

Prof. Thibault Schrepel

Assistant Professor

School of Law

Utrecht University

t.schrepel@uu.nl

Re: Shaping competition policy in the era of digitisation

I hereby wish to submit my comments to the European Commission for its conference on competition policy in the era of digitization, in particular to the Panel 2 entitled “*Digital Platforms' Market Power.*”

Four points are developed:

- (1) the need to recognize predatory innovation as an anti-competitive practice ;
- (2) the challenges created by blockchain on competition rules ;
- (3) the combination of the predatory innovation and blockchain ;
- (4) the need to consider R&D investment in fine calculation.

On the one hand, competition law must indeed be adapted to new anti-competitive practices. This will increase legal certainty for the benefit of all. But on the other hand, competition law must also take into account the risk taken by companies in the digital sectors in terms of R&D investment. These changes will together make it possible to better protect innovation.

I. To recognize predatory innovation as such

Conventional wisdom assumes that competition law mechanisms are well suited to the study of practices in technology markets and that only adjustments should be made to these mechanisms, and sparingly at that. This is untrue. Several practices fall outside the scope of competition law because mechanisms for assessing the legality of those practices from a competition perspective are not adequate. In fact, no one can accurately identify a typical legal approach for non-price strategies, which results in the emergence of somewhat chaotic jurisprudence.

There is, indeed, little published literature on the subject of the new anti-competitive strategies nestled in these markets. The process of competition generally encourages companies to lower their prices, which benefits the consumer. And yet, in certain specific cases, competition rules sanction low prices because they are deemed to be predatory and thus intended to eliminate the competitive process itself. A similar situation applies to innovation. Innovation is one of the main bases for competition between companies and it is beneficial to consumers who may enjoy new products that are also better suited to their needs. But certain “*innovative*” behaviors are

considered predatory and are punished accordingly, despite the fact that no legal concept specifically addresses this issue.

This absence of a legal category specifically dedicated to anti-competitive practices disguised as “*innovation*” leads judges to create numerous type I and II errors. The jurisprudence has not yet generalized the etiquette of “*predatory innovation*,”¹ in spite of the fact that it answers some of the modern problems encountered by competition law with respect to developments in high-tech markets.² In fact, most predatory innovation practices are currently addressed under the label of “*technological tying*.” The creation of some legal rules dedicated to predatory innovation would lead to the removal of this dubious legal concept (technological tying) and result in a more coherent legal regime.

We propose applying the “*enhanced no economic sense*”³ test to non-price strategies, including to predatory innovation. Without creating numerous type-I or II errors, this test results in the creation of a uniform rule of law, which will ultimately increase consumer welfare by encouraging companies to continue innovating.

II. The challenges created by blockchain on competition rules⁴

The very nature of blockchain raises fundamental questions for competition law not seen since the advent of the Internet. Because blockchain is decentralized, anonymous and immutable, multiple questions arise regarding the detection of practices as well as the identification of perpetrators.

Anti-competitive practices on blockchain

One of the major issues faced by competition law in the face of blockchain is related to the identification of anti-competitive practices. This problem is new and twofold. First, algorithms are drastically accelerating the implementation of anti-competitive practices. They create issues on how to detect such practices and, incidentally, how to address evidence.⁵ But

¹ Thibault Schrepel, L’INNOVATION PRÉDATRICE EN DROIT DE LA CONCURRENCE (Larcier, 2018). Also, Thibault Schrepel, *Predatory Innovation: The Definite Need for Legal Recognition*, SMU SCI. & TECH. L. REV. (2018), at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2997586.

² This has been seen as such by the Italian Parliament (http://www.camera.it/_dati/leg17/lavori/stampati/pdf/17PDL0060920.pdf) as well as the Belgian Parliament (<https://www.lachambre.be/flwb/pdf/54/3246/54K3246001.pdf>) which both introduced legislative proposals on predatory innovation.

³ Thibault Schrepel, *The “Enhanced No Economic Sense Test”: Experimenting With Predatory Innovation*, 7 N.Y.U. JOURNAL OF INTELL. PROP. & ENT. LAW 30 (2018) at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3115949.

⁴ For more on the intersection between blockchain and competition law, see Thibault Schrepel, *Is Blockchain the Death of Antitrust Law? The Blockchain Antitrust Paradox*, 3 GEO. L. TECH. REV. (forthcoming) at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3193576.

