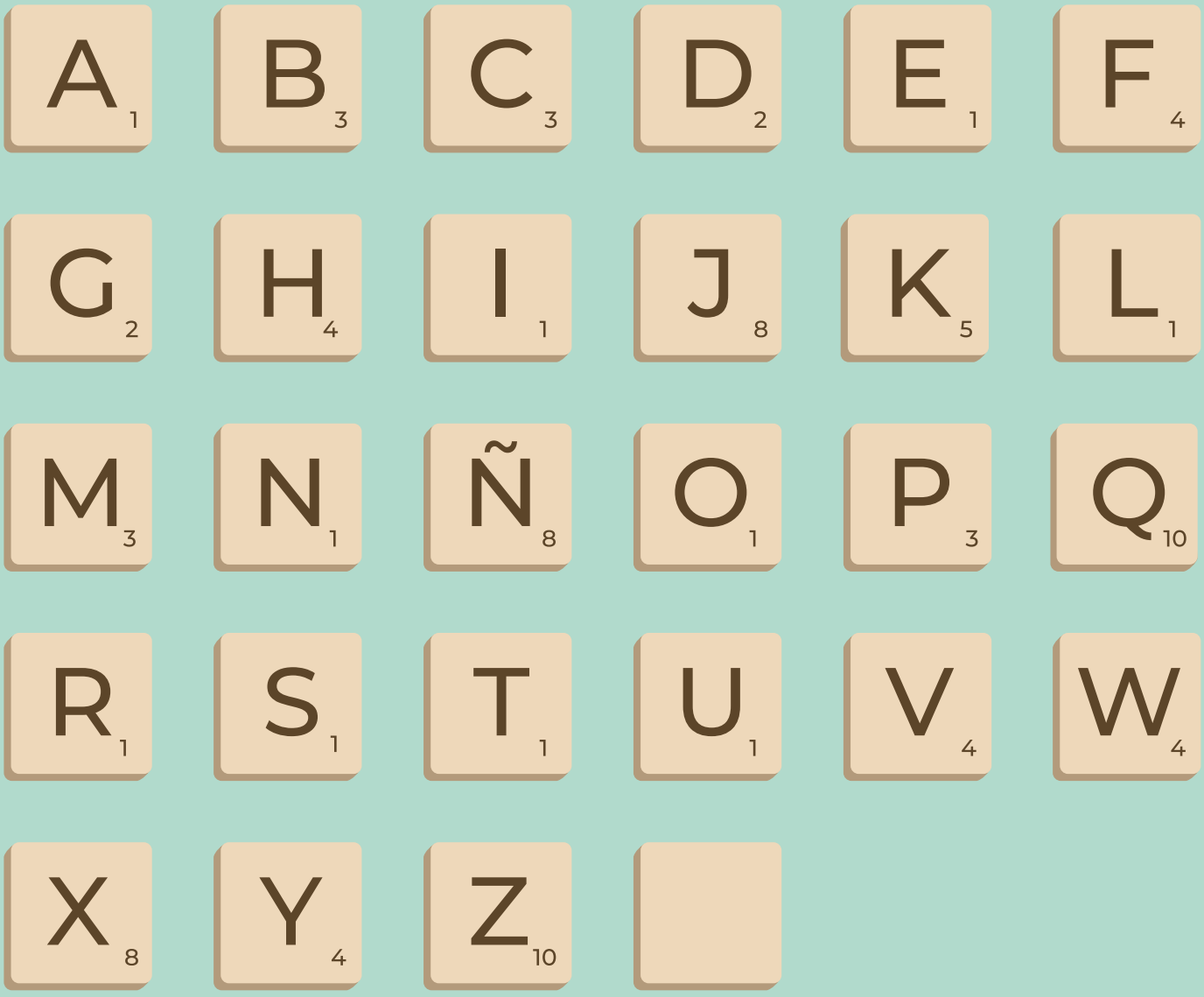
Tech REG CHRONICLE™

EDITORIAL BOARD EDITION

AUGUST 2022



CPI COMPETITION POLICY INTERNATIONAL™

Competition Policy International, a What's Next Media and Analytics Company

LETTER FROM THE EDITOR

Dear Readers,

In this August edition of the TechREG Chronicle, we host a selection of articles from our esteemed Editorial Advisory Board. This set of contributions opens with a TechREG Talks discussion between **Philip Marsden** & **Jacqueline Downes**, moderated by **Katharine Kemp**. The panelists discuss the pressing issues facing legislators, regulators and litigants throughout the world as the regulation of online platforms appears on the policy radar to an ever-greater extent, particularly insofar as it relates to the protection of consumer rights, online privacy and expanding antitrust legislation.

Martin Cave discusses the trend of "softwarization" in certain industries. Advances in data and digitalization create substantial opportunities for cost savings and enhanced competition in many network industries subject to regulation. Softwarization refers to innovations which reduce the need for hardware assets; these can be not only code, but the use of any smart asset, algorithm or economic tool across the whole value chain. Two sectors are considered. In mobile communications, the scope for digitisation and the starting level of competition are high; in electricity, both are substantially lower.

Katharine Kemp follows, with a timely piece on the theme of anonymization and data privacy. Representations in online privacy policies that certain data is anonymous or "not information that personally identifies you" can have significant consequences. They may indicate that a firm considers the data to be outside the scope of data protection regulation, and/or give consumers the impression that this is data which

cannot have an individual impact; for example, that it will not add to the individual consumer's profile. However, there are a growing range of data practices and services offered by adtech and data analytics providers that do affect individuals' privacy while claiming not to use personal information. The article argues that such claims require tighter regulation.

Turning to crypto, **David S. Evans** tackles the question of how to regulate so-called stablecoins. Such decisions should be based on crypto's past and present and discount overly optimistic forecasts of its future. The past demonstrates public blockchains cryptocurrencies are highly volatile; main blockchains have no mechanisms for ensuring stability; and that after 13 years there are unfulfilled promises and no widespread use of cryptocurrencies for productive purposes. The present shows that speculation is the main use case for currencies with the leading exchanges investing in feeding hype with celebrity-studded ads among other things. There is hard evidence that lax regulations of stablecoins, combined with the inherent volatility of the native cryptocurrencies result in the classic systemic financial risks from runs and contagion.

Liyang Hou & Shuai Han turn to the question of platform regulation. The fast expansion of the digital sector has raised regulatory attention across the world. In order to maintain competition, major economies have proposed legislative drafts to regulate digital platforms. This article offers a comparative view on those drafts in China, European Union, and the United States, and submits suggestions for future revision for the Chinese drafts.

Mihir Kshirsagar looks to how consumer protection regulators across a variety of jurisdictions are taking on the challenge of combating so-called "dark patterns" online, through targeted enforcement actions and new rulemaking initiatives. Broadly speaking, "dark patterns" are user interface techniques that benefit an online service by leading users into making decisions they might not otherwise make. Some are outright deceptive, while others exploit cognitive biases or shortcuts to manipulate user actions. But businesses complain that authorities' newly found attention to the issue of dark patterns risks targeting legitimate persuasion techniques that have been long used in the marketplace.

As always, many thanks to our great panel of authors.

Sincerely,
CPI Team

TABLE OF CONTENTS

CPI COMPETITION POLICY™ INTERNATIONAL

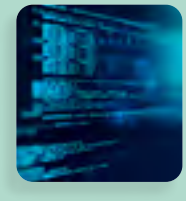
EDITORIAL BOARD EDITION

AUGUST 2022

SUMMARIES

TechREG Talks...
...with Katharine Kemp, Philip Marsden & Jacqueline Downes

In this edition of CPI TechREG Talks, we have the pleasure of presenting a summary of a discussion with Philip Marsden and Allens partner Jacqueline Downes, moderated by Katharine Kemp. This discussion was hosted by the UNSW Allens Hub for Technology Law and Innovation in Sydney, Australia on August 10, 2022. We thank all the participants for contributing to this discussion for CPI.

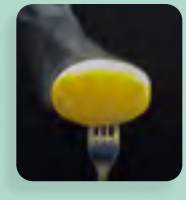


THE SOFTWARIZATION OF REGULATED NETWORK INDUSTRIES AND ITS CONSEQUENCES FOR COSTS AND COMPETITION
By Martin Cave

Advances in data and digitalisation create substantial opportunities for cost savings and enhanced competition in many network industries subject to regulation. By softwarization to mean innovations which reduce the need for hardware assets; these can be not only code, but the use of any smart asset, algorithm or economic tool across the whole value chain. The scale of the potential effect on costs of softwarization is linked to the weight of digitizable activities in the typically 'fused' digital and physical processes which make up network industries. Two sectors are considered. In mobile communications, the scope for digitisation and the starting level of competition are high; in electricity, both are substantially lower. In each case, the potential financial and structural impacts of such innovation are quantitatively significant. The paper also notes regulatory issues which may arise when owners of hardware networks may seek to limit the access to market of their new software competitors.

"A ROSE BY ANY OTHER UNIQUE IDENTIFIER": REGULATING CONSUMER DATA TRACKING AND ANONYMISATION CLAIMS
By Katharine Kemp

Representations in online privacy policies that certain data is anonymous or "not information that personally identifies you" can have significant consequences. They may indicate that the firm considers the data to be outside the scope of data protection regulation, and/or give consumers the impression that this is data which cannot have an impact on the individual; for example, that it will not add to the individual consumer's profile. However, there are a growing range of data practices and services offered by adtech and data analytics providers that do affect individuals' privacy while claiming not to use personal information, including persistent unique identifiers, data matching using hashed emails and other "identity resolution" services – practices which are not within most consumers' knowledge or understanding. Obfuscation about such activities may not only mislead consumers, but hinder competition on privacy quality by firms that seek to compete on the basis of genuinely privacy-enhancing features. This article argues that claims of anonymization and pseudonymization require tighter regulation under data protection law and should also be rigorously scrutinized under consumer protection law for potential misleading conduct.



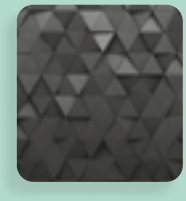
THE CASE FOR STRINGENT REGULATIONS OF STABLECOINS
By David S. Evans

Decisions on how to regulate stablecoins, and other parts of the crypto industry, should be based on what we know about crypto's past and present and discount starry-eyed forecasts of its future. The past demonstrates public blockchains cryptocurrencies are highly volatile; main blockchains have no mechanisms for ensuring stability; and that after 13 years there are unfulfilled promises and no widespread use of cryptocurrencies for productive purposes. The present shows that speculation is the main use case for currencies with the leading exchanges investing in feeding hype with celebrity-studded ads among other things. Crypto exchanges and other participants with a stake in the continued trading of currencies are now selling the "vision thing": a vague and distant future of a decentralized internet and financial system. Now we also have hard evidence that lax regulations of stablecoins, combined with the inherent volatility of the native cryptocurrencies have resulted in the classic systemic financial risks from runs and contagion. This article advocates for stringent regulation of stablecoins: fully backed with cash and short-term instruments, with a trustee, and in a regulated bank. It also argues for regulators going further to ensure stablecoins are not used to support unsafe applications.

CONVERGING PROPOSALS FOR PLATFORM REGULATION IN CHINA, THE EU, AND U.S.: COMPARISON AND COMMENTARY

By Liyang Hou & Shuai Han

The fast expansion of the digital sector has raised regulatory attention across the world. In order to maintain a competitive market and to promote healthy and fair competition, major economies have come up with proposed legislative drafts to regulate digital platforms. This article offers a comparative view on those legislative drafts in China, European Union, and the United States, and submits suggestions for future revision for the Chinese drafts.



WHY REGULATION OF DARK PATTERNS IS HERE TO STAY

By Mihir Kshirsagar

Consumer protection regulators across a variety of jurisdictions are taking on the challenge of combating online "dark patterns" through targeted enforcement actions and new rulemaking initiatives. Broadly speaking, dark patterns are user interface techniques that benefit an online service by leading users into making decisions they might not otherwise make. Some dark patterns deceive users, while others exploit cognitive biases or shortcuts to manipulate their actions. But businesses complain that authorities' newly found attention to the issue of dark patterns risks targeting legitimate persuasion techniques that have been long used in the marketplace. Alternatively, they complain that dark patterns are a squishy or amorphous concept and that the lack of standards creates an unacceptable degree of regulatory uncertainty. This article examines the future of dark patterns regulation for the tech industry and explains why the issue is not a passing fad. I argue that businesses should prepare for continued scrutiny of their practices and should develop proactive mechanisms to address regulatory risk.

WHAT'S **NEXT**

For September 2022, we will feature a TechREG Chronicle focused on issues related to **Connected Healthcare**.

ANNOUNCEMENTS

CPI TechREG CHRONICLES October & November 2022

For October 2022, we will feature a TechREG Chronicle focused on issues related to the **Behavioral Economics**. And in November we will cover **Interoperability**.

Contributions to the TechREG Chronicle are about 2,500 – 4,000 words long. They should be lightly cited and not be written as long law-review articles with many in-depth footnotes. As with all CPI publications, articles for the CPI TechREG Chronicle should be written clearly and with the reader always in mind.

Interested authors should send their contributions to Sam Sadden (**ssadden@competitionpolicyinternational.com**) with the subject line "TechREG Chronicle," a short bio and picture(s) of the author(s).

The CPI Editorial Team will evaluate all submissions and will publish the best papers. Authors can submit papers in any topic related to competition and regulation, however, priority will be given to articles addressing the abovementioned topics. Co-authors are always welcome.

TechREG TALKS...

...WITH

KATHARINE KEMP

PHILIP MARSDEN

JACQUELINE DOWNES

Katharine Kemp is Senior Lecturer at the Faculty of Law & Justice, at the University of New South Wales, Sydney. Philip Marsden is Deputy Chair of the Bank of England's Enforcement Decision Making Committee and Professor at the College of Europe. Jacqueline Downes is Partner, Practice Group Leader, Competition, Consumer & Regulatory at Allens.

In this edition of CPI TechREG Talks, we have the pleasure of presenting a summary of a discussion with Philip Marsden and Allens partner Jacqueline Downes, moderated by Katharine Kemp (Senior Lecturer at the Faculty of Law & Justice, at the University of New South Wales, Sydney). This discussion was hosted by the UNSW Allens Hub for Technology Law and Innovation in Sydney, Australia on August 10, 2022. We thank all the participants for contributing to this discussion for CPI.

