. L. 385 (2013); Jasper Vereecken and Jarich Werbrouck, *Goods with Embedded Software: Consumer Protection 2.0 in Times of Digital Content?* 30 IND. INT'L & COMP. L. REV. 53 (2019); Michael Faure and Franziska Weber, *The Diversity of the EU Approach to Law Enforcement - Towards a Coherent Model Inspired by a Law and Economics Approach*, 18 GERMAN L.J. 823 (2017); Karin Sein, *The Draft Geoblocking Regulation and Its Possible Impact on B2C Contracts,* 6(4) J. EUR. CONSUMER & MKT. L. 148 (2017); Mateja Durovic, *Adaptation of Consumer Law to the Digital Age: EU Directive 2019/2161 on Modernisation and Better Enforcement of Consumer Law*, 2020 ANNALS FAC. L. BELGRADE INT'L ED. 62 (2020); *Magdalena Tulibacka, Proceduralisation of EU Consumer Law and Its Impact on European Consumers*, 8 REALAW, REV. EUR. ADMIN. L. 51 (2015).

[29] EUROPEAN COMMISSION, Sweeps, https://ec.europa.eu/info/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/sweeps_en (last visited Jan. 10, 2022). *See also* Larry A DiMatteo and Stefan Wrbka, *Planned Obsolescence and Consumer Protection: The Unregulated Extended Warranty and Service Contract Industry* 28 CORNELL J. L. & PUB. POL'Y 483 (2019).

[30] Paddy Leerssen, *Platform research access in Article 31 of the Digital Services Act: Sword without a shield?*, VERFASSUNGSBLOG (Sep. 7 2021), https://verfassungsblog.de/power-dsa-dma-14/.

frameworks have not been very adapted to.[31] With more powers to raise the veil of opacity, public authorities tasked with the enforcement of market regulation may make progress in ensuring legal compliance in the digital economy. On the other hand, with great power comes great responsibility. Leaving aside the discretion entrusted to public authorities, the main question arising from monitoring activities on digital markets is—how exactly are they supposed to be undertaken? Manual sweeps and mystery shopping, as investigative methods, have been traditionally performed through internal institutional capacities. In more recent times, and with digital business models developing at an incredible speed, the digitalization and automation of monitoring activities can become a heavy burden on public administration. This can lead to an indirect form of privatization of legal enforcement, as will be discussed in the next section.

III. Privatizing Digital Legal Enforcement: Problems and Solutions

The general gap between how the state and the private sector (especially big tech) currently understand and hone the power of technology (and the power *in* technology) is mind-boggling. During the past decades, the exponential benefits and harm known by societies through the proliferation of Internet technologies allowed some players to rise to incredible power and technology (e.g., companies such as Amazon or Facebook). This has been possible due to regulatory subsidies[32] governing Internet business models, which have usually been too volatile and unpredictable for lawmakers to determine with some degree of evidence-based accuracy how they can best be regulated. On other actors, such as states, technological development inflicted a detriment, if only through the inequality of information on market practices.

Around the world, the pace of government digitalization has varied quite widely,[33] given the complexity of this process and its massive needs of resources such as personnel, infrastructure, and expertise. Its benefits have been articulated repeatedly. In the words of Cary Coglianese, "[c]rafting government regulations imposes significant information demands on regulatory agencies, from completing scientific, engineering, and economic analyses to processing and responding to

[31] *See* for instance Daniel Neally, *Data Brokers and Privacy: An Analysis of the Industry and How It's Regulated*, 22 ADELPHIA L.J. 30 (2019-2021); Rebecca J Wilson et al., *Busting the Black Box: Big Data, Employment and Privacy*, 84 DEF. COUNSEL J. 1 (2017); Lindsey Barrett, *Deconstructing Data Mining: Protecting Privacy and Civil Liberties in Automated Decision-Making*, 1 GEO. L. TECH. REV. 153 (2016); Julie E Cohen, *Power/Play: Discussion of Configuring the Networked Self*, 6 JRSLM REV. LEGAL STUD. 137 (2012); Danielle Keats Citron and Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1 (2014); Zeynep Tufekci, *Algorithmic Harms beyond Facebook and Google: Emergent Challenges of Computational Agency* 13 COLO. TECH. L.J. 203 (2015).

[32] For a more general discussion on regulatory subsidies see Mark Naftel, *Market Implications of Technologically Neutral Regulation*, 3 J. NETWORK IND. 231 (2002); Peter Humphreys and Seamus Simpson, *Globalization, the Competition State and the Rise of the Regulatory State in European Telecommunications* 46 J. COMMON MKT. STUD. 849 (2008); George S Georgiev, *Too Big to Disclose: Firm Size and Materiality Blindspots in Securities Regulation*, 64 UCLA L. REV. 602 (2017).