⁵ Computational law is that branch of legal informatics concerned with the mechanization of legal analysis (whether done by humans or machines), see <http://complaw.stanford.edu/> and <https://law.stanford.edu/projects/computational-law/>.

when practices implemented by algorithms are identified, the perpetrator is generally known concomitantly. The second issue faced by competition law is relative to blockchain. Indeed, blockchain is a technology that ensures the anonymity - or at least pseudonymity - of its users. The pseudonymity of transactions on the blockchain, combined with the anonymity of the nodes on the chain create obstacles in terms of enforcement. Thus, the distributed network architecture of blockchain constitutes a real barrier to competition law enforcement. No single entity can realistically control a public blockchains;⁶ indeed, blockchains were specifically designed to require consensus among the many decentralized transaction verifiers (typically, the so-called “miners” who undertake proof of work)⁷ and thereby avoid the problems of centralized control.⁸ For that reason, although a practice may be seen as being anti-competitive, the author may remain unidentified.

In addition to the issue raised by pseudonymity,⁹ other issues occur in relation to the effectiveness of sanctions and remedies¹⁰ because there are no “choke points” on blockchain. For instance, Augur - “a decentralized oracle & prediction market platform” - has no central party that can stop its operation.¹¹ This platform will continue to work even if governments get tough — and even if penalties are imposed on the original parties who develop or promote the blockchain.¹² No “technically skilled people of goodwill”¹³ are needed to keep the blockchain going, in fact, Daaps cannot be shut down because there is no server to take down.¹⁴ They can only be modified under specific and technical circumstances.¹⁵

⁶ Individual control of the blockchain would require a so-called 51% attack, whereby a single entity takes control of 51% of the nodes on a chain. The cost of such an attack is presumed to be greater than any benefit that could be obtained from fraudulent transactions that could be made as a result.

⁷ Please note that other consensus mechanisms are used. All blockchains are decentralized by nature nonetheless.

⁸ Gur Huberman, Jacob D. Leshno & Ciamac C. Moallemi, *Monopoly without a Monopolist: An Economic Analysis of the Bitcoin Payment System* 37 (2017): “Monopolies are often regulated to prevent or at least mitigate their abuse of power. Bitcoin is not regulated. It cannot be regulated. It need not be regulated because individually the miners are price takers.”

⁹ This issue has been raised in the past, at a time when Internet wasn’t “designed to reveal who someone is, where they are, and what they’re doing,” see Lawrence Lessig, *CODE: AND OTHER LAWS OF CYBERSPACE*, Version 2, 38 (New York: Basic Books, 2006).

¹⁰ Indeed, Primavera De Filippi & Aaron Wright, *BLOCKCHAIN AND THE LAW: THE RULE OF CODE* 44 (2018): “Blockchains thus enable the creation of autonomous software programs run through the collaborative effort of parties with different incentives and in different locations scattered across the globe, none of which can unilaterally affect the code’s execution. Once deployed on a blockchain, these programs no longer need or necessarily heed their creators; they are run on a decentralized network, making it difficult to unwind or halt their execution.”

¹¹ Robert P. Murphy & Silas Barta, *UNDERSTANDING BITCOIN*, Version 1.11, 78 (2017): “Remember that no one is “in charge” of Bitcoin. So long as just one copy of the blockchain survives on someone’s hard drive somewhere on Earth, the Bitcoin network can quickly propagate to thousands of other computers once that person gets online.”

¹² Primavera De Filippi & Aaron Wright, *BLOCKCHAIN AND THE LAW: THE RULE OF CODE* 104 (2018).

¹³ Jonathan Zittrain, *THE FUTURE OF THE INTERNET—AND HOW TO STOP IT*, 246 (Yale University Press, 2008): “Our generative technologies need technically skilled people of goodwill to keep them going, and the fledgling generative activities above—blogging, wikis, social networks—need artistically and intellectually skilled people of goodwill to serve as true alternatives to a centralized, industrialized information economy that asks us to identify only as consumers of meaning rather than as makers of it.”

¹⁴ Siraj Raval, *DECENTRALIZED APPLICATIONS: HARNESSING BITCOIN’S BLOCKCHAIN TECHNOLOGY* 7 (O’Reilly Media, 2016): “Data in a dapp is decentralized across all of its nodes. Each node is independent; if one fails, the others are still able to run on the network.”