Q1

We see abuse allegations before regulators and courts against various tech companies, both exclusionary (notably Amazon in respect of its competition with merchants on its marketplace, Google allegedly giving itself advantages over other ad tech providers; Apple preventing app developers from using other in-app payment systems, and so on), and exploitative (e.g. Meta's alleged excessive accumulation of consumer data as a condition of using their platform). In spite of all this activity, there is great dissatisfaction with competition litigation as a means of solving these issues.

Philip, by way of background, can you talk about what's going on globally in response to that dissatisfaction, especially in proposals for ex ante or upfront regulation, particularly in the EU and the U.S.?

Philip Marsden: As regards the U.S. and the EU, the substantive rationale for *ex ante* regulation tends to be structural problems relating to network effects and data accumulation. These can give firms an opportunity to exert market power and use it in some way, to exclude or to exploit. And that's substantially what the rationale is usually for enforcement action. But, one of the clear rationales for many governments getting involved in this now is also they feel that all of the many cases that have happened so far have either happened too slowly, or remedies have been completely ineffective or too late.

The intellectual market has moved on, so to speak. And so, this kind of surgical approach that competition authorities try to have with respect to *ex post* enforcement has been used as an excuse to say, "No, actually we're not going to go surgical, we will go much broader and much much earlier." And I think the biggest, best example of the broad, early approach (which I don't agree with in its details though) is the European approach. I was very excited when the European Digital Markets Act or DMA was being proposed, but when you actually saw the provisions, it seemed that they were too general, and they didn't seem to be self-executing at all.

By that, I mean I don't think the platforms can understand what some of the provisions mean with respect to some of their business practices, and therefore you wouldn't necessarily instill a culture of compliance in tech firms the EU. And therefore, that's why I've said that I think that the European Commission is "coding for infringements" and therefore huge fines. And so just an extraction of rents from the platforms and then appeals. And then 18 years later, we may get a judgment that the actual conduct at issue was not illegal, or if

so, there might not even be a means to prevent the conduct in some ways. So that approach, if I'm right, isn't particularly effective, though it does mean that the legislature — and this might resonate in Australia — gets to say, we've done a bunch of studies, we've enacted a law, and look, we've had some violations, and the big fines that go to the Treasury. But the market hasn't changed, then it's been no improvement.

The U.S. approach is extremely politically driven, and they have a similar approach in that sense, but the legislative provisions being proposed are much more detailed. But because the U.S. is steeped in litigation, they have a tendency towards using litigation as a model of enforcement to really bolster the *ex ante* regulation, and especially class actions. Class actions are all over the place in the U.S. In the UK, there's scores of them already that are starting up against all the big platforms. And I don't think that's been a particularly helpful model at all. It's obviously something that can complement regulation or enforcement, but I think it's, again, something that doesn't necessarily change behavior. It extracts rents or compensation. I'm more interested in stopping the harm in the first place.

In the UK, we are thus trying a bespoke model: it is focused on the actual business operation or service that's at the core of the platform, and that we are actually concerned about, as opposed to a general ban on self-preferencing, say, or a general mandating of data sharing by all platforms. We're tackling each platform in a different way, whether it's a commerce platform or communications or another kind of platform, and saying, we have a number of complaints in this area, a number of concerns, and what justifications might you have, and what can we together – government and business - do about it? And we're hoping that, through a dialogue, we will discover that platforms might either say "we're not even discussing that with you because that is core to our business model" or "actually, we've done that for many, many years, we've never had any complaints about it, but if you are so concerned, we could lose it."

We're trying to do this in a very hopeful, optimistic way. We think that, through dialogue, we can create a code for each platform's business line that is relevant to our concerns, and then ideally instill a culture of compliance, because compliance officers will be appointed within each platform. And they would be responsible regarding a report about how they comply, signed off by the board ideally.

Of course, the immediate criticism would be that you're going to get really nice compliance reports every year that say "everything's fine at Amazon," for example. And then, who's going to judge whether it is or not? My plea for the CMA — and so far they've been doing this really well — is to hire scores of experts in data and data analytics, digital science, etc., to be able to help assess whether or not these compliance programs are legitimate, and whether or not the concerns have been addressed, because a lot of these issues are far too technical, with respect, even to lawyers and economists, and you need to actually have the tech people to judge the technical work.

I'm hoping that model will proliferate a little bit. I have a feeling that across the channel from the UK, there's just going to be a *per se* prohibition resulting in tons of fines; that the businesses might adjust to that model; and the UK looks too soft. But of course a key finding of our Furman Report was that in moving in the direction of ex ante regulation, we're trying not to kill innovation at the same time.

Q2

Jacqui, to bring us back to Australia, these developments certainly haven't gone unnoticed here. We've had the ACCC Digital Platforms Inquiry earlier, and various proposals and recommendations following on from that. Can you give us an outline of what's happened locally and what you expect will happen from here?

Jacqueline Downes: The ACCC really kicked off this globally back in 2017 with its original inquiry into the impact of digital platforms on local media, and at that time really none of the overseas regulators were paying a lot of attention other than the Google Shopping case in the EU, certainly not from a legislative point of view, until this groundbreaking report. And of course, the result of that report was the implementation of the News Media Bargaining Code, which I'll talk a little bit more about later. But what it also did was highlight a whole lot of other issues that the ACCC felt it needed time to explore.

And so that led in 2020 to a referral from the government to conduct a five-year six-monthly review of digital platforms. And effectively the way the ACCC has been approaching that over the last couple of years now is every six months to issue a new interim report dealing with a different type of digital platform or area of digital platform involvement. They've indicated they may come back and review those different areas as the five years rolls on. But so far, they've issued interim reports in online messaging, app stores, ad tech, web browsers and choice screens for example. What they're doing this year is using their interim report for this six months to consider *ex ante* regulation. So, this report is due to be produced to government in September. We don't yet know when it might be released publicly.

But it's been reviewing this since February this year. And so the discussion paper this year seeks stakeholder views on the need for *ex ante* regulation, because of a perceived ineffectiveness of, as Philip as said, competition and consumer laws, really focusing on questions around the length of time it will take, and also that the number of different issues and the fact that taking a court case or opening a particular investigation by the ACCC really has to be quite fact-specific. I think the way in which the ACCC is seeing this, similar to overseas regulators, is there's general trends that go through various different platforms, various different industries, and this is best dealt with by some form of *ex*

ante regulation rather than picking issues off one by one. So, it's no surprise that it has taken a look at some of the overseas models that have already started to develop and asking stakeholder views on those models, including an outright prohibition in legislation of certain practices, similar to the Digital Markets Act and, and the American Online Choice and Innovation Online Act. This is the prescriptive approach which will just prohibit various forms of conduct, such as, data aggregation, self-preferencing, exclusivity, and so forth. They've asked for comments on that, and I am interested in Philip's views around the challenges with that, because you can certainly see how that may also lead to a lot of litigation.

The other model they're looking at is codes of practice. I think they feel they've had a fair degree of success with the News Media Bargaining Codes, so could something similar be developed perhaps also looking at the way in which they're using codes in the UK to regulate practice? I suppose one concern is that if they are voluntary codes, if you're requiring cooperation from the platforms, have we really seen evidence of willingness to cooperate to date? And so is that kind of wishful thinking, Philip? I'm interested in your views on that.

Rule-making powers is another area, similar to what we have in the energy space with the Australian Energy Regulator, having the power to develop and implement tailored rules specific to digital platforms. Of course, this gives the ACCC a lot of power, so there are concerns around that and there would certainly need to be some checks and balances. Measures to promote competition — another one that's developed from the UK approach where the ACCC could potentially impose a specific measure on a platform following a finding of consumer harm — again, I think you really need to look at the checks and balances there.

And then the third is that because a lot of these platforms are considered to be essential facilities potentially, is a sort of an access regime type arrangement like we have for natural monopolies in Part III A and Part XIC of the Act. It's unclear at this stage, the review is ongoing, and the ACCC has given some indication of some areas it's really thinking of focusing on and they include anticompetitive conduct. It could be dealt with under the Competition Act and more specific measures be implemented in *ex ante* regulation to deal with issues such as self-preferencing, exclusivity, etc., measures to improve data advantage such as data interoperability and portability, protecting consumers. The ACCC has also been looking to enhance consumer protection for a while, specifically unfair dealing between the platforms and the buyers. These are pretty broad topics, but they seem to be the areas that the ACCC is focusing on. In addition, I read recently that the new competition minister, Dr Andrew Leigh, has suggested that the government might implement interim measures in relation to digital platforms. So, it's safe to say the government is waiting on that report from the ACCC and it's keeping an open mind on what might need to happen. So that's where we are in Australia, Katharine.

Q3

Philip, before we go on, you mentioned the UK proposals, and I wanted to get an update on the bill's status in the UK, because I know that back in May, there was some controversy when there was a lot of anticipation around the time of the Queen's Speech, but some disappointment about the progress of the UK Bill. Where are we at now and why?

Philip Marsden: I shouldn't have faith in the current UK government necessarily for a range of reasons. But the actual civil service, the monolith itself below the political froth, is actually reasonably respectable and once it starts moving, it's like the wheels of the gods, I mean, they grind slowly but they grind exceedingly fine. So, one of the things that I take comfort in is that when I saw the news report from the FT and then immediately rang my contacts and asked why there is a delay to our Digital Markets Unit? The clever response I had back was that there are five online harms related bills going through, dealing with extremely important sociological issues, and this one odd DMU draft bill that may appear to be related essentially to commerce on digital platforms. So, politically, that looks like a dry, boring competition law and economics proposal, and there was a concern that politicians, when they get a hold of these many bills, will ask "What's this DMU one? We don't understand it really, let's hive it off." What they've decided to do, I'm told, is put the five really important ones through – the ones that actually deal with issues like platforms fanning teen anorexia and political revolt and all sorts of social problems and privacy breaches. The DMU bill is still moving forward in "draft." And because of that, the civil service is moving through drafting internal guidance, preparing the documents, preparing the codes, already talking with the platforms for some time about what these problems and solutions would look like.

I don't even really think it's a delay — as an eternal optimist — because they'd be doing that anyway. But the CMA has its dedicated unit. It's been there in shadow form for a while. They're going to be hiring scores of data scientists in the next year or two. It's a big deal for a competition authority to be doing something like that. Usually, it's a very tiny unit that exists, if at all. And they're beefing up their remedies units. I think it's all on track. The CMA is not like a cowboy shooting guns blindly: they're actually going to look really carefully at who they will shoot. (Laughter)

Q4

At the moment, in the U.S., there's a big ad campaign that's under the banner of "Don't Break What Works," sponsored by "big tech" among others. It is essentially threatening that people might lose their two-day Prime delivery and Google Maps. We've similarly

seen back when there was debate over the media bargaining code in Australia, certain threats or posturing by Google and Facebook.

Jacqui, what do you think about this kind of lobbying and strategic behavior? Do you think it is going to hobble or prevent the digital platform regulations that are being proposed?

Jacqueline Downes: There's certainly no doubt that the large platforms are very good at intensive lobbying, and, and I think with mixed results. I'm not really sure that the actions they took in relation to the news media bargaining code did them much service in Australia. You might recall firstly, Google had ads every time you searched something which told you how outrageous it is, but then Meta decided to pull news for a couple of weeks, including public safety, educational pages, right in the middle of a pandemic. I think that this particular action, particularly by Meta, had more of an impact of harming their stance.

There were some further developments in the news media bargaining code after that, but ultimately the news media bargaining code was adopted. And the intention of the code was effectively fulfilled. Over $200 million of deals reported by the ACCC have been made under that code. The lobbying didn't really have the desired effect. And I do think that there is a sense that the more we hear this from the large platforms, the more it undermines their position and makes regulators and government think there is something to be worried about here.

Q5

Moving into the territory of privacy (and there is some crossover here between these types of regulation), what we're tending to see in some cases with the platforms, is that they are essentially regulating privacy standards for other players in the market.

For example, we see Apple with its App Tracking Transparency framework, and its lack of access to contactless payments infrastructure on its iPhone on security grounds. And then Google, with the impending third-party "Cookie Armageddon" that is creating a lot of consternation among other players and a potential conflict between privacy interests and competition interests. How do you think we might address that potential conflict?

Jacqueline Downes: It's a difficult question. I don't purport to be a privacy expert, but I do see some difficulties in that intersection between protecting privacy and promoting competition. And I think we have seen examples where some of the larger platforms might use the privacy cloak, in fact, to protect their position. And so that, you know, it's more difficult for others to compete.

One example of this is the way in which platforms offer consumers the ability to opt out of individual apps collecting data. That really denies those app developers the ability to obtain data that is useful in their own product development. But often times, the platform itself is still collecting that data. I think there are real issues that have to be determined around who owns the data. Is it the consumer? Should they have complete control over that data? Who has the ability to use the data? Is it the platform? Or is it the content developer that then has the ability to use that data?

These are really difficult questions because obviously, as consumers, we all believe that we should have a degree of control our data. But also, it's in our interest to ensure there is a fair degree of competition. It's a really difficult question, but I think one that regulators definitely need to be turning their minds to.

Philip Marsden: One of the things about managing a situation like that is you have to have simplicity. It boils down to simplistic choices, and that means there's all sorts of gaming that can happen around how a given system is designed. But one of the things that we've learned in the EU is that competition officials thought the GDPR was not going to be very helpful from a competition point of view. I'm speaking as a competition official and almost every competition authority, as the GDPR was being drafted, observed that there was a range of areas here that might have odd consequences: you may actually entrench market power and entrench, certain privacy standards by a big player that may not be the best standards.

We've learned from that mistake. It's not like the competition authority is pleading to have a say, rather that privacy people should now be obliged to check with the competition authority about whether a given measure could be implemented in the least anticompetitive manner possible.

Q6

Another area where we need to look at potential overlap and even duplication — perhaps rather than conflict or tension — is between privacy regulation and consumer regulation. In the past couple of years, we've seen the ACCC taking enforcement action along the lines of the kind of proceedings that the U.S. FTC has brought over the years, alleging misleading conduct in respect of privacy notices, and some privacy settings. As no doubt, many of you will be aware, in the action against Google in the Federal Court, the privacy settings in respect of location tracking were found to be misleading.

The question is whether companies who are designing their privacy policies and privacy notices, should have to fit in with both the Privacy Act and the Australian Consumer Law says? Should it be enough that they have complied with the Privacy Act?

Jacqueline Downes: They're both laws of the country. One of the interesting things is that the actions that you mentioned the ACCC has taken against, for example, Google and Meta and others, alleged misleading conduct in relation to the disclosure of private information and the extent to which data was collected. I think our view — and I've spoken to privacy experts on this — is that this case could have been taken as a privacy action. So there actually was a breach of both or, or potentially breach of both. What is interesting is the fact that we are seeing the ACCC being more active still in this area and taking these actions as consumer law contraventions when potentially they could have been brought as privacy breaches.