[33] See, for instance, Marcelo D Varella et al., *Frog Leap in Public Policies through Digital Government: Opportunities and Challenges*, 7 BRAZ. J. PUB. POL'Y 561 (2017); Leticia Regina Camargo Kreuz and Ana Cristina Aguilar Viana, *4th Industrial Revolution and Digital Government: Analysis of Brazilian Experiences* 5 REV. EUROLATIN DER. ADM. 267 (2018); Makoto Hong Chang and Hui Choon Kuen, *Towards a Digital Government: Reflections on Automated Decision-Making and the Principles of Administrative Justice* 31 SAC. L.J. 875 (2019).

extensive public comments."[34] However, its pitfalls have also been the focus of academic scrutiny. One of the most notable points of criticism articulated by Mulligan and Bamberger has been the so-called "procurement mindset" when contracting for "technical systems that employ machine learning."[35] In describing this narrative, the authors emphasize how the government relies on purchasing technology from private parties.[36] Given the lack of resources and strategies to turn public authorities into technology makers, they generally retain the status of technology users and must rely on industry actors to provide automation or digitalization solutions that can be offered to the public.

At first sight, this makes sense. Economically speaking, without major investments in technology, governments may not be able to develop innovative technologies able to compete with the market status quo.[37] Companies can specialize in data products that can be purchased by public actors. However, generally speaking, data science companies use (as opposed to developing themselves) mainstream models and deploy them in various fields of application. However, as state-of-the-art scholarship on computational legal research shows,[38] the interdisciplinary research that is necessary to break down regulatory questions into measurable tasks is in its infancy.[39] This is particularly the case when discussing the translation of complex regulation into computational frameworks to tackle legally uncertain market practices such as dark patterns.[40] At the moment, in-depth, interdisciplinary research and development that can map and connect regulatory complexities, enforcement needs, and state-of-the-art technology is highly necessary and generally not readily available. What is more, enforcement authorities may have vastly different needs, which may require the development of vastly different technologies. Automating sweeps for the detection of dark patterns will normally require a web measurement study, whereas enforcing product safety rules by checking if traders offer forbidden products will need to heavily rely on computer vision tasks.

---

[34] Cary Coglianese, *E-Rulemaking: Information Technology and the Regulatory Process*, 56 ADMIN. L. REV. 353, 354 (2004). *See also* Joe Tomlinson, *Justice in Automated Administration*, 40 OXFORD J. LEGAL STUD. 708 (2020).

[35] Deirdre K Mulligan and Kenneth A Bamberger, *Procurement as Policy: Administrative Process for Machine Learning*, 34 BERKELEY TECH. L.J. 773 (2019).

[36] *Id.* at 774.

[37] However, global public spending on IT is expected to increase. *See* Gartner, *Gartner Forecasts Global Government IT Spending to Grow 5% in 2021*, Gartner (23 Feb. 2021), https://www.gartner.com/en/newsroom/press-releases/2021-02-18-gartner-forecasts-global-government-it-spending-to-grow-5-percent-in-20210.

[38] Proceedings of the Natural Legal Language Processing Workshop 2021, ACL Anthology: The 2021 Conference on Empirical Methods in Natural Language Processing (Nikolas Aletras, Ion Androutsopoulos, Leslie Barrett, Catalina Goanta, & Daniel Preotiuc-Pietro eds., 2021), https://aclanthology.org/volumes/2021.nllp-1/.

[39] For an overview of legal research on artificial intelligence, including research pertaining to the 'law and AI' community of scholars focusing on legal reasoning and expert systems see Catalina Goanta, Gijs van Dijck, & Gerasimos Spanakis, *Back to the future: Waves of Legal Scholarship on Artificial Intelligence*, in Time, Law, and Change: An Interdisciplinary Study (Sofia Ranchordás & Yaniv Roznai eds., 2020). *See also* Constanta Rosca, Bogdan Coverig, Catalina Goanta, Gijs van Dijck, & Gerasimos Spanakis, *Return of the AI: An analysis of legal research on Artificial Intelligence using topic modeling*, in (eds.), PROCEEDINGS OF THE NATURAL LEGAL LANGUAGE PROCESSING WORKSHOP 2020 (N. Aletras, I. Androutsopoulos, L. Barrett, A. Meyers, & D. Preoţiuc-Pietro eds., 2020), http://ceur-ws.org/Vol-2645/paper1.pdf; *and* Ronald J. Allen, *Taming Complexity: Rationality, the Law of Evidence and the Nature of the Legal System*, 12 LAW, PROBABILITY & RISK 99 (2013).