¹⁵ See Max Raskin, *The Law and Legality of Smart Contracts*, 1 *GEO. L. TECH. REV.* 305, 326 (2017). They could be

Blockchain also creates issues related to emergency measures due to the fact that it is nearly impossible to impose an injunction against a decentralized autonomous organization. The only way around, once again, would be to encode these measures into the blockchain's governance.

More broadly, it will be necessary to ensure a sufficiently effective deterrent effect,¹⁶ because practices are immutable and written on the blockchain forever. And many other procedural questions will arise,¹⁷ as the usefulness of dawn raids will be called into question insofar as the seizure of a single computer will not make it possible to go back to the source, added to the fact that all the data – the amount of a transaction, its object, the identity of the parties – will be encrypted and unbreakable.¹⁸ Questions also arise as to the territoriality of the law.¹⁹ Competition authorities could lack the ability to seize the organization's assets or enforce an injunction. Blockchain users located outside of the country in which the legal action is brought could indeed refuse to grant access to the blockchain.²⁰

In short, if competition law is maintained as it is today, it will quickly become ineffective for technical reasons that will not be possible to overcome. Because of the need for regulatory infiltration, fascinating debates of public policies are ahead of us on how to proceed. And we need to get to the subject quickly, because, as Lawrence Lessig already underlined in 2006, “*we are at a stage in our history when we urgently need to make fundamental choices about values, but we should trust no institution of government to make such choices.*”²¹

Competition *via* blockchain

Network effects are often used in the literature on digital sectors.²² They are twofold - direct or indirect - the idea being that the more a technology is used, the more new users are encouraged to join the group.²³ This is a fairly classic mass effect, also known as Metcalfe's Law in the context of information technology, according to which the value of a network is approximately proportional to the square of the number of users (people plus machines) that

linked to publicly available relevant legal provisions which, when they are modified, will automatically change smart contracts. These contracts could also be written with the option of inserting code later.

¹⁶ Lawrence Lessig, *CODE: AND OTHER LAWS OF CYBERSPACE*, Version 2, 152 (New York: Basic Books, 2006): “*Even with open code, if the government threatens punishments that are severe enough, it will induce a certain compliance.*”

¹⁷ This paper focusses on substantial issues.

¹⁸ This is all the more true if the blockchain uses a “*Zero knowledge proof*” system.

¹⁹ On the need for regulatory cooperation in face of new technologies, see Hannah L. Buxbaum, *Transnational Antitrust Law*, *OXFORD HANDBOOK OF TRANSNATIONAL LAW* 11 (Peer Zumbansen ed., forthcoming).

²⁰ Primavera De Filippi & Aaron Wright, *BLOCKCHAIN AND THE LAW: THE RULE OF CODE* 145 (2018).

²¹ He further adds that “*the government we now have is a failure. Nothing important should be trusted to its control, even though everything important is.*” Lawrence Lessig, *CODE: AND OTHER LAWS OF CYBERSPACE*, Version 2, 8 (New York: Basic Books, 2006).

²² Showing how network effect can positively and negatively affect social welfare, see Michal S. Gal, *The Power of the Crowd in the Sharing Economy*, *LAW AND ETHICS OF HUMAN RIGHTS* (Forthcoming, 2018).

²³ Also, on blockchain, as on current platforms, “*reputation has emerged as one of the most vital facets of competition in many modern markets,*” for more on that see John M. Newman, *Complex Antitrust Harm in Platform Markets*, CPI (2017).

are connected to it. When reaching a certain number of users, “*the value exceeds the cost for the majority of potential users, and they start multiplying rapidly, increasing the value in total, and to other individual users.*”²⁴ That number effect is also described by “*Aggregation Theory*”²⁵ based on which “*consumers are attracted to an aggregator through the delivery of a superior experience.*”²⁶ The idea of *experience* here is added to the simple mass effect. So does the blockchain, thanks to its intrinsic qualities, allow network effects to be limited in time?²⁷ Is blockchain the “*most viable way out from the antitrust trap created by Aggregation Theory*”?²⁸ That is very likely²⁹ and if that were to be the case, “*New Googles*” will soon be created.