We know that the ACCC and the privacy regulator are talking a lot and working these things out. But I don't think you're going to see the ACCC backing down on this anytime soon. Companies still need to ensure that not only are they complying with privacy laws, but also that whatever disclosures they're making, are complying with Australian Consumer Law.

Q7

Philip, the CMA put out recently a report in respect to online choice architecture, and some of the concerns raised there included concerns about deceptive design or what is sometimes called "dark patterns". Do you think that's the best description for these terms and where is the CMA headed on these issues?

Philip Marsden: I do think "dark practices" is the best description of these terms, because essentially you can't find your way out, you can't even see there's a problem, so it's a dark pattern. You can't find out how to decide or whether you even need to. Escape or switching for example is never one click away. I find it very interesting that no one has really complained too much yet that the CMA is actually getting quite close to product design here, which is what we're not supposed to do, as a competition authority. And yet that's the whole issue here.

There are complicated behavioral questions here. Look at your own behavior, whether it's revealed preferences or your stated preferences: how are you responding to given offers? False urgency. We've all felt this kind of frustration online. And there are, I think, some clear ways of resolving this, and this is why the competition authorities are negotiating with the platforms as to how this should be changed and what their concerns are. We need to remember that we're rationally lazy. We need simple mechanisms. Otherwise it just won't work.

This is an area where data teams are able to test in real time, using data sandboxes, to see what would happen if you set up a given remedy a certain way. This is not as possible in traditional markets, but in digital markets, if you get the platforms involved, it obviously is. We did this in open banking. Authorities can set up real-life A/B testing of algorithmic controls and remedies. Even though this extremely important financial consumer data was protected by the FCA in their sandbox, we could do tests to see how our remedies would work.

Ironically, it takes a really humble authority to do that. An authority with existing powers would rather simply take an alleged infringer to court. That's a very binary decision. It is very adversarial by definition, and it means you risk getting a remedy that might not actually work.

Q8

For one final question. we've seen in Australia this year a Consumer Policy Research Centre report on "dark patterns" following the ACCC's own report on choice screens. And the CPRC was pointing out various dark patterns, like the hidden costs or automatic additions to people's online shopping carts, "Hotel California" cancellation designs – "you can check out any time you like, but you can never leave."

Under Australian Consumer Law, some of these practices may be "unfair," but not necessarily "misleading." We've seen proposals for the introduction of an unfair practices prohibition in Australia to fill this gap. Jacqui, do you see that as necessary in this context.

Jacqueline Downs: Australia has very strong consumer laws already, and an extremely active regulator on the consumer front, unlike many other jurisdictions. And it rarely loses consumer cases in court. I don't think we need more laws at this point around consumer law. If there are some new practices that are concerning, they can be tested under current laws. There are laws on unconscionable conduct, unfair terms, and a range of other more specific laws. There has been a debate raging for a few years now about unfair practices. There is a real issue with introducing a very broad concept of an unfair practice. The ACCC as I said, is already having a lot of success dealing with privacy issues and data issues with existing provisions. Before we introduce new provisions, I think perhaps if some of these practices are harming consumers, they should be tested under existing law.

Philip Marsden: And just in contrast, the U.S. has an extraordinary array of consumer protection laws. And yet I think one of the most interesting elements in the next 12 months will be the introduction of expanded rule-making powers under section 5 of the FTC Act, which directly address these issues. And the U.S. wouldn't normally increase regulation or rule making or law making. That's just not the way they do things unless they thought it was a real problem. It would be interesting to see whether the Australian approach goes that way or the American version or something else happens. I do think there is a role for rulemaking here. It may be that yours are sufficient and that's fine, but the U.S. is definitely going to be taking a hard look at expanding the unfair practices legislation.


_mod = modifier_ob.modifiers.new("
object to mirror_ob
_mod.mirror_object = mirror_ob
ion == "MIRROR_X":
_mod.use_x = True
_mod.use_y = False
_mod.use_z = False
ation == "MIRROR_Y":
_mod.use_x = False
_mod.use_y = True
_mod.use_z = False
ation == "MIRROR_Z":
_mod.use_x = False
_mod.use_y = False
_mod.use_z = True
ction at the end -add back the desel
.select= 1
.select=1
t.scene.objects.active = modifier_
lected" + str(modifier_ob)) # modifi
_ob.select = 0
.context.selected_objects[0]
objects[one.name].select = 1
("please select exactly two objects,
OPERATOR CLASSES ----------
.Operator):
mirror to the selected object"""
t.mirror_mirror_x"
X"
ext):
t.active_object is not None

THE SOFTWARIZATION OF REGULATED NETWORK INDUSTRIES AND ITS CONSEQUENCES FOR COSTS AND COMPETITION

BY
MARTIN CAVE

London School of Economics. The views expressed belong to the author alone.

01 INTRODUCTION

The argument of this paper is simple and straightforward. It is that there are immense opportunities associated with the use of data and digitalization to achieve a combination of significant cost savings and the enhancement of competition in network industries, such as energy and telecommunications. In particular, competitive pressure in different forms can be imposed on the network component of the value chain, in many cases hitherto seen as being impervious to it. And this benefit can be achieved from innovation either within that component or upstream and downstream in the value chain.

This new element in network industries can be called the softwarization of network functions. In caricature, when there is a need to a need to replace existing network assets or when demand for a sector's end product has risen, the only solution available has been a hardware one - re-

placing an old transmission line, or building a new one (the latter being a process in the energy sector which in some jurisdictions takes as long as a dozen years). However, data and digitalization introduce new "software" possibilities, by which I mean the presence not only of code, but of any relevant smart asset, algorithm or economic tool across the whole value chain which can "replace" hardware assets. This can be done relatively quickly, and in some cases at a cost an order of magnitude or more lower than the hardware alternative.

> *This new element in network industries can be called the softwarization of network functions*

I illustrate these possibilities with two different examples. The first is mobile communications, where the traditional value chain (typically comprising a fiber fixed backhaul connection to a tower, which supports antennae giving access to a radio access network connecting the network's retail subscribers) relied on a local distribution technology which since its origins forty or so years ago has demonstrably been a natural oligopoly, rather than the then more generally observable natural monopoly in fixed communications. In fact, the number of mobile networks observable in advanced economies is now (and has for decades almost invariably been) either three or four, the outcome often depending on past merger control investigations, and probably including a fair amount of sharing of fixed assets.

In consequence softwarization of mobile does not introduce network competition where there was none before, but rather – in conjunction with a potentially game-changing new 5G technology - creates major new possibilities for competition, as described below, which have the potential to disrupt the industry's structure.

The second is the energy sector – where physical transmission and distribution networks are still bastions of natural monopoly. The recent focus in many countries on attaining net zero carbon emissions by 2050 implies a many-times-over increase in electricity demand – the generation and network hardware costs of supplying which would be enormous. But my definition of software includes anything from a demand reduction scheme which signs up a million households which allow their fridges to be switched off for an hour or so in the face of an expected increase in peak demand, or a time-of-day tariff which incentives householders to charge their electric vehicles ("EVs") overnight rather than in the evening, to carefully located battery storage which overcomes a bottleneck in a distribution network, or a real time "flexibility platform" which runs auctions in which a variety of firms can offer competing services which circumvent hardware capacity constraints. The multiplicity of options brings in many new potential providers to compete with the hardware monopolist.

In terms of the level of head-to-head competition in their pre-existing market structures, our two case studies lie pretty much at the opposite ends of the spectrum observable in sectors with local delivery networks. This is linked to a second broad underlying difference between them which arises from the nature and ease of the digitalization processes occurring within them. The communications sector was the first to be subject to a digital transformation, beginning in the 1980s. The same process for broadcasting started a little later. By now, all over the world, analogue communications exist mainly in small pockets and specialized uses.

Government digital strategies (not always fully implemented) for the whole economy or the public sector alone have appeared with increasing frequency in recent years. Consultancies have not only proffered advice on strategy but have prepared copious international league tables. For example, the Financial Times/Omdia Digital Economies index computes 16 digital economy measures for 39 countries for 2020-2024.[2] The measures comprise 2 for connectivity, 4 for devices or I0T, 2 for Enterprise ITspend, 6 for entertainment and 3 for payments.

The focus here on data transmission and communications is apparent and natural. However, whole economy digitalization requires the fusion of digital and physical processes. While data downloads and telephone calls require only the transport of bits, which may of course fulfil the aims of education or health, as well as of communication or entertainment, the provision of energy also requires such physical assets as gas pipes or electricity transmission networks, both of which may carry attendant risks to life and limb. Equally, the large-scale use of IoT based on a dense 5G network within an advanced manufacturing factory will involve physical processes, including major tangible capital assets, and other material inputs, at whatever geographical scale it is attempted. The degree of digital/physical fusion required in a sector's digital transformation has a big impact on what cost reductions and increases in competition can be achieved in it, and at what cost.[3]

02

SOFTWARIZATION IN MOBILE TECHNOLOGY[4]

In mobile communications, these developments are inextricably connected with the development of 5G, which in

2 https://www.ft.com/content/d6ebd098-3f81-4638-afba-b1a1a572163c.

3 As a further illustration of this point, compare the purely digital changes associated with development of ride-hailing platforms such as uber, with fusion of digital and physical processes associated with the use of driverless cars.

4 For more details on this section, see M. Cave, "5G and the wider goals of digitalisation in the EU," in E Bohlin & F Cappelletti (eds), *Europe's Future Connected: Policies and Challenges for 5G and 6G Networks*, ELF 2022 available at https://liberalforum.eu/wp-content/uploads/2022/06/Europes-Future-Connected_ELF-Study_Techno-Politics_vol.2-2.pdf.

some cases takes the form of a somewhat better version of 4G, often still using some 4G elements, but in another more expansive stand-alone version is capable of embodying much greater versatility and of delivering the speeds of 1 gigabit which (made universally available) are the target of digital strategies in several jurisdictions, including the EU.[5]

A. 5G Networks

5G is the first generation of networks to embed two key software features. The first is software defined networking (SDN). This transfers the functionality needed in the network such as switching and handover from hardware to software, enabling variation in services and functionality to be made more readily.

The second is network function virtualization ("NFV"). This involves implementing the functions of the communications infrastructure in software running on standard computing equipment, following the precedent of data centers, which went through a similar transformation. This reduces costs and simplifies the addition of new services. The framework for these developments has been standardized by bodies such as ETSI.

These two advances allow a single network to supply bespoke combinations of speed, latency, geographical coverage, and other attributes to meet their customers' varying needs. This is known as "network slicing." It also allows the provider of a digital education or transport service, for example, to buy connectivity at wholesale and bundle it with the rest of its service.

An early example of this is provided by Rakuten's 2020 5G network in Japan. A second is new U.S. Dish network in 2021.[6] According to The Economist the latter is "except for antennas and cables, mostly a cluster of code that runs on Amazon Web Services." This "cloudification" of networks brings new giant software firms into the game, competing in the same space as pre-existing hardware providers.
Finally, the above-noted Dish network adopts the practice of using different tiers of spectrum bands, known as versatile spectrum: "each band of the 5G spectrum will work together as best needed to provide more data capacity. By combining the bands, DISH Wireless ensures a better 5G network where all its spectrum works together towards a common goal."[7]

B. Changes in Competition

What else might happen in the marketplace? One possibility is wide-area coverage for niche applications. This may be needed to support a growing number of IoT applications with homogeneous geographical needs. Existing networks meeting enhanced mobile broadband needs and providers of niche services might be active here. Examples cited include smart metering, public safety networks and broadcasting.

A further example is the market for local coverage and capacity, meeting the needs of a group of contiguous end users, who may be a specified private interest group, such as a group of firms in an industrial park, a group of firms offering driverless vehicles, or individual members of a residential community.

In the limit, it could be a private network provided for a single firm. It is notable that AWS has announced a new managed service to help enterprises to set up and scale the new private 5G networks described below, and Ericsson has made an agreement with BT jointly to supply the same service in the UK.[8]

Spectrum regulators are increasingly preparing to make licenses available for such so-called verticals. In a recent German spectrum auction, the regulator reserved one quarter of available spectrum for such closed user groups, which can rent access for 10 years for €31,000 per square km. By mid-2021, 117 such licenses were approved. A less radical way of achieving the same end is to authorize or mandate localized spectrum sharing in appropriate bands.

Finally, many mobile operators have sold their masts to specialized companies, which now, particularly in the light of the above changes, have the capacity to integrate into network provision and become wholesale only operators.

In combination these changes have the potential to lead to a major shift in the structure of the mobile market.

03
SOFTWARIZATION IN THE ELECTRICITY SECTOR

As noted in the introduction, the electricity sector is far more capital-intensive and complicated than mobile communications and entails a much more thorough-going fusion of the digital and the physical. As a result, the developments I describe in this sector are much more diverse. I limit myself to describing two simple examples which illustrate my wide definition of softwarization set out above, and then note, under the more comprehensive rubric of flexibility (and flexibility platforms), the infinitely more varied and sophisticated set of measures which are currently under development.

5 European Commission, *Europe's Digital Decade*, 2021, available at https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade.

6 https://godish.com/dish-spectrum-holdings-and-5g-plans/ (accessed Jan. 10 2022).

7 https://godish.com/dish-wireless-versatile-5g-spectrum/.

8 *Financial Times*, May 31, 2022.

I also discuss one of the regulatory issues created by the emergence of this new form of competition to hardware.

A. A Simple Retail "Software" Illustration

Electricity must be consumed in the second it is produced (unless it is expensively stored – see below). Accordingly, the major hardware costs of generating capacity and networks have been dimensioned to meet the maximum load from business and domestic customers, which varies predictably by season, day of week and ambient weather conditions, generally peaking in early evening.

A wide class of demand-side reduction measures which pay customers on a more ad hoc basis to reduce consumption has been discussed and implemented for many years, in many variations and with respect to both business and domestic customers. But here we focus on a very simple means of reducing peak demand. This is time-of-day pricing, which encourages customers to switch to off-peak consumption times. This requires a meter which measures consumption in each 5, 10 or 30 minutes. Large business consumers have had this facility for many years, and many jurisdictions have dictated a universal roll-out of such smart meters to households.