[40] Constanta Rosca, Bogdan Covrig, Catalina Goanta, Gerasimos Spanakis, & Gunes Acar, *Digital Monitoring of Unlawful Dark Patterns: What Role for Public Interest Technology?*, CHI Position Paper (2021), https://drive.google.com/file/d/10NkPlhzWncTS2hu_waY_inS1dFfWmshD/view.

Unfortunately, these complexities are disconnected from the debate around digital monitoring activities through the mere referral to technology as leading to "tools" that can magically fix the information gap between the private and the public sectors. Data products developed with the necessary interdisciplinary expertise may become essential assets for legal enforcement. However, in the current indirect privatization landscape, not acknowledging the need for sustained scientific work as a foundation for the development of public interest technology assets is detrimental as it reflects at least three issues: the snake oil issue, the capacity stagnation issue, and the discretion abuse issue.

First, suppose context-specific technology still needs to be developed for legal enforcement. In that case there is a risk that market products are snake oil,[41] and it is not practically easy for public authorities (or any other stakeholder) to verify the accuracy of such products. Such a result can be highly problematic for public trust in the event of incidents that prove an accuracy problem. Second, outsourcing public interest technology to market actors can have a long-term role in the development of capacity and architecture in public authorities. The privatization of the development of legal enforcement may absorb funding that could be better spent on transforming institutional infrastructure and resource availability. Lastly, relying on private solutions considerably increases the opacity associated with decision-making. As we established earlier in this position paper, market surveillance activities have a history of legitimacy in the European Union, and this legitimacy has been recently widened through the new CPC Regulation. The discretion such instruments confer to national authorities need not be doubled by further discretion in the privatization of legal enforcement. Otherwise, the entire legal enforcement framework risks becoming the very harm it is supposed to protect consumers and citizens from: the hidden interests of actors with power.

Moving away from the "procurement mindset" and embracing the "policy mindset" through "processes that foster deliberation reflecting both technocratic demands for reason and rationality informed by expertise, and democratic demands for public participation and political accountability"[42] is not an easy task. After the digitalization of government services, it is now necessary for the government to further shape its identity as the driver of public interest technology.[43] As we have seen above with the case of the Canadian Competition Bureau, there is momentum for public authorities to create pockets of expertise by bringing together public administration and law experts with technologists and behavioral scientists. In addition, there must be a further public discussion relating to the role of academia and civil society in the pursuit of scientific solutions which may be brought into the service of public interest technology. So far, formal collaboration frameworks like public tenders provide some possibilities for the co-development of public interest technology, with the caveat that interests are often difficult to align in interdisciplinary science. However, institutes aiming to fill the need for in-depth interdisciplinarity seem to be a growing trend that will hopefully repair current pitfalls.[44]

---

[41] *See* Matthew Ivey, *The Ethical Midfield in Artificial Intelligence: Practical Reflections for National Security Lawyers*, 33 GEO. J. LEGAL ETHICS 109 (2020).
[42] Mulligan & Bamberger, *supra* note 34, at 781.
[43] *See* Luz Herrera & Louise G. Trubek, *The Emerging Legal Architecture for Social Justice* 44 N.Y.U. REV. L. & SOC. CHANGE 355 (2020).
[44] Stan. Univ., *Human-Centered Artificial Intelligence*, Stanford University: Human-Centered Artificial Intelligence (2 Nov. 2021), https://hai.stanford.edu.

IV. Conclusion

This position paper aimed to discuss the legitimacy of market surveillance and digital enforcement in the European Union, particularly with respect to recent legal reforms around the CPC Regulation. As such, market surveillance in the EU has been traditionally welcomed to keep consumers away from unsafe products. Building on this tradition, the CPC Regulation expands monitoring activities also to other types of consumer issues, making it an instrument to be reckoned with in digital markets. After reflecting on the various powers and types of surveillance activities public authorities may pursue, we briefly analyzed them in the context of collecting data through activities such as web scraping.

In pursuing their administrative powers, authorities around the world have been indirectly relying on the privatization of legal enforcement, which leads to at least three problems: the snake oil issue, the capacity stagnation issue, and the discretion abuse issue. In order to remedy these issues, the solution proposed by Mulligan and Bamberger, namely the shift from the "procurement mindset" to the "policy mindset", is discussed as a viable alternative to privatization.[45] In addition, it is important to further reflect on the need to coordinate with academia and civil society for the development of public interest technology.

[45] Mulligan & Bamberger, *supra* note 34, at 781.