With public blockchains, much of the relevant data are public and shared by the distributed ledger system. This structure is opposite to the client-server platforms as we know them. The result is an acceleration of the competitive process to the extent that it creates an incentive to share information about the blockchain in order (i) to make it effective against third parties and (ii) to encourage other users to share information (sense of community).³⁰ In the words of Fred Ehrsam, “*while some blockchain-based data will be encrypted and private, much of it will also be open out of necessity...this open data has the potential to commoditize the data silos most tech companies like Google, Facebook, Uber, LinkedIn, and Amazon are built on and extract rent from. This is great for society: it incentivizes the creation of a more open and connected world. And it creates an open data layer for AIs to train on.*”³¹

The incentive system of public blockchains also creates a strong motivation for potential users to join a platform as soon as possible, contrary to what happens on digital platforms as we know them today. This results in a weakening of these traditional platforms against blockchains whose users have an interest in quickly joining the community — and not only once the network effect is created. This difference between “*network effects*” and “*token effects*” (network effects on blockchain) also lies in the fact that tokens help “*overcome the bootstrap problem by adding financial utility when application utility is low.*”³²

²⁴ Michael Spence, *THE NEXT CONVERGENCE: THE FUTURE OF ECONOMIC GROWTH IN A MULTISPEED WORLD* (Picador, 2012).

²⁵ Ben Thompson, *Antitrust and Aggregation*, STRATECHERY (April 26, 2016) <https://stratechery.com/2016/antitrust-and-aggregation/>.

²⁶ *See id.*

²⁷ *See generally* David S. Evans & Richard Schmalensee, *Debunking the ‘Network Effects’ Bogeyman*, 40 REGULATION 36 (2018).

²⁸ Rhys Lindmark, *Macro Blockchain #1: The End of Aggregation Theory*, TOKEN ECONOMY (June 6, 2017).

²⁹ *See* Neil Gandal & Hanna Halaburda, *Can We Predict the Winner in a Market with Network Effects? Competition in Cryptocurrency Market*, GAMES (2016): “*While Bitcoin essentially dominates this market, our data suggest no evidence of a winner-take-all effect early in the market.*” Also, Abeer ElBahrawy, Laura Alessandretti, Anne Kandler, Romualdo Pastor-Satorras & Andrea Baronchelli, *Evolutionary dynamics of the cryptocurrency market*, R. SOC. OPEN SCI. (2017).

³⁰ As underlined by Eric Posner, Marx and Weber have argued that market—or, capitalism—undermines community, *see* Eric A. Posner, *LAW AND SOCIAL NORMS 221* (Cambridge, MA: Harvard University Press, 2009). Blockchain, which is driven by capitalism, proves this analysis to be incorrect.

³¹ Fred Ehrsam, *Blockchains are a data buffet for AIs*, MEDIUM (March 6, 2017).

³² Chris Dixon, *Crypto Tokens: A Breakthrough in Open Network Design*, MEDIUM (June 1, 2017) <https://medium.com/@cdixon/crypto-tokens-a-breakthrough-in-open-network-design-e600975be2ef>.

In fact, token effects sort out the bootstrapping problem by creative different sorts of incentives.³³ Initial Coin Offerings³⁴ are one of them because they drive the buyers to make the blockchain prosper³⁵ in order to make their tokens valuable.³⁶ Other blockchains give away tokens,³⁷ which is called an “*airdrop*.”³⁸ We can imagine all kinds of conditions to get these tokens for free: the creation of an account *via* a social network³⁹ in order to share some information as the contact list, proof of the possession of other tokens,⁴⁰ for example, which may possibly create anti-competitive concerns.

As a result, interest in joining a new blockchain can be extremely high, potentially putting rapid and powerful competitive pressure on market leaders. The European Commission will have to take this into account when deciding if a company is engaging in anti-competitive practices. This shouldn't stop authorities from acting when harm to consumers is established, but it raises at least two fundamental questions: how to evaluate whether a company is truly dominant and how competition authorities should be allocating their resources.

III. The two combined: predatory innovation & blockchain

Predatory innovation and blockchain can be combined to cause great harm to the consumer, notably by ejecting competitors from the blockchain. This is especially true of private blockchains (i.e. blockchains that rely on verification by permissioned).

³³ For instance, Steemit - a decentralized Reddit-like token network - makes payments to users who post and upvote articles.

³⁴ Paul Vigna, *What's an Initial Coin Offering? ICOs Explained in 11 Questions*, WALL STREET JOURNAL (October 2, 2017) <https://www.wsj.com/articles/whats-an-initial-coin-offering-icos-explained-in-11-questions-1506936601>. Christian Catalini & Joshua S. Gans, *Initial Coin Offerings and the Value of Crypto Tokens* (2018), explaining why “*ICO mechanism allows entrepreneurs to generate buyer competition for the token, which, in turn, reveals consumer value without the entrepreneurs having to know, ex ante, consumer willingness to pay.*”

³⁵ For “*a taxonomy of initial coin offerings,*” see Dirk Zetsche, Ross P. Buckley, Douglas W. Arner & Linus Föhr, *The ICO Gold Rush* 6 (2018).