The clearest opportunity for such time-shifting arises in connection with charging electric vehicles. Tariffs available overnight can be a small fraction of those at peak hours. Numerous trials over several years have demonstrated the large consumer response.[9] Customers can also install digital assistants which choose the optimal moment to charge vehicles or use other electrical equipment.

In some jurisdictions tariffs link the price charged directly to the spot price in the wholesale energy market. This subjects such customers to considerable risks. Thus when wholesale prices spiked dramatically in Texas in February 2021 as a result of very low temperatures, some customers were reported as having faced bills amounting to many thousands of dollars over a very short period.

However, such time-of-day pricing options may be most fully exploited by households which own EVs, have large premises and are digitally competent. Poorer and older households may end up continuing their previous consumption habits at now much elevated peak rates. This is a matter of concern to regulators which are charged with protecting such vulnerable customers.[10]

B. Wider Applications of Softwarization: Distributed Energy Resources and Flexibility Markets

The potential of digitalization ("smart energy") goes way beyond the above, and is driven by several factors. One is the increase in the role of weather-dependent (and hence intermittent) renewable sources of energy, which adds greatly to the complexity of balancing supply and demand. The second is the growing number of distributed energy resources ("DERs"). These are small-scale units of power generation that operate locally and are connected to a larger power grid at the distribution level. DERs include solar panels, small natural gas-fueled generators, electric vehicles, and controllable loads, such as electric water heaters. An important feature of a DER is that the energy it produces or stores is often consumed close to the source.

"The clearest opportunity for such time-shifting arises in connection with charging electric vehicles

This permits a broader change in the supply-demand paradigm, from one in which large and controllable power stations were required to adapt supply to a given demand, to one on which demand has to be made more elastic and controllable. This generates a need for so-called flexibility markets which bring together a large variety of different generation, storage, and demand reduction technologies which to allow the supply/demand balance to be achieved in a new way. The EU's "clean energy packages" are designed to fulfil this function.[11] The UK is pursuing a similar plan.[12]

To facilitate flexibility markets, it may be necessary to create a platform, as a venue on which providers can make their offers available and buyers can signal their needs. Two types can be distinguished: peer-to-peer platforms - which facilitate energy trading between individual businesses or "prosumers," operating at local levels. And grid services platforms - those which provide a wide range of grid services, often involving greater network coordination and bringing together either large assets, or smaller assets that have been aggregated together to meet grid requirements. Regulators in many jurisdictions are encouraging the development of such platforms.[13]

9 See for example the results of an early trial by Vector in New Zealand, at https://www.ena.org.nz/resources/publications/document/826.

10 For an analysis of how softwarization might affect regulation in this area, see Chris Decker, *Protecting consumers in digitized and multi-source energy systems,* available at https://www.tandfonline.com/doi/full/10.1080/15567249.2021.2012541.

11 See for example Energy Systems Catapult, *Towards a smarter and more flexible European energy system,* 2021, available at https://esc-production-2021.s3.eu-west-2.amazonaws.com/2021/10/Catapult-EU-FLEX-Report.pdf.

12 *Transitioning to a net zero energy system: smart system and flexibility plan 2021*, BEIS available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1003778/smart-systems-and-flexibility-plan-2021.pdf.

13 See Ofgem*, Flexibility Platforms in Electricity Markets*, available at https://www.ofgem.gov.uk/sites/default/files/docs/2019/09/ofgem_fi_flexibility_platforms_in_electricity_markets.pdf.

C. Regulating Hardware/Software Competition in Electricity

The depth and coverage of electricity regulation exceed that of mobile regulation by many times. Transmission and distribution networks in private ownership, currently subject to very little competition, are almost invariably price-regulated, and usually very profitable. This may give them an incentive to expand their networks.

At present, in many European jurisdictions in particular, the so-called task of "systems operation" (coordinating the planning, management and real time operation of the electricity networks with the activities of generators and retailers) is allocated to the country's transmission and distribution operators.

As the competitive options described above grow, they may fall victim to self-preference on the part of the network owner charged with systems operation. It may prefer to earn the return allowed by the regulator on additional network assets than to procure competing alternatives. This concern has led to plans or proposals in Great Britain and elsewhere to structurally separate the two tasks at transmission level, following the example of independent systems operators in north America in particular.[14] As local flexibility markets multiply, the same may occur at distribution company level.

Whoever makes the above hardware/software choices over how to meet at lowest cost the changing demand for the product must, however, find a rationale for doing so. Pressure to achieve net zero will almost certainly increase demand for electricity in coming decades, as will the need to accommodate more renewable generation.

This is not an unprecedented investment choice problem. Consider the owners of a factory making mousetraps. When the number of mice is forecast to grow, they face a choice between a hardware solution (expand the factory, but by how much?) and a software solution (add a night shift to the existing production roster, which can be done quickly and is reversible). With some approximations to knowledge of the probability distribution of demand growth, the slope of the supply curve of software solutions, and the lead times for and degree of economies of scale associated with different hardware expansion options, there is probably a determinate solution to this problem. It might be the case that some of the software solutions are substantially cheaper than some equivalent hardware solution but are indefinitely replicable. It would be surprising if either of the two corner solutions ("hold the software solutions in reserve solely to deal with forecasting under-estimates" and "first use up all available software solutions") would be optimal.

04
EXTENSIONS AND CONCLUSIONS

This account has just scratched the surface of the possibilities created in network sectors by data and digitalization. As noted, these depend upon the combination of digital and physical activities. In the nature of things, the nature of this combination is likely to determine the degree to which the growth of softwarization makes a difference both to costs and to competition.

In mobile communications, each new network generation has a major effect on costs and quality of service. These benefits are closely associated with softwarization in the case of 5G, which will be followed by 6G with its much greater degree on sustainability. In the electricity sector, by contrast, the impact will be more limited. I am not aware of firm estimates of how far flexibility markets and other software tools will go to reduce costs. It is likely to be small fraction of total sector costs, but so large is the likely expansion in demand in a country like Great Britain, this might plausibly amount to annual savings of many billions by 2050.

The two sectors considered here stand at opposite ends of the spectrum in relation to the degree of head-to-head competition they can embody. We have noted above in mobile communications the scope for a proliferation of digital networks, whereas in energy competing software remedies sit within a framework which revolves around price-controlled hardware monopolies whom regulators may suspect to have an incentive to stifle software, if they control the single buyer of software services.

What are the general lessons here for network regulators?

- Softwarization is a set of innovations which can confer substantial benefits on the customers (businesses and households), whose interests regulators are usually duty-bound to protect.
- Within that customer group, there may however be some, especially those who are less digitally qualified and affluent, whose position may be worsened by the process.
- Regulators must be aware of the possibility that hardware networks whose market power is diminished by such developments may seek to impede entry by software competitors across the whole value chain.

14 BEIS and Ofgem, *Joint Statement on the Future Systems Operator*, 2022, available at https://www.gov.uk/government/consultations/proposals-for-a-future-system-operator-role/outcome/joint-statement-on-the-future-system-operator.

"A ROSE BY ANY OTHER UNIQUE IDENTIFIER": REGULATING CONSUMER DATA TRACKING AND ANONYMISATION CLAIMS

BY
KATHARINE KEMP

Senior Lecturer, UNSW Faculty of Law & Justice. I am grateful to Nicholas Felstead for Research Assistance.

01 INTRODUCTION

Representations in online privacy policies that certain data is anonymous or "not information that personally identifies you" can have significant consequences. They may indicate that the firm considers the data to be outside the scope of data protection regulation, and/or give consumers the impression that this is data which cannot have an impact on the individual; for example, that it will not add to the individual consumer's profile.

However, there are a growing range of data practices and services offered by adtech and data analytics providers that do affect individuals' privacy while claiming not to use personal information. These include the development of persistent unique identifiers, data matching using hashed emails and other "identity resolution" services – practices which are not within most consumers' knowledge or understanding.

Applying another identifier to individual consumers ("O, be some other name!") does not overcome the reality that these practices are designed to track and influence the behavior of an individual person, no matter the label ("Thou art thyself").

Obfuscation about such activities may not only mislead consumers, but hinder competition on privacy quality by firms that seek to compete on the basis of genuinely privacy-enhancing features. This article argues that claims of anonymization and pseudonymization require tighter regulation under data protection law and should also be rigorously scrutinized under consumer protection law for potential misleading conduct.

02
"BLANK CHEQUE" PRIVACY POLICIES

It is often said that consumers pay for most digital services with their personal data and attention to advertisements. The personal-data price is essentially set by the supplier in its privacy policy. This may be the main price in the case of some "free" apps and online services, or an additional price where consumers pay a monetary amount for a product or subscription but are also required to accept extra collection and uses of their personal data.

The problems with this method of payment run deep. If privacy policies set the personal-data price, many suppliers are in fact requiring consumers to sign a blank cheque. Privacy terms tend not to set any clear limits on the types of extra and unnecessary personal data that may be collected from or shared with third parties, or the extent of monitoring of the consumer's activities on other apps or websites or offline, or extra commercial and even political purposes for which the consumer's data may be used.

If privacy terms set the price, they also allow the supplier to unilaterally increase that price long after the actual transaction with the consumer, as suppliers reserve the right to sell the dataset as part of an asset or business sale and amend the privacy terms without limitation.

There are currently a number of high-profile cases and campaigns which challenge the legality of the personal-data price charged by digital platforms. Johnny Ryan has long advocated against the lack of purpose limitation in Google's data terms. Liza Lovdahl Gormsen and the Bundeskartellamt have framed Facebook's data practices as abuses of dominance.

There is another common theme in suppliers' representations about consumer data practices that deserves our attention. Privacy terms often state that certain data is "anonymous" or does not include the consumer's name or contact details, and may even specify that the supplier can use this data in any manner "as it sees fit."

The implication is that these data practices cannot affect the individual's privacy. At the same time, many publishers, data brokers and adtech providers tell a very different story to advertising customers, emphasizing their ability to track and influence the activities of millions of individual consumers without reference to their name or email, in some cases even where the consumer has expressly opted out of tracking or identification.[2]

03
PRIVACY POLICY REPRESENTATIONS: "NOT YOUR NAME OR EMAIL"

Firms commonly make representations in online privacy policies that certain data the firm uses is "anonymous" or "pseudonymous" or does not "personally identify" the individual (for present purposes, collectively, "anonymous data" claims). The reason for including such claims appears to be two-fold. First, most data protection regulations only

2 As explained in Katharine Kemp, 'How to track consumers who don't want to be tracked: Examples from Australia's largest media companies and their suppliers' (Presentation to ACCC National Consumer Congress, June 16, 2022) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4141609.

apply to "personal information" of some description:[3] firms may argue that the information in question is not "personal" and therefore not subject to the obligations imposed by the regulation. Second, such representations may suggest to consumers that the relevant data practice does not have any impact on their privacy.

For example, Amazon Australia promises consumers that:

> [W]e do not associate your interactions on unaffiliated sites with information which on its own identifies you, such as name or email address, and we do not provide any such information to advertisers or to third-party sites that display our interest-based ads.[4]

Google emphasizes to consumers that, in its exchanges of data with advertising customers:

> We don't share information that personally identifies you with advertisers, such as your name or email, unless you ask us to.[5]

Similarly, Yahoo tells users it only discloses limited data to advertising customers and data analytics companies:

> We do not share personally identifiable information (like phone number or email address) with these partners, such as publishers, advertisers, ad agencies, or analytics partners.[6]

News Corp Australia informs online readers of *The Australian* newspaper that:

> We may also supplement this collected information with information collected from other trusted businesses with whom you also have a relationship or from public sources. All of this is anonymous information (unless we collect it when you are logged in as a recognisable registered user) …[7]

While these representations are expressed in various ways, the common theme is that they emphasize the data practice does not involve the consumer's name, email, or other contact details. The implication appears to be that it is only data associated with these contact details that could concern the consumer. In turn, the firm's reassurance that these details are not included implies there is little or no impact on the consumer's privacy and makes it less likely that consumers will object to the practice.

04

UNIQUE IDENTIFIERS, HASHED EMAILS, AND IDENTITY RESOLUTION

Such privacy policies tend not to describe for consumers how the firm exchanges information relating to the consumer with advertisers, data analysts and other firms where that information is not labelled with the consumer's name or email address. Yet there are a growing number of such data practices discussed and advertised in the marketing press, which most consumers will never see.

For instance, various firms have developed **unique identifiers** to track consumers' activities across different websites and apps, even where the consumer does not disclose their email address or login as a user for a particular visit. For example, while News Corp Australia tells consumers that various types of data are "anonymous" if the consumer is not logged in, it tells advertisers that it identifies 16 million consumers using unique identifiers (apparently, a string of numbers) which attaches to the individual consumer's activity even when they are not logged in.[8]

3 In Australia, e.g. the *Privacy Act 1988* (Cth) ("*Privacy Act*") only applies to "personal information" as defined in section 6 of the Act.

4 Amazon Australia, "Interest-Based Ads" (Web Page) https://www.amazon.com.au/gp/help/customer/display.html?nodeId=202075050&ref_=footer_iba.

5 Google, "Privacy Policy" (Web Page) https://policies.google.com/privacy?hl=en-US.

6 Yahoo!, "Welcome to the Yahoo Privacy Policy" (Web Page, April 2022) https://legal.yahoo.com/us/en/yahoo/privacy/index.html. See also BuzzFeed, "BuzzFeed's Privacy Policy and Cookie Policy" (Web Page, June 22, 2022) https://www.buzzfeed.com/about/privacy, referring to "[d]ata that indirectly identifies you such as your IP address, mobile device ID and location data. This data does not include anything that allows us to identify you by name or contact details."

7 News Corp Australia, "Data Usage Policy," *Privacy Centre* (Web Page, August 25, 2020) https://preferences.news.com.au/data.

8 As per News Connect "Customer Match" promotional video narration, available at https://www.newscorpaustralia.com/growth-stories/discover-new-digital-solutions-to-get-customers-to-notice-want-and-buy-your-brand/.

The impetus to develop unique identifiers has increased following changes – and announcements of impending changes – to browsers which no longer support tracking of consumers via third-party cookies. There is a particular drive for a unique identifier to become the common standard so that consumers' online and offline activities can be tracked and combined as pervasively as possible.[9]

Firms also commonly engage in **data matching using hashed email addresses**. For instance, firm A and firm B may each have databases of information concerning their own individual customers and wish to obtain further information about their customers' attributes and activities, without asking the individual customer for that information. One way firm A and firm B can achieve this is by each applying the same hashing algorithm to all email addresses in their respective customer databases, and exchanging data on relevant individual customers when the resulting hashed versions of the email addresses match.[10]

> *Firms also commonly engage in data matching using hashed email addresses*

By using hashed email addresses, firms avoid broadcasting their entire customer database, including names and contact details, to other firms. Nonetheless, following a successful match of the hashed versions of the email addresses, firm A and firm B each collect further information about the individual consumer from the other firm to add to their profile on that consumer, even though the consumer did not disclose that information themselves and has not received notice of the actual exchange.