³⁶ But see Christian Catalini & Catherine Tucker, *Seeding the S-Curve? The Role of Early Adopters in Diffusion* 1 (2016): “*We then show not only that natural early adopters are more likely to reject the technology if they are delayed, but that this rejection generates spillovers on adoption by their peers who are not natural early adopters.*”

³⁷ For instance, Mstoken, Bethereum, Sharelectric, Xriba, ConcertVR, Blockport, Wt, Articlex. For more details see *What new ICOs are giving away free tokens right now?*, QUORA. To track them, see <https://airdropalert.com>. See also Paul Vigna & Michael J. Casey, *THE TRUTH MACHINE: THE BLOCKCHAIN AND THE FUTURE OF EVERYTHING* 103 (St. Martin's Press, 2018): “*Brave's model included a token-issuance strategy for dealing with that challenge. It set aside a 300 million-strong “user growth pool” to attract new users. There's a plan, for example, to deliver a small amount of BATs to the integrated Brave wallet whenever there's a unique new download of the browser. In this way, the token is designed as a tool to bootstrap adoption, to foster network effects.*”

³⁸ This is also called “*coin drop,*” see Melanie Swan, *BLOCKCHAIN: BLUEPRINT FOR A NEW ECONOMY* 73 (O'Reilly Media, 2015).

³⁹ See for instance <https://topicolist.com/airdrops/kasko2go> or <https://topicolist.com/airdrops/avinoc>.

⁴⁰ See for instance Pioneer Badge which requires ERC20 tokens (based on Ethereum) <https://topicolist.com/airdrops/pioneer-badge-program>.

When the blockchain governance is modified,⁴¹ it could be seen as an innovative practice — being a new product. Such a situation is similar to the one of a software company uploading the new version of one of its products. And where there is innovation, there is a risk of “*predatory innovation*” which, once again, we define as “*the alteration of one or more technical elements of a product to limit or eliminate competition.*”⁴²

In the words of Ethereum creator Vitalik Buterin, “*the consortium or company running a private blockchain can easily, if desired, change the rules of a blockchain, revert transactions, modify balances, etc.*”⁴³ This is predatory innovation through blockchain. Such practices are expected to be more common on private blockchain where a change in the rules is easy and does not require any approval from the users. In fact, immutability is a characteristic that is shared only among open decentralized peer to peer blockchains and it does not apply to private blockchains. Accordingly, private blockchains can modify their governance design anytime as they do not need to convince any user to adopt the change. And predatory innovation could be made on public blockchains as well if the new governance design is adopted by a majority of the miners. But this seems unlikely at this time, first, because any change to the public blockchain governance design requires coordination and consensus among all of the stakeholders,⁴⁴ and second, because it is impossible to “*replace*” the original blockchain.⁴⁵ When it is done, a “*hard fork*” is created,⁴⁶ a copy of the ledger is made and miners switch their hardware (hashing capacity) to the new governance design. If they do not, the software running under the old rules see the blocks produced according to the new rules as invalid, which creates a situation in which the original blockchain is split into multiple blockchains.⁴⁷ Therefore, as the community grows on public blockchains, it becomes increasingly difficult to reach a consensus on changing governance.⁴⁸ But let us already note that the future introduction of new governance models in public blockchain will reduce these difficulties and thus facilitate predatory innovation.

⁴¹ Peder Østbye, *The Case for a 21 Million Bitcoin Conspiracy* (March 2018): “*certain stakeholders may have a more influential roles than others. As just explained, block-validators play such a role. There is a risk of concentration among such validators, which increases their influence. If changes in the protocols are to be implemented, it is ultimately the block-validators that must execute these changes.*”

⁴² Thibault Schrepel, *Predatory Innovation: The Definite Need for Legal Recognition*, SMU SCI. & TECH. L. REV (2018).

⁴³ Vitalik Buterin, *On Public and Private Blockchains*, ETHEREUM BLOG (August 7, 2015) <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/>. In fact, this is a “*godmode.*” The blockchain owner can freeze any account or move the funds away; but chances are that people will eventually discover it and sell all the stocks/securities/tokens.