These processes of hashing email addresses or applying unique identifiers might explain some firms' representations that certain information is "pseudonymous." For example, Amazon Australia states in the later passages of its Interest-Based Ads Notice that:

Some third parties may provide us pseudonymized information about you (such as demographic information or sites where you have been shown ads) from offline and online sources …[11]

No further information is offered as to how this is achieved.

Some firms also offer other **"identity resolution"** services which seek to connect various identifiers that relate to an individual consumer across different transactions, devices, and websites (which is sometimes then tied to a new unique identifier). Identity resolution might be used across different departments dealing with the same customer within the one firm. But it has also been used to connect information about a consumer's activities across different websites, apps, devices, and email addresses, even where the consumer has actively opted out of identifying themselves with a consistent identifier.

The location data company, Near, for example, outlines the following unusual logic:

- Consumers' activities have generally been identified and tracked through an advertising identifier on their mobile phone;
- Changes to Apple's operating system mean that Apple iPhone users can now opt out of this tracking by refusing access to their advertising identifier;
- Many Apple iPhone users have in fact opted out of this tracking and made their advertising identifier unavailable;
- There is therefore a "need" for an alternative means of identifying and tracking these consumers.[12]

Accordingly, Near developed a method of identifying the individual behind a device using over 27 signals from their various digital devices which can still be collected, even after the individual has refused access to their identifier.

These practices demonstrate that there are various methods of tracking the activities of an individual consumer

9 See 'Mi3 Special Report: Australia post-cookies, post-privacy: Implications for brands, publishers and media supply chain' (Mi3, November 2021) https://www.mi-3.com.au/23-11-2021/australia-post-privacy-post-cookies-how-marketers-major-publishes-and-media-supply-0.

10 If the same hashing function is applied to the same email address, it always results in an identical string of numbers and letters unrecognisable to humans, making for highly accurate matching across databases.

11 Amazon Australia, "Interest-Based Ads" (Web Page) https://www.amazon.com.au/gp/help/customer/display.html?nodeId=202075050&ref_=footer_iba.

12 Near, "Understanding Apple's App Tracking Transparency Framework and Its Impact on the Ad Ecosystem" (Blog Post, July 12, 2021) https://blog.near.com/marketing-advertising/apples-app-tracking-impact-on-the-ad-ecosystem/; *US Patent No 10979848*, filed on January 5, 2021 (Issued on 13 April 2021) https://patents.google.com/patent/US10979848B1/.

– and combining data about an individual consumer's attributes and activities across organizations – without any reference to the consumer's legal name or contact details.

Further, these tracking and identification methods are generally hidden from consumers who do not actively opt into the unique identifier (and may even believe that they have successfully opted out of identification) and have no information about the complex processes by which firms disclose and collect data about the consumer "behind the scenes."

05
MEANING OF "ANONYMOUS," "PSEUDONYMOUS," AND "DE-IDENTIFIED"

Given that individual tracking, data combination and influence are possible in these ways, one might ask whether the data in question is in fact properly classified as "personal information" and therefore subject to existing data protection legislation. The answer to this question will vary across jurisdictions.

A. United Kingdom

Like most data protection regulations, the law in the United Kingdom does not refer to "anonymous information" in its operative provisions. However, recital 26 of the UK General Data Protection Regulation does explain that the GDPR does not apply to "anonymous information" which is "information which does not relate to any identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable."

The UK Information Commissioner's Office has also explained in its guidance the high standard of irreversible de-identification necessary to render information anonymous:

> Anonymisation means that individuals are not identifiable and cannot be reidentified by any means reasonably likely to be used (i.e. the risk of reidentification is sufficiently remote). Anonymous information is not personal data and data protection law does not apply. Pseudonymization means that individuals are not identifiable from the dataset itself, but can be identified by referring to other information held separately. Pseudonymous data is therefore still personal data and data protection law applies.[13]

This provides some clarity on standards for the anonymization and pseudonymization of information: the latter is classified as personal information while the former is not.

B. California

The *California Consumer Privacy Act of 2018* provides definitions of some relevant terms. For example, the extensive definition of "personal information" – information that identifies, relates to, or could reasonably be linked with a consumer or household – specifically includes IP addresses, unique personal identifiers and inferences drawn from information to create a consumer preference profile.[14] This is supported by definitions of "deidentified" and "pseudonymized" information.

Information is "deidentified" where it:

> cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer

with added requirements that a business using that information has implemented safeguards that prohibit reidentification; has implemented business processes that specifically prohibit reidentification and prevent inadvertent release of deidentified information; and makes no attempt to reidentify the information.[15]

The Californian definition of "pseudonymization" is similar to that put forward in the UK, emphasizing the need to separate additional information which would make the consumer identifiable:

13 Information Commissioner's Office (UK), *Introduction to Anonymisation: Anonymisation, Pseudonymisation, and Privacy Enhancing Technologies* (Draft Guidance, May 2021) https://ico.org.uk/media/about-the-ico/consultations/2619862/anonymisation-intro-and-first-chapter.pdf.

14 Cal Civil Code § 1798.140(o)(1) (West 2020). https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

15 *Ibid* § 1798.140(h) (West 2020).

> the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.[16]

Pseudonymous information generally remains subject to the same obligations as other personal information, as opposed to deidentified information which is exempt. However, the Californian legislation does not make any separate reference to "anonymous" information.

> ***Firms also commonly engage in data matching using hashed email addresses***

C. Australia

In other jurisdictions, there is less clarity. In Australia, for example, "personal information" is defined with reference to whether information is "*about* an identified individual, or an individual who is reasonably identifiable."[17] Personal information is deemed to be "de-identified" if "the information is no longer about an identifiable individual or an individual who is reasonably identifiable."[18]

However, based on the Australian case law to date, it is unclear to what extent a court will consider that technical information such as IP addresses, browser information and device identifiers is "about" an individual and therefore "personal information."[19] Further, there is no definition of "anonymous" or "pseudonymous" information under the Australian statute, and no clear and binding rules concerning how such information should be treated.

In response to the Australian Competition and Consumer Commission's *Digital Platforms Inquiry* recommendations for privacy reform,[20] the Australian Government has undertaken a major review of the *Privacy Act*,[21] leading so far to recommendations by the Attorney-General's Department in its 2021 Discussion Paper.[22]

The Discussion Paper recognizes that the current definition of "personal information" is "somewhat unclear" in its application to technical information.[23] It proposes broadening the definition to refer to information that "relates to" an individual rather than being "about" an individual,[24] more closely aligning the Australian definition with the GDPR definition of "personal data" and likely clarifying that the concept includes technical information used to track the individual's activities.

The Discussion Paper also includes a proposal for requiring that the collection, use or disclosure (collectively, processing) of personal information is "fair and reasonable."[25] This represents a welcome move away from overreliance on a "notice and consent" model that depends on consumers impaired understanding of firms' actual data practices, and

16 *Ibid* § 1798.140(r) (West 2020).

17 *Privacy Act 1988* (Cth) s 6 (definition of "personal information") (emphasis added).

18 *Ibid* (definition of "de-identified"); OAIC, *Australian Privacy Principles Guidelines*, [B.59]-[B.62]; OAIC, 'Deidentification and the Privacy Act' (Web Page, March 21, 2018) https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-and-the-privacy-act.

19 *Privacy Commissioner v. Telstra Corporation Ltd* (2017) 249 FCR 24, 35–7 [59]– [65] (Dowsett, Kenny & Edelman JJ).

20 Australian Competition and Consumer Commission, *Digital Platforms Inquiry: Final Report* (Report, June 2019) Recommendations 16, 17 https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf.

21 See generally Attorney-General's Department (Cth), "Review of the Privacy Act 1988" (Web Page) https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988; Australian Government, *Regulating in the Digital Age: Government Response and Implementation Roadmap for the Digital Platforms Inquiry* (Report, 12 December 2019) 6 https://treasury.gov.au/sites/default/files/2019-12/Government-Response-p2019-41708.pdf.

22 Attorney-General's Department (Cth), *Privacy Act Review* (Discussion Paper, October 2021) https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/user_uploads/privacy-act-review-discussion-paper.pdf.

23 Attorney-General's Department (Cth), *Privacy Act Review* (Discussion Paper, October 2021) 21 https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/user_uploads/privacy-act-review-discussion-paper.pdf.

24 *Ibid* 26 (Proposal 2).

25 Attorney-General's Department (Cth), *Privacy Act Review* (Discussion Paper, October 2021) 85 (Proposal 10.1).

would be supported by several legislated factors relevant to determining whether processing is fair and reasonable in the circumstances.[26]

06

BEYOND DEFINITIONS: TRANSPARENCY AND ACCURACY

However, even clearer definitions of terms such as "anonymous," "pseudonymous," and "de-identified" will not be a complete solution to the kinds of representations raised in this article. As evident in the examples listed above, firms already choose to use other, vaguer terminology to describe the relevant data, such as "not information which on its own identifies you."

With this nebulous wording, consumers are not only left in the dark about the extent to which the data practice will affect their individual privacy, but often cannot tell whether the firm is claiming that such information is outside the scope of the data protection regulation, or that it is within the scope of the data protection regulation and, if so, for what specific purposes the firm proposes to use it.

Such uncertainty is unacceptable when firms are obliged to provide individuals with transparent and accurate information about their data practices. If the firm accepts that the information is personal information, there is a strong argument that qualifications about the absence of names and contact details should not be permitted to muddy the waters and obscure the substance of the data practice. If the firm claims the information is not personal information, it should make clear the basis for this claim: the absence of a name or contact details will not be sufficient.

07

SCRUTINY UNDER CONSUMER PROTECTION REGULATION

Consumer protection law also has a vital role to play in regulating representations about anonymization and methods of tracking in the meantime. Importantly, under consumer protection laws, a court is not constrained to consider whether certain mandated disclosures have been made in the fine print of a privacy policy, but must consider whether the firm's conduct as a whole creates an impression that misleads, or is likely to mislead, consumers about the nature of their data practices, having regard to consumers' likely level of information and comprehension.

We should not proceed on the unrealistic assumption that a consumer will be capable of unravelling the semantic intricacies of the fine print on the fifth page of a privacy policy. The realistic capacity of the reasonable consumer must be taken into account. This is reflected in the reasoning of the Federal Court of Australia in the *Google Location Data case*,[27] where Thawley J acknowledged that there are limits to the trouble that reasonable users would take to arrive at an accurate understanding of a firm's data practices, even for consumers who are concerned about their privacy.[28] Thus his Honor noted that "[t]here is a point where reasonable people give up drilling down to plumb the depths of further information."[29]

Similarly, in proceedings arising out of Facebook's data policies and the Cambridge Analytica scandal, a court in the United States noted the obstacles to comprehension for those reading Facebook's contractual language: "it would have been difficult to isolate and understand the pertinent language among all of Facebook's complicated disclosures."[30]

In the present context, consumer protection regulators should consider whether a given "anonymous data" representation is likely to create the false impression that:

- the relevant data exchange can add no further infor-

26 Attorney-General's Department (Cth), *Privacy Act Review* (Discussion Paper, October 2021) 89 (Proposal 10.2).

27 *Australian Competition and Consumer Commission v Google LLC [No 2]* (2021) 391 ALR 346.

28 *ACCC v Google LLC (No 2)* [2021] FCA 367, para 210.

29 Ibid 389 [210].

30 *Re Facebook Inc*, 402 F Supp 3d 767, 792 [17] (Chhabria J) (ND Cal, 2019).

mation to the firm's collection of data about the consumer as an individual,
- the consumer's relevant activities will not later be associated with any profile that identifies the consumer or the consumer's device, or
- the information in question cannot be used to determine what communications and offers will be displayed on the individual consumer's device based on their specific attributes and activities.

We should also question whether it is appropriate to use terms such as "pseudonymous" which may have absolutely no meaning for the average consumer and serve only to confuse. There is a need for research to determine consumers' understanding of these terms and representations, and therefore the risks created by their use.

08
HINDERING COMPETITION ON PRIVACY QUALITY

The lack of transparency and choice regarding these practices has significance beyond the question of compliance with data protection and consumer protection regulation. Obfuscation about the nature of these practices is also likely to hinder firms who seek to compete on the basis of superior privacy quality.

Consider a search engine that competes on the basis of privacy-enhancing features, abstaining from collecting any personal information. Such a supplier will not be able to make these advantages as salient to consumers seeking improved privacy if the privacy-degrading features of its rivals' services can be concealed in vague representations that certain data does not personally identify users.

> *Firms also commonly engage in data matching using hashed email addresses*

Adtech providers who innovate with business models – including innovative contextual advertising models[31] – that do not depend on tracking consumer behavior, will also be disadvantaged. These representations prevent consumers from making a comparison between the privacy-enhancing approach to advertising of these providers and the privacy-degrading approach to advertising of those who pervasively monitor consumer behavior and combine personal data across multitudes of businesses to create a "360-degree view" of consumer that allows their behavior to be predicted and manipulated.

In most cases, this hindrance of competition due to the conduct of any given firm is unlikely to amount to an antitrust contravention. Practices would be more likely to fall foul of competition laws where rivals coordinate their activities: for example, if rival firms adopt a common identifier to track individual consumers across their respective sites, apps, and services subject to the same terms and representations. More generally, competition policy depends on adequate consumer protection regulation and enforcement to ensure that consumers have the information necessary to select products according to their true preferences.

09
CONCLUSION

Firms should not be permitted to make confusing and potentially misleading representations about data practices that do not include consumers' names and contact details. Many firms are aware that the absence of such details does not prevent their data practices – such as data matching, unique identifiers, and identity resolution – from intruding upon the individual consumer's privacy. In the circumstances, these "anonymous data" representations prevent consumers from making accurate comparisons of data terms and impair effective competition on privacy quality by firms who innovate to enhance privacy.

31 See e.g. Greens EFA, "The future of advertising: Innovative practices on the rise" (April 19, 2022) https://www.youtube.com/watch?v=17aZdbFLGIA.

To comply with their data protection obligations to provide transparent and accurate information on their data handling, firms should only make "anonymous data" representations if they clearly articulate their claim that the data is not personal data under the relevant regulation and the basis for this claim. Consumer protection regulators should also scrutinize such representations to determine whether the firm's conduct is likely to mislead consumers about the true nature of the firm's data practices.

> ***In most cases, this hindrance of competition due to the conduct of any given firm is unlikely to amount to an antitrust contravention***

THE CASE FOR STRINGENT REGULATIONS OF STABLECOINS

BY

DAVID S. EVANS

Chairman, Global Economics Group and Founder, Market Platform Dynamics. For more details visit https://davidsevans.org.

01 INTRODUCTION

Fortunately, despite all the hype, cryptocurrencies are a small part of the financial system.[2] At the peak value in October 2021 the market cap of crypto was about $2.7 trillion.[3] The total value of physical money ("M0") was about $40 trillion that year and the broader money supply ("M3") was about $90 trillion.[4] And crypto is largely confined to its own ecosystem.

Thus, when the prices of cryptocurrencies plunged, a large stablecoin issuer collapsed in early May 2022, and crypto investors started

2 For the purposes of this paper, I use the term "cryptocurrencies" to refer to the crypto currency native to public blockchains (such as ether for Ethereum) and not to stablecoins. I use the shorthand "crypto" to refer to the public blockchains and related entities.

3 ConDesk, "Crypto Market Cap Surges to Record $2.7T," October 21, 2021. https://www.coindesk.com/markets/2021/10/21/crypto-market-cap-surges-to-new-record-27-trillion/.

4 Go BankingRates, "How Much Money Is In the World Right Now," June 8, 2022. https://www.gobankingrates.com/money/economy/how-much-money-is-in-the-world/.

pulling funds in classic runs, nothing happened to the traditional financial system. There was no material contagion. The crypto world became a case study, however, of what can go wrong in the absence of the banking-type supervision. The answer, which we've known for better than a century, is just about everything.

There is now increased interest in regulating crypto in case it gets so big and intertwined with our financial system that it does pose systemic risk to the economy.[5] This article explores striking the balance between regulation and innovation by focusing on a key part of the crypto business — stablecoins — and drawing some comparisons with an almost contemporaneous money innovation, mobile money. It concludes there should be stringent regulation of stablecoins but not an outright ban at this point in time.

02
STABLECOINS AND THE HOT POTATO PROBLEM

Stablecoins show how far crypto has come from its early promises. Cryptocurrencies were supposed to replace fiat currencies. This was just not possible because bitcoin and the other currencies are inherently unstable and cannot function as money. There is no mechanism — human or algorithmic — for ensuring that the major cryptocurrencies have stable value, and they don't. Between 2012 and 2021, for example, the average annual volatility of bitcoin was 16 times higher than the dollar.[6] Crypto prices tend to move in tandem and high volatility is endemic.

As a payment method, crypto is a hot potato. Gambling aside, businesses don't want to be paid with currency that could plummet in value. An early example of this involved Ross Ulbricht, the founder of Silk Road, who negotiated a contract for a hitman on the dark web. He paid the hitman, who was an undercover agent, $90,000 in bitcoin but pledged to send more if the bitcoin price tanked.[7] Today, wallet providers that enable consumers to pay merchants with crypto solve the hot potato problem by almost immediately converting the crypto that the consumer has paid to fiat currency. El Salvador's experiment in making bitcoin a national currency has failed largely because of the hot potato problem. Businesses and people avoid it since they cannot manage their budgets with it.

Crypto volatility even made it risky to trade cryptos for other cryptos or with fiat. The prices were volatile even in short windows. The volatility also made it problematic to develop financial services applications on the public blockchain. Ethereum was supposed to be a platform for smart contracts with decentralized finance the main use case. There is little appetite for contracts, particularly long-term ones, when the money involved has highly uncertain value.

Stablecoins were the solution to these problems. They are tokens typically relying on Ethereum's ERC-20 protocol but usable across other public blockchains. As of July 16, 2022 Tether's USDT, Circle's USDC, and Binance's BUSD accounted for 90.6 percent of the market cap of stablecoins. As the initials suggest they are all pegged to US$1.00. Each of the sponsors claims to keep full liquid dollar-denominated collateral (such as cash and short-term treasuries) for their stablecoins. Terra's Luna stablecoin, which collapsed following a classic run, was pegged to the U.S. dollar but relied on algorithmic trading to maintain the peg.

Stablecoins do not replace the native cryptocurrencies for the public blockchains. Those public ledgers are recording transactions in their native currencies. Transaction processing is based on incentive schemes — whether proof of work or proof of stake — tied to those native currencies. In fact, Terra's collapse was precipitated by massive rapid decline in the value of cryptocurrencies — by about half in the roughly six months from their November 2021 peak to the when Luna started deviating from the peg in early May 2022. Then the well-known knock-on effects of the resulting runs led to crypto currencies plummeting further. Stablecoins can alleviate the hot potato problem in exchange but not the fundamental crypto volatility problem.

Regulators are looking at how to balance systemic risk versus systemic innovation in considering regulations and have a heightened concern over stablecoins following what looks like classic bank runs and financial contagion. In considering that, a trip to Kenya is helpful.

5 Kim shows that cryptocurrencies and traditional financial markets are linked through stablecoins which lead to fluctuations in the demand for commercial paper and this could pose systemic risks absent regulation if stablecoins became a larger part of the financial system. Sang Rae Kim, "How the Cryptocurrency Market is Connected to the Financial Market," May 7, 2022. At https://ssrn.com/abstract=4106815.

6 David S. Evans, "Can Crypto Fix Itself in Time," *CPI TechREG Chronicle,* February 2022. At https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4031977.

7 PYMNTS, "The Alleged Bitcoin Silk Road Hitman Operation," February 6, 2015. At https://www.pymnts.com/in-depth/2015/the-alleged-bitcoin-silk-road-hitman-operation/.

03

M-PESA AND THE REGULATION OF MOBILE MONEY

In many lower and middle-income countries people can load money onto a mobile phone, often paying cash at agents (typically small shops), and send that money to other people, who take cash out at agents. Increasingly, mobile money stays in the system as it is used to pay for goods and services directly rather than being converted to cash. The mobile money platforms support other financial services such as saving and borrowing.

As of 2021, according to GMSA, 98 countries had live mobile money deployments, there were 1.35 billion accounts of which 518 million had been active in last 90 days, and around $1 trillion was processed that year by mobile money schemes. That's a lot of money since many of the people are dirt poor. About half of the users in are in Sub-Saharan Africa.[8] There, mobile money brought banking and other financial services to large portions of the population, particularly the poor, and those living outside urban centers.

Decisions on how to regulate mobile money have important effects on the success of mobile money schemes — whether they take hold at all and how rapidly they grow. Key considerations concern the role of banks in mobile money schemes and the extent to which traditional banking regulation should apply to the new schemes. Some countries decided to insist that banks take the lead role in operating new schemes or imposed burdensome KYC and agent regulations. Banks lobbied for policies since they viewed the new schemes as competitors. Other countries adopted light regulations and a wait-and-see approach as the schemes evolved.

My paper with Alexis Pirchio studied the first wave of mobile money schemes from the mid 2000s to 2014.[9] In practice, the choice was between lightly regulated schemes operated by mobile carriers, or heavily regulated schemes with significant bank involvement. We found that all the successful ones (there were eight) had light regulatory regimes — they didn't have to be run by banks and the other restrictions were not onerous. Almost all the ones that failed (seven of eight) had heavy regulatory regimes that required that banks take the lead role in the scheme or had heavy KYC and agent regulations.

The launch and regulation of M-PESA, which established the pioneering and most successful mobile money scheme illustrates the issues. In 2005, Safaricom, the dominant mobile carrier in Kenya, together with Vodafone Group and the Commercial Bank of Africa, asked the Central Bank of Kenya ("CBK") to authorize what became M-PESA. The CBK could have just denied the application. But, as a study sponsored by the Gates Foundation noted, the CBK chose to "navigate the necessary risks to find a regulatory solution that would foster greater financial inclusion."[10]

The CBK insisted that mobile money exchange at par with fiat and that the consumer retain ownership in that mobile money. When a consumer gave 100 Kenyan shillings ("KES") to an agent to put mobile money on their SIM card, the value of the mobile money on the SIM card was pegged at 100 KES. That money belonged to the consumer and not M-PESA or the agent. M-PESA and the agent could not, like a bank, lend or invest those deposits. The mobile money was extinguished when it was converted back into cash by an agent. The cash backing the mobile money went into a trust under the custody of a trustee and deposited into a bank. Safaricom and its partners had no access to these funds. In February 2007 the CBK authorized the launch of M-PESA, which happened in a few days, but put M-PESA into a sandbox where the CBK oversaw the mobile money scheme while considering a complete regulatory framework.[11]

M-PESA grew quickly in part because it met an enormous need in Kenya.[12] There were few banks. Family members often left villages for the cities to earn money which they wanted to get back to relatives back home. The countryside was dangerous, at the time torn by civil war. M-PESA was an alternative to giving cash to drivers and hoping it would make successful journey to its intended recipient. There were 5 million registered users by April 2009, among about 39.6 million adults, and 25 million registered users by February 2015. As a share of GDP, M-PESA transactions increased from 7 percent in 2008 to 45 percent in 2014. As

8 GMSA, *State of the Industry Report on Mobile Money*, 2022. At https://www.gsma.com/sotir/wp-content/uploads/2022/03/GSMA_State_of_the_Industry_2022_English.pdf.

9 David S. Evans & Alexis Pirchio, "An Empirical Examination of Why Mobile Schemes Ignite in Some Developing Countries but Flounder in Most," *Review of Network Economics,* 2014, vol. 13, issue 4, 397-451. At https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2578312.

10 Brian Muthiora, *Enabling Mobile Money Policies in Kenya: Fostering a Digital Financial Revolution*, GMSA, January 2015. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2015/02/2015_MMU_Enabling-Mobile-Money-Policies-in-Kenya.pdf p. 9.

11 *Id*.

12 David S. Evans & Richard Schmalensee, *Matchmakers: The New Economics of Multisided Platforms* (Cambridge, MA: Harvard Business Review Press, 2016).

of 2022 most adults in Kenya use M-PESA. It has expanded from money transmittal to bill payment, credit and savings, and paying at merchants.[13]

Not surprisingly, as M-PESA use exploded after 2007, Kenyan banks were unhappy. They lobbied the government to shut it down on the grounds that it would cause a financial crisis. A Kenyan newspaper reported that the banks approach the Minister of Finance and claimed that M-PESA was "similar to a 'pyramid scheme' and that 'people could lose their money if it collapsed.'"[14] The bank lobbying ultimately failed in Kenya. Other countries were not as lucky, as Pirchio and I showed.

04
REGULATION, INNOVATION, AND RISK

Without sound regulation, however, the bankers might have been proved right. M-PESA eventually became the main financial system for Kenya. People trusted it to put their money. And eventually to borrow and invest money. A large number of agents — small shop owners — in Kenya trusted it too. They had to keep funds on hand to redeem mobile money. Merchants also took mobile money payment. A lot could go wrong here in the usual ways for banking systems. There could be runs, contagion effects, waves of personal and business bankruptcies, dragging the economy down into recession or worse.

The CBK recognized all this. It had to make a tradeoff between heavier regulation that could reduce these risks but also dampen, if not kill, innovation and lighter regulation that could promote innovation but pose some risks. It could have put more trust in Safaricom and let it hold on to the funds and even invest them like a bank. After all, Safaricom was a large regulated mobile carrier, not a start-up. Alternatively, it could also have concluded that mobile money schemes should be reserved for banks. It had to strike the balance in the face of great uncertainty, with the risks and costs in both directions.[15]

M-PESA, and the experience of mobile money schemes, highlights three important points for regulators. First, it is better to nurture innovation even if it could be harmful. It is hard to know for sure just how important innovation could be to an economy. Second, it makes sense to retain flexibility in the fact of uncertainty. If regulation can kill an innovation it is better to take a lighter touch at first until the risks and rewards are better known. That is the premise behind the use of regulatory sandboxes. Third, it is important to guard against incumbents seeking to use regulation to preserve their own rents, and to be skeptical of claims that innovation will lead to the end of the world.

Regulators, however, also need to avoid reasoning by analogy. Striking that balance is a fact-dependent, context-specific, exercise. There may be cases where initiatives should be stopped dead cold or ruled with a heavy hand. That light regulation was the right solution for mobile money, particularly as done in Kenya, doesn't mean that it is for other different initiatives, in different situations, elsewhere.[16]

05
SELLING CRYPTO'S FUTURE

The current consideration of regulation for stablecoins and other aspects of crypto occurs in a vastly different environment than mobile money, FinTechs, or many other new financial services innovations. Bitcoin launched more than 13 years ago. We've had the chance to learn a lot about public blockchains and their cryptocurrencies

As the Silk Road example illustrates, in bitcoin's first few years, its main use case was for illegal trading activity that took place on the dark web. The convenience of using a difficult to trace digital currency — rather than say credit cards — was worth the price of bearing the volatility. It still is. Bitcoin is the currency of choice for the cybercriminals behind ransomware. When I first starting writing about

13 See https://www.safaricom.co.ke/personal/m-pesa/m-pesa-home.

14 Mwangi S. Kimenyi, "Mobile Wars and Political Barriers to Entry: Safaricom vs. Equity Bank," Brookings, October 29, 2014. At https://www.brookings.edu/blog/africa-in-focus/2014/10/29/mobile-wars-and-political-barriers-to-entry-safaricom-vs-equity-bank/.

15 Decision theory, which is the basis for error-cost analysis, provides the analytic framework for this sort of problem. For an introduction in the context of antitrust see David S. Evans, "Why Different Jurisdictions Do Not (and Should Not) Adopt the Same Antitrust Rules, *Chicago Journal of International Law*, Vol. 10, No. 1. At https://chicagounbound.uchicago.edu/cjil/vol10/iss1/9/.

16 *Id*.

crypto, in 2014, hardly any legitimate merchant accepted bitcoin.[17]

Crypto advocates and their backers, however, insisted that it was going to replace traditional payments. In May 2014, Brian Armstrong, the founder of a two-year old startup, Coinbase, claimed, according to Andy Kessler of the Wall Street Journal, that his company wanted "to be the Visa and Mastercard of Bitcoin payment processing, taking those behemoths out of the picture as merchants and customers move to virtual transactions" and as these giants had to drop their fees "to match cheaper technology."[18]

This was nonsense. Bitcoin couldn't be a currency that people used for payment because experience had shown that it was too volatile, and it was clearly incapable of solving this problem. It also turns out that Bitcoin couldn't be like Visa or Mastercard, because it wasn't capable handling anything remotely close to their transaction volumes.[19] Eight years later, in July 2022, the major public blockchain still are not scalable and rely on volatile cryptocurrencies.[20]

No killer app for public blockchains has emerged for which there has been widescale adoption. There are apps such as remittances and lending but there is no evidence than any of these are in widespread use. The major new competition to incumbent remittance and lending business have come from FinTechs and Neo-Banks who do not rely on public blockchains for the bulk of their services. There is no success story remotely close to M-PESA in its first few years much less its first thirteen, or to FinTech Wise for remittances.