⁴⁴ But still, no rule is set in stone, since they can all be modified with a broad consensus.

⁴⁵ This subject is being discussed. The creation of an hard fork depends on the governance system. Some blockchains, according to the chosen governance, will thus allow a modification of governance without the creation of hard forks.

⁴⁶ Joon Ian Wong, *Everything You Need to Know about the Ethereum Hard Fork*, QZ.COM (July 18, 2016) <https://qz.com/730004/everything-you-need-to-know-about-the-ethereum-hard-fork>.

⁴⁷ To read about the Ethereum “hard fork,” see Kevin D. Werbach, *Trust, But Verify: Why the Blockchain Needs the Law*, Berkeley Tech. L.J. Forthcoming: “*Whether or not the Ethereum Foundation made the right call, the fact is that the controversy raised questions that could not be answered within the framework of the blockchain. They required appeal to some higher-level principles. The viability of trustless trust is ultimately a matter of governance.*”

⁴⁸ Patrick Murck, *Who Controls the Blockchain?*, HARVARD BUSINESS REVIEW (April 19, 2017) <https://hbr.org/2017/04/who-controls-the-blockchain>.

In addition, there are reasons to believe that predatory innovation may be particularly effective on blockchain and, therefore, a common practice. First of all, predatory innovation on blockchain is *cheap* as it can be implemented at no cost. Its implementation can also be very *fast*, in fact, interactions/validations *via* blockchain only take a few seconds or minutes at most. Although transactions and modification are not *invisible* on public blockchain, they can be on private blockchains — the access to information and the history of the blockchain can be limited to some users. And predatory innovation on blockchain can have a *radical* effect: it will produce immediate effects by excluding a targeted user which also is a competitor. Lastly, predatory innovation practices can take *different forms* with multiple effects, beyond the mere exclusion from the blockchain. A company that owns a private blockchain can indeed modify its governance design so that a user's access is purely and simply denied, or, to a lesser extent, that the user can no longer read all the information on the blockchain, register transactions or take part in the block validation process. Of course, a poorly designed blockchain operating rules to the detriment of some users would be unattractive, hence the interest to modify it once its adoption is generalized or to make some transactions not visible by all.

Here lies a similar problem to the one related to the platforms that we know today. The modification of blockchain governance may create issues while the initial choice of the type of blockchain — public, private... — should be exempt from competition law scrutiny,⁴⁹ although the type of governance that is chosen indicates the likelihood of anti-competitive practices being committed. But what is particularly worrying is that our legal concepts are blind to the full extent of this type of practice. Two concepts are generally used to analyze what is actually predatory innovation — *tying*⁵⁰ and *leveraging*,⁵¹ but they are ineffective. *Tying* is inoperative to the extent that, with blockchain, only one product is involved. Moreover, it may not be sold — at least its access — and for this reason too, tying would be ineffective. *Leveraging* is unenforceable as well because, in the absence of two separate markets, it cannot be used. This concept is also ineffective when only one competitor is foreclosed but a wide competitive field remains active.

In short, predatory innovation is — for the time being — subject to several legal rules that are ill-adapted.⁵² And yet, it is one of the most anticipated and dangerous anti-competitive unilateral strategies that can be implemented on a blockchain. This should raise questions about the need to adapt our legal rules to a blockchain — and more broadly, about the role of the regulator.

IV. Fines calculation

⁴⁹ Hanno F. Kaiser, *Are “Closed Systems” an Antitrust Problem?*, 7 COMP. POL'Y INT'L 91, 102 (2011).

⁵⁰ For instance, *Telex Corp. v. Int'l Bus. Machs. Corp.* (Telex 1), 367 F. Supp. 258, 347 (N.D. Okla. 1973); also, *United States v. Microsoft Corp.*, 253 F.3d 34 (D.C. Cir. 2001).

⁵¹ See *C.R. Bard, Inc. v. M3 Sys., Inc.*, 157 F.3d 1340 (Fed. Cir. 1998). Also, Richard S. Markovits, *ECONOMICS AND THE INTERPRETATION AND APPLICATION OF U.S. AND E.U. ANTIRUST* (Springer 2014); Alan Devlin. & M. Jacobs, *Anticompetitive Innovation and the Quality of Invention*, 27 BERKELEY TECH. L.J. 1 (2012).

⁵² See Thibault Schrepel, *L'INNOVATION PRÉDATRICE EN DROIT DE LA CONCURRENCE* (Larcier, 2018).