For the last decade, cryptocurrencies have mainly been used for trading by people betting on the value of the coins. Crypto businesses have made money largely by supporting this trading activity directly (as is the case for exchanges) or indirectly through processing these trades (as is the case for miners). Coinbase, for example, never put a dent in the card networks. It makes its money mainly from trading which is stoked by greater volatility.[21]

In fact, speculation has become the main use case for crypto. The exchanges have gotten increasingly aggressive at persuading retail investors to buy crypto. The recent Superbowl in the U.S. had ads promoting crypto. FTX's ad had comedian Larry David telling Thomas Edison that the light bulb stinks, with the commercial closing with "Don't be like Larry. Don't miss out on the next big thing." Crypto.com, featuring Lebron James, said "Fortune favors the brave." Coinbase had a rotating QR code that took people to a page giving them $15 of free bitcoin to sign up for its wallet and entry into a $3 million lottery.

"Crypto advocates and their backers, however, insisted that it was going to replace traditional payments

The July 4 issue of the *New Yorker* features a two-page spread with Gisele Bündchen, the Brazilian supermodel, boosting FTX. She's "In" because she "share[s] a passion for creating positive change." That's followed by with a two-page spread with FTX bounder Sam Bankman-Fried who is "in on crypto because [he] want[s] to make the biggest global impact for good." The "You In" campaign has run in other magazines. Seven-time Superbowl winner Tom Brady, Ms. Bündchen's husband, is also promoting crypto for FTX,[22] and the couple reportedly have an equity stake in the exchange.[23]

The ads do not disclose the extraordinary historical volatility of cryptocurrencies. The celebrity promotions started occurring during 2021. Over the last 12 months bitcoin had a high of close to $68,991 in November 2021 and a low

17 David S. Evans, "Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms," Coase-Sandor Institute for Law and Economics, University of Chicago, May 2014. At https://chicagounbound.uchicago.edu/law_and_economics/680/.

18 Andy Kessler, "Angling to Be the MasterCard of Bitcoin," *Wall Street Journal*, May 16, 2014. At https://www.wsj.com/articles/SB10001424052702303908804579563951822782842.

19 David S Evans, "Can Crypto Fix Itself in Time," op. cit.

20 Ethereum promises to ameliorate the scalability problem by switching to from proof of work to proof of stake — possibly in the next few months.

21 Khristopher J. Brooks, "Coinbase to cut workforce by 18% amid wide crypto sell-off," CBS News, June 15, 2022. At https://www.cbsnews.com/news/coinbase-layoffs-cryptocurrency-sell-off-brian-armstrong/. Coinbase, *Annual Report 2021*. At https://d18rn0p25nwr6d.cloudfront.net/CIK-0001679788/8e5e0508-da75-434d-9505-cba99fa00147.pdf.

22 You should not watch this if you are a Tom Brady fan but here is one of his ads: https://www.instagram.com/reel/Cfl_fCEAmO9/?igshid=MDJmNzVkMjY%3D.

23 Vildana Hajric, "Tom Brady and Gisele Bündchen Take Equity Stake in Crypto Firm FTX," Bloomberg, June 29, 2021. At https://www.bloomberg.com/news/articles/2021-06-29/tom-brady-gisele-b-ndchen-take-equity-stake-in-crypto-firm-ftx.

of $17,602 in June 2022. Between Superbowl (February 13) and Independence Day (July 4) it fell from $42,068 to $20,260. The ads also do not disclose the fact that after 13 years, and many promises, cryptocurrencies are not in widespread use for any productive purpose, or the abject failure of El Salvador's decision to make crypto a national currency.

Crypto promotions are backed by claims that it is "the future". The blockchain will be the basis for web3 (often described as a decentralized internet based on blockchain) or financial nirvana (often described as lacking intermediaries and promoting financial equality). That future is distant, uncertain, and vague. The latest promises beg the question why the future, the next big thing, which crypto enthusiasts have promised for the last 13 years, isn't here already.

The actual present, with exchanges paying celebrities to encourage people to speculate on crypto, in the face huge historic volatility, and great uncertainty that latest visions will ever be realized, isn't very attractive.

06

STRIKING THE RIGHT BALANCE

Regulators considering where to strike the balance between innovation and regulation for crypto are working with a far different set of knowledge in which to form expectations of benefits, costs, and risks compared to what regulators had for mobile money or more recently for FinTechs. Mobile money schemes and FinTechs came to regulators with a clean slate. They could pose problems, but there wasn't any evidence that they had or would. They were also nascent, so it was possible to put guardrails in place to limit risk while regulators collected data from actual use.

There was no certainty at first that these were significant innovations that could help society. But they all had immediate constructive use cases. Also, within a couple of years from the start it was apparent that mobile money was a powerful force for economic progress by layering the country with an inexpensive banking and payments system that, in fact, helped large numbers of poor people.

By contrast, crypto comes to regulators today with a problematic past, a dubious present, and a concerning future. The past is filled with unlawful activity, volatility, and failed promises. The present is based on speculation and celebrity-fueled hype. Recent events demonstrate that crypto volatility combined with lax supervision can result in financial calamity and contagion. The future is one where there appears to be no solution for the underlying volatility of native cryptocurrencies which could be long-run source of systemic risk for the economy. And these are just the highlights.

Regulators should also have different priors on the likelihood that crypto will result in important innovations than a new FinTech business. Crypto has a credibility problem. For many years, crypto supporters claimed it was going displace fiat money and traditional payments rails. Many economists, including me, explained that was just not possible and years went by, predictably, with no mass adoption. Other promises, involving various applications, came and went. Important ones, such as smart contracts, went on hiatus when, in 2017, Ethereum recognized it had to go back to the drawing board to develop a scalable efficient platform. The credibility of crypto defenders is not helped by silly similes that crypto is just like the internet and some people said the internet wouldn't amount to anything.[24] Regulators should therefore view current claims about web3 with a healthy dose of skepticism.

Regulators cannot discount the possibility that overly onerous crypto regulations could prevent the realization of valuable innovations. Crypto is a vast, heavily-funded enterprise and it could lead to disruptive innovation that would be socially valuable. Ethereum is close to moving to proof of stake and taking other steps that could improve the scalability of this blockchain. It has invested in developing a platform for smart contracts which could lead to innovations. That wouldn't solve the inherent volatility of existing cryptocurrencies. It is possible, however, that new solutions — based on or inspired by the work that has gone on — could emerge that would not be based on volatile cryptocurrencies.[25]

Nevertheless, when it comes to stablecoins, it is time for regulators to err on the side of caution. The risks posed are too high and immediate while the likelihood of valuable innovation too uncertain and remote. To begin with, regulators should consider imposing the firmest guarantee possible that people will be able to redeem their stablecoins at par for fiat. In practice that means 100 percent reserves of fiat for stablecoins, in cash or very short-term instruments, held by an independent trustee, in a regulated bank.

24 Crypto is just like alchemy. People said you couldn't turn lead into gold. They were right. QED!

25 It is also possible that completely different technologies could emerge, without the problems of crypto, that could result in similar innovations.

Regulators should consider doing more. There is not simply a bank solvency issue for stablecoins. There are an increasing number of crypto apps that are unregulated, and pose substantial financial risks themselves, based on stablecoins.[26] When crypto prices collapsed, many investors lost the stablecoins they had deposited in return for high interest rates in entities such as Celsius. More of these dangerous crypto apps will arise.[27] Eventually, those entities should be subject to regulation too. That may be difficult given the ability of crypto apps to locate in places — or nowhere at all in theory — where there is little regulation or operate as decentralized autonomous organizations for which there is no one to regulate.

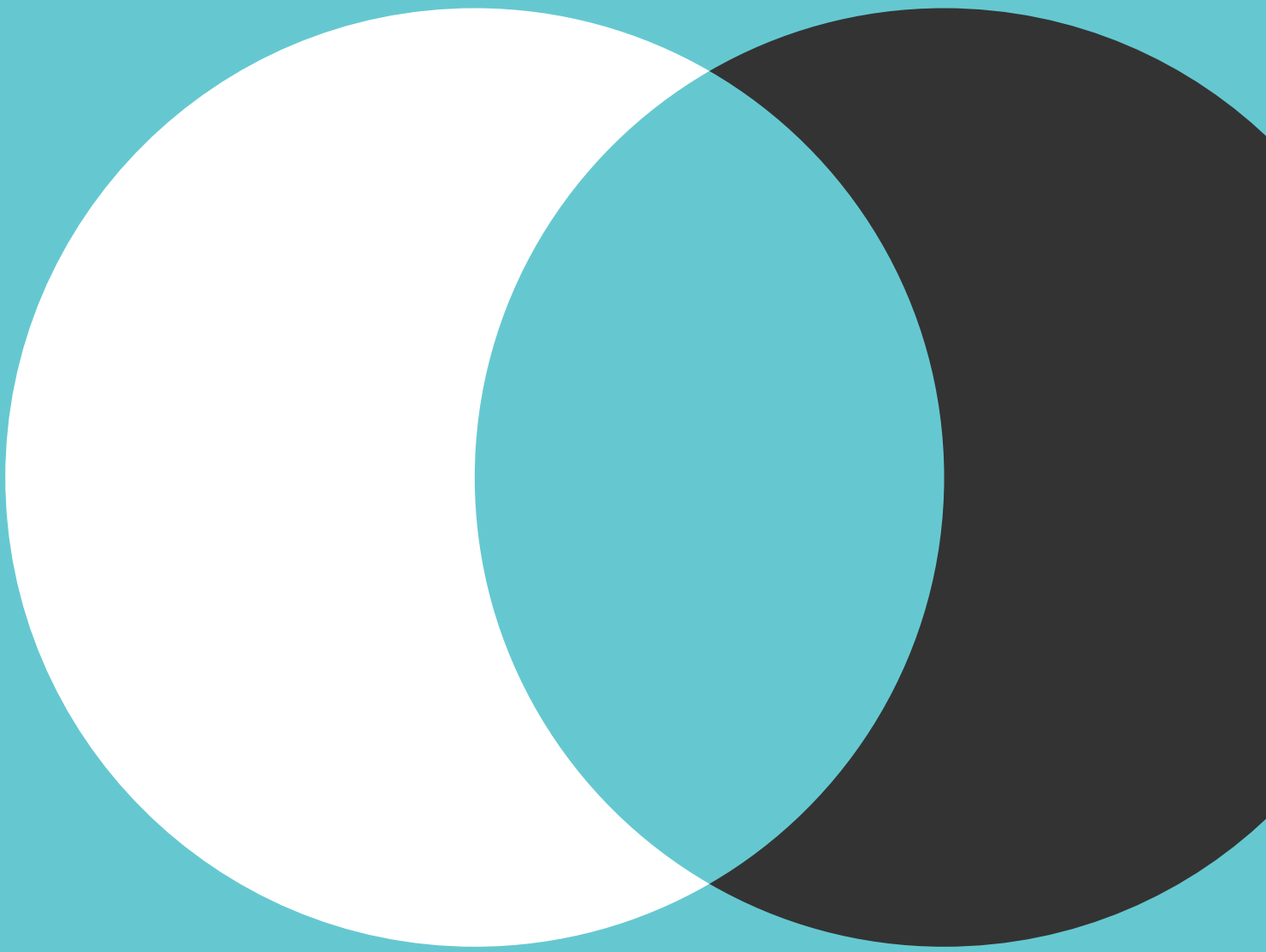
Regulators could deal with this problem by limiting the use of stablecoins in unsafe applications. There are two potential ways to do this, helped by the fact that stablecoins are programmable. First, the regulator could approve stablecoins only for use on approved applications. It could approve applications directly or ones that have been approved by another reputable regulator. Second, the regulator could require the stablecoin issuer to have an application review process and allow its stablecoins only to be used a approved application. In either case, the stablecoin issuer should be subject to penalties, including a possible halt in activities, if it failed to limit the use of its stablecoins with the designated safe applications.

These proposed regulations ignore the elephant in the crypto room: the use of stablecoins to facilitate speculative trading, which results in increased volatility and systemic risk as well as harm to hype-fed consumer investors. That is worth serious attention by banking, exchange, and consumer protection regulators.

> ***Regulators cannot discount the possibility that overly onerous crypto regulations could prevent the realization of valuable innovations***

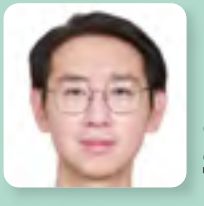
26 Rachel Louise Ensign, "They Thought 'Crypto Banks' Were Safe, and Then Came the Crash," *Wall Street Journal*, July 23, 2022. At https://www.wsj.com/articles/they-thought-crypto-banks-were-safe-and-then-came-the-crash-11658568780.

27 For a recent example see, Scott Chipolina and Stefania Palma, "SEC charges 11 in 'massive' crypto Ponzi scheme," *Financial Times*, August 1, 2022. At https://www.ft.com/content/c011817f-7f1f-4462-95b5-d4e0fecd9004.



CONVERGING PROPOSALS FOR PLATFORM REGULATION IN CHINA, THE EU, AND U.S.: COMPARISON AND COMMENTARY

BY LIYANG HOU



& SHUAI HAN

Professor, KoGuan School of Law, Shanghai Jiao Tong University.Doctoral Candidate, KoGuan School of Law, Shanghai Jiao Tong University.

01 INTRODUCTION

As the greatest engine for economic growth in the recent history, digital platforms have transformed people's ways of lives, and brought convenience as a standard. With innovated ways of doing businesses, platforms with the help of technology advances are now able to substantially bring down, if not to eliminate, transaction costs, by bypassing middleman and expanding business reach nation-wide or even world-wide. Consumers are now able to enjoy a wider range of products with reduced

prices. More jobs are created as platforms increase opportunities and ways of doing businesses. Competitors in the traditional non-digital world certainly have different thoughts, however, as innovations and the fast expansion of their digital counterparts are threatening the very existence of their livelihood. Users, in particular business ones, are highly dependent upon those platforms, and hence have concerns over the influence exerted by platforms on their businesses.