According to Article 23(2) of Regulation No 1/2003, the fines imposed by competition authorities cannot exceed 10% of the overall annual turnover of the concerned company. This limit is intended to avoid disproportionate sanctions that would jeopardize the company's future. In practice, however, while this turnover threshold is useful, it can be inadequate. The digital economy requires companies to compete by innovating. R&D investments have become the lifeblood of the digital economy and the very essence of competition. The specific competitive dynamics of the industry should also be taken into account in considering the extent to which fines imposed by competition authorities can disrupt the investment capacity of companies.

We have found indeed that a vast majority of the European Commission's fines represent a very high percentage of what companies invest annually in R&D. As a matter of fact, an empirical study³³ conducted over the period 2004 to 2018 (Android included) on all the fines imposed by the European Commission on the basis of Article 102 TFEU shows that the imposed fines represent on average 277% of what companies invest annually in R&D. The percentage is significantly lower — 166% on average — for companies with annual sales of more than one billion euros. As for companies operating in digital sectors with an annual revenue of more than one billion euros, the fines represent 21.7% of their annual R&D investment on average, which remains considerable insofar as the three targeted companies (Qualcomm, Google and Intel) have increased their R&D spending up to, respectively, 4.9 billion, 15.1 billion and 5.65 billion euros.³⁴ And lastly, let us note that several fines are out of any kind of proportion. This is particularly the case for those pronounced against OPCOM, ARA Foreclosure and Telekomunikacja Polska, which respectively reach 909%, 600% and 907% of their R&D investment.

Even for the largest companies, these fines are highly likely to force them to cut their R&D investments, or, at least, to slow them down. No company can be fined several hundred million euros — or several billion — without its R&D budget being impacted, regardless of its profits. The structure and organization of companies do not allow them to absorb such fines without it affecting one of their most significant sources of expenditure.

Given the possibility that innovation could be affected by fines even within the upper global-revenue-based limit, and given the double effect on consumers, agencies and legislatures should undertake further investigation of the relationship between fines and innovation and if appropriate introduce caps on fines that are relative to investment in innovation rather than global revenue. This is necessary to ensure that innovation is not curbed by greatly reducing the investment capacity of companies, whether or not they have been partially enriched through the breach of competition rules. It hence seems appropriate to take account of this in the context of assessing the quantum of the fines imposed by competition authorities, in particular on the basis of Article 102 TFEU where effects on competition are often being discussed.

³³ Thibault Schrepel, *The European Commission Is Undermining R&D and Innovation: Here's How to Change It*, ICLE ISSUE BRIEF 2018-2

³⁴ Amounts spent on R&D in the year of the sanction.

If we are to acknowledge the need to cap the fines imposed by competition agencies, we must also ensure that they actually promote competition rather than setting them at such high levels that they do not. The 10% turnover cap is inappropriate as it fails to ensure the proportionality of fines imposed in digital sectors. In fact, one may wonder why such fines should vary so widely as a function of turnover, let alone of innovation.

A new cap should therefore be considered,⁵⁵ and we propose doing so by limiting the fines to a certain percentage of companies' investment in R&D.⁵⁶ Indeed, although sanctions are not calculated on the basis of companies' investment in R&D, this investment must be taken into account when calculating the fine. Presumably no company would have an incentive to voluntarily reduce its investment in R&D over the years for the sole purpose of obtaining a smaller sanction in a possible, though unlikely, competition law decision at an unknowable date. Such a mechanism should therefore have no adverse effect on firm behavior, and, conversely, would provide better protection for innovation.

And, as matter of fact, structural and behavioural remedies may also have a direct impact on innovation, regardless of the size of the firm. The latter are not subject to any proportionality control which simply limits the amount of the fines. It may therefore be necessary to introduce such a control and/or limitation mechanism to behavioural remedies, as well, lest the failure to take R&D into be reflected in these remedies as well. Behavioral remedies that are supposed to correct abuses but nevertheless deter competition are not remedial. In the end, the consumer would benefit from such limiting mechanisms by not suffering two damages: the first because of anticompetitive practices and the second because of sanctions that penalize innovation.

*
* *

⁵⁵ For more on this, *see* Thibault Schrepel, L'INNOVATION PREDATRICE EN DROIT DE LA CONCURRENCE, 549-550 (Larcier, 2018).

⁵⁶ It is up to economists to establish the optimal level of this threshold.