Governments as well have showed their worries about platforms' extensive influences and controls on users and the economy. Furthermore, with the digital economy being the trend come new types of anti-competitive practices that are complex in nature and are not easily judged or regulated. Should we encourage maximizing total welfare as Bork suggested and thus tolerate the existence of market power, or should we adopt some more strict ways of regulation as what the Neo-Brandeisians have suggested to protect small businesses and to reduce platforms' influences? It seems that digital way of life is a bittersweet experience, but one thing to be sure, digital platforms are now on the radar of major nations worldwide. China, the United States (hereinafter U.S.), and the European Union (hereinafter EU) all have drafted proposals with the intention of keeping platforms in check.

The State Administration for Market Regulation in China ("SAMR") announced two guidelines in October 2021. The drafted Guidelines for Classification and Grading of Internet Platforms (互联网平台分类分级指南) ("Classification Guidelines") categorize digital platforms into super, large and medium-to-small platforms by size, and the drafted Guidelines for Implementing Subject Responsibilities on Internet Platforms (互联网平台落实主体责任指南) ("Responsibilities Guidelines") impose extra responsibilities and obligations when a platform falls into the category of "super" or "large", with the purpose of securing fair competition, equal internal governance, and an open ecosystem.[2] China is certainly not alone in doing so. The EU adopted the Digital Markets Act ("DMA") on July 18 2022,.[3] At the other side of the Atlantic, the U.S. House of Representatives, based on a similar idea, formed a set of five bills, trying to implement regulations on Big Tech companies to hold them accountable for a number of anti-competitive conduct.[4] All these guidelines and proposed acts have one common goal that is to seek government regulation against big platform operators outside the box of competition law[5].

02
DRAFT REGULATIONS IN THE EU AND THE U.S.

With the competition law analysis into mind, the logic behind those proposals in both the U.S. and the EU can be easily observed to follow the same three-step analysis.

The first step is to define relevant markets. The EU confines platform services to be governed by the DMA to 11 types under the term of "Core Platform Services". These are comprised of online intermediation services, online search engines services, online social networking services, video-sharing platform services, number-independent interpersonal communications services, operating systems, web browsers, virtual assistants, cloud computing services, and online advertising services.[6] In comparison, the U.S. uses three kinds of business functions as a guide, and defines the relevant market as "Online Platforms" that can: (1) enable a user to generate content that can be viewed by other users on the platform or to interact with other content on the platform; (2) facilitate the offering, sale, purchase, payment, or shipping of goods or services, including software applications, between and among consumers or businesses not controlled by the platform; or (3) enable user searches or queries that access or display a large volume of information.[7]

Different as they may seem, the EU and the U.S. are similar in nature. In fact, all those "Core Platform Services" can

2 See the State Administration for Market Regulation, "The Announcement for Public Comments on the 'Guidelines for Classification and Grading of Internet Platforms (Draft for Comment)'and the 'Guidelines for Implementing Subject Responsibilities on Internet Platforms (Draft for Comment)' [关于对《互联网平台分类分级指南（征求意见稿）》《互联网平台落实主体责任指南（征求意见稿）》公开征求意见的公告]," October 29, 2021, available at https://www.samr.gov.cn/hd/zjdc/202110/t20211027_336137.html.

3 Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), adopted on July 18 2022.

4 U.S. House Lawmakers Release, "A Stronger Online Economy: Opportunity, Innovation, Choice" (2021), https://cicilline.house.gov/press-release/house-lawmakers-release-anti-monopoly-agenda-stronger-online-economy-opportunity, last visited on January 3, 2022.

5 Competition law is as a matter of fact an EU term, which is equivalent to anti-monopoly law in China and antitrust law in the U.S.

6 European Commission, "Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)," COM(2020) 842 final, December 15, 2020, Article 2.

7 See Ending Platform Monopolies Act, H. R. 3825, June 11, 2021, Section 5(10).

also be more or less covered by the "Online Platforms" of the U.S. Thus, it is clear that both jurisdictions, instead of establishing something new and deviating from the existing competition law completely, still rely heavily upon the traditional analysis framework of the competition law by defining the relevant market as the initial step for regulatory action.

With relevant markets successfully defined, the next step of the competition law analysis is the analysis of the market power. This is exactly what the EU and the U.S. legislators do in their proposed acts. Just as the principle of the competition law states, not all conduct is condemnable unless there is dominant market power associated with. The wording for platforms with market power in the regulatory zone may be different, as in the EU prefers "Gatekeepers"[8] whereas the U.S. uses "Covered Platforms,"[9] but both refer to an identical method comprising four factors, namely active end user numbers, active business user numbers, revenue, and market capitalization. The only difference is the thresholds applied for each factor, as illustrated in Table 1.

Table 1: Thresholds for Market Power in the EU and the U.S.

	Active End Users (mil.)	Active Business Users (thous.)	Revenue (bil.)	Market Value (bil.)
EU	45	10	€7.5	€75
U.S.	50	100	$600	$600

It is not hard to find out that all of those four factors are also ones to evaluate dominance under the competition law. Market shares and the market structure reflect the weight of a firm on its relevant market, and hence indicate its market power. The idea of market structure has been integrated into the competition law analysis since the emergence of the Harvard School, under the "SCP" paradigm that certain types of market structures (S) give rise to abusive conduct (C) that results into anti-competitive performance (P). Thus, in order to prevent anti-competitive behavior, it is best to go after the root cause. After taking care of the market structure anti-competitive behavior will disappear itself.[10]

> ***With relevant markets successfully defined, the next step of the competition law analysis is the analysis of the market power***

This idea is so embedded in modern antitrust policy that often the market shares of a firm are viewed as a strong proxy for its market power. Assumptions concerning dominance based on the scale of market shares have been officially or unofficially established across jurisdictions. In terms of weighing platforms' market power, it can be observed that both the U.S. and the EU are heavily influenced by the Neo-Brandeisian school, which advocates the restoration of the structuralist paradigm of the Harvard School and the idea that with great power, comes greater responsibilities and obligations.[11]

In order to maintain a fair and healthy competitive market for the digital sector, those powerful and dominant platforms must be kept in check. The last step of competition law analysis is to specify obligations and to take actions. Just as the traditional anti-monopoly law analysis framework would do, the EU's and the U.S.'s proposals both come up with detailed obligations. The EU's act sets mainly five groups of obligations, (1) obligations on transparency to business users; (2) obligations on interoperability to third party applications; (3) prohibitions on the practice of self-preferencing; (4) prohibitions on exclusive dealing, and (5) obligations on data portability and interconnection.[12]

The U.S.' proposed acts mainly include (1) limitations on business scope;[13] (2) prohibitions on acquisitions;[14] (3) prohibitions on self-preferencing;[15] (4) obligations concerning interoperability with third party applications;[16] and (5) obliga-

8 See DMA, *supra* note 2, Article 3.

9 See Ending Platform Monopolies Act, *supra* note 6, Section 5(5).

10 See Herbert Hovenkamp, "The Harvard and Chicago Schools and the Dominant Firm" (2007), *Faculty Scholarship at Penn Law. 1771*, https://scholarship.law.upenn.edu/faculty_scholarship/1771.

11 See Lina Khan, "The New Brandeis Movement: America's Antimonopoly Debate," 9 *Journal of European Competition Law & Practice* 131 (2018).

12 See DMA, *supra* note 2, Article 5-6.

13 See Ending Platform Monopolies Act, *supra* note 6, Section 2.

14 See Platform Competition and Opportunity Act of 2021, H. R. 3826, June 11, 2021, Section 2.

15 See American Choice and Innovation Online Act, H. R. 3816, June 11, 2021, Section 2.

16 See Augmenting Compatibility and Competition by Enabling Service Switching Act of 2021, H. R. 3849, June 11, 2021, Section 3.

tions concerning data portability.[17] It can be inferred from those proposed obligations that the EU is attempting to restore the competitiveness of the digital sector by confining the power of gatekeepers, whereas the U.S. takes one step further to even divest covered platforms. The limitations in business scope and the prohibitions on acquisitions may give the U.S. government the power to step into the digital market and to actively break apart those digital conglomerates. This is indeed a way of protecting those small firms, albeit with great sacrifice.[18] Legislators in the U.S. should be aware of the benefit of economic of scale and scope and the network effect, all of which can increase efficiency and consumer's welfare.[19] Blind redistribution may reduce the level of competition, efficiency and consumer's welfare, and only lets the benefit flow to smaller firms or those that are still clinging to old technologies that have been rendered outdated by new ones, namely digital platforms in particular.[20]

Furthermore, the U.S.'s acts on self-preferencing are rather general and leave plenty room for interpretation. As what the American Innovation and Choice Online Act states, it is unlawful for covered platforms to engage in conduct that "advantages the covered platform operator's own products, services, or lines of business over those of another business user". In comparison, the EU's act specifies those particular practices that are considered self-preferencing to make regulation enforcement clear and direct without too much freedom for interpretation.[21] From such a sense the EU proposal is more practical than the U.S. one.

03
DRAFT REGULATION IN CHINA

China's two guidelines for regulating the digital sector follow the proposed acts of the EU and the U.S. The Classification Guidelines use business types and sizes to categorize platforms into different category. The Responsibilities Guidelines set obligations for platforms in certain categories. These two guidelines, however, did not capture the essence of the draft legislations in the EU and in the U.S., and contain three major problems.

First, the Classification Guidelines, instead of defining relevant markets where there may exist durable monopoly power, as those proposed acts in the EU and the U.S., choose to exhaustively list out all the business services that are available in the market. Those services are divided in six main categories with in total 31 sub-categories. Those six main categories are Online sales, life services, social entertainment, information, financial services, computing applications. Such a classification suggests the underlying assumption that all types of platforms may have the ability to exert market power. However, it is not compatible with the real market situations. Consequently, the Classification Guidelines, once adopted in such a manner, would possibly lead to over-deterrence to the digital competition.

Second, the thresholds for market power are comparatively low. It may square a large number of platforms under unnecessary regulation. Although the Classification Guidelines set distinct thresholds for super and large platforms, the Responsibilities Guidelines regulate the two with no difference, as illustrated in Table 2. Thus, the real threshold for regulation is those for large platforms.

Table 2: Platforms Proposed to be Regulated in China

	Active End Users (mil.)	Market Value (¥ bil.)	Business Scope	Power to Monopolize
Super Platforms	500	1,000	≥ two sub-categories of services	Super strong ability to limit access to users
Large Platforms	50	100	≥ two sub-categories of services	Strong ability to limit access to users

According to the statistics of the China Industrial Control Systems Cyber Emergency Response Team ("CIC"), a total number of 23 Chinese platforms might be categorized as large platforms. Among those, five of them meet the threshold for super platforms, namely Tencent, Alibaba, Meituan, ByteDance, and Ant Group. If international platforms that have strong Chinese footprint are counted, including but not limited to Google, Apply, Microsoft, and Oracle, the to-

17 *Ibid.*

18 See Herbert Hovenkamp, "Antitrust and Platform Monopoly," 130 *Yale Law Journal* 73 (2021).

19 See Daniel Sokol, "A Framework for Digital Platform Regulation," 17 *Competition Law International* 95 (2021); and Marco Cappaia & Giuseppe Colangelo, "Taming Digital Gatekeepers: the 'More Regulatory Approach' to Antitrust Law," 41 *Computer Law and Security Review* 105559 (2021).

20 See Hovenkamp, Herbert, "Is Antitrust's Consumer Welfare Principle Imperiled?," 45 *Journal of Corporation Law* 117 (2019).

21 See DMA, *supra* note 2, Article 7(2).

tal number can easily approach 30. In comparison, the U.S. covered platforms so far only cover the so-called GAFAM, i.e. Google, Apple, Amazon, Facebook, Amazon, and Microsoft. The EU thresholds are a bit lower, and may only include 13 platforms.[22] Even though the number of platforms that fall under the regulation coverage in the EU is far less than that in China, some scholars still criticized the threshold being a bit too low, and suggesting raising the threshold to reduce the number of platforms under regulation to be less than ten.[23]

Third, the Responsibilities Guidelines impose only four obligations nonetheless in a very general sense.[24] Those are (1) prohibition on the use of business users' data to compete with them; (2) prohibition on self-preferencing; (3) obligations on interoperability, and (4) prohibition on the use of one service on the condition of another. In comparison with proposed acts in both the U.S. and the EU, China's proposed draft has fewer obligations, and leaves too much discretion for the agency in the subsequent enforcement.

04
ROOM FOR IMPROVEMENT

The analyses above suggest that these two proposed guidelines need to be significantly revised in order to fulfill the goal of strengthening anti-monopoly in the field of platform economy in the future.

First and foremost, the 31 subcategories of platform services need to be reduced, and to focus on areas where durable market power may exist and would affect the competitiveness of the digital sector in the medium to long run. The EU's categorization of core platform services can be a good reference. The platform governance should rely on the interaction between competition law and sector-specific regulation. Once there is the lack of durable market power competition law should suffice to govern anti-competitive conduct thus arouse.[25] Consequently, the delineation of platform services, as an initial step, should serve the purpose of identifying platforms' services that might lead to medium to long term sustainable market power, rather than embracing all the types of digital services. As such a more or less clear borderline can be drawn between the competition law and the platform regulation. Otherwise, not only the proposed sector-specific regulation might be too broad so as to cover unnecessary digital services, but also the intrusive obligations imposed afterwards may distort competition in the digital sector. For such a goal, public inquiries should be carried out as to whether it is necessary to square a certain type of platform service for sector-specific regulation.

Moreover, the thresholds in the Classification Guidelines are too low in defining super and large platforms with factors such as business types and power. As analyzed before, the Chinese proposal would net much more platform operators than the EU and the U.S. The inclusion of platforms without durable market power gives the agency too much discretion, thereby possibly leading to governmental capture. Furthermore, unnecessary obligations also make platforms incur extra costs for compliance, and reduce their incentive for innovation and the desire for seeking economic efficiency.[26]

Last but not least, the Responsibilities Guidelines aim at eliminating anti-competitive practices, and restoring a healthy and fair digital market. However, the ambiguous terms in the current version are unable to achieve the effect of better regulating the digital sector, and would generate too many legal uncertainties for the subsequent enforcement. Therefore, it is proposed to not only include more obligations, but also lay out more detailed conditions for the particular scenarios for those obligations.

> ***"The Responsibilities Guidelines aim at eliminating anti-competitive practices, and restoring a healthy and fair digital market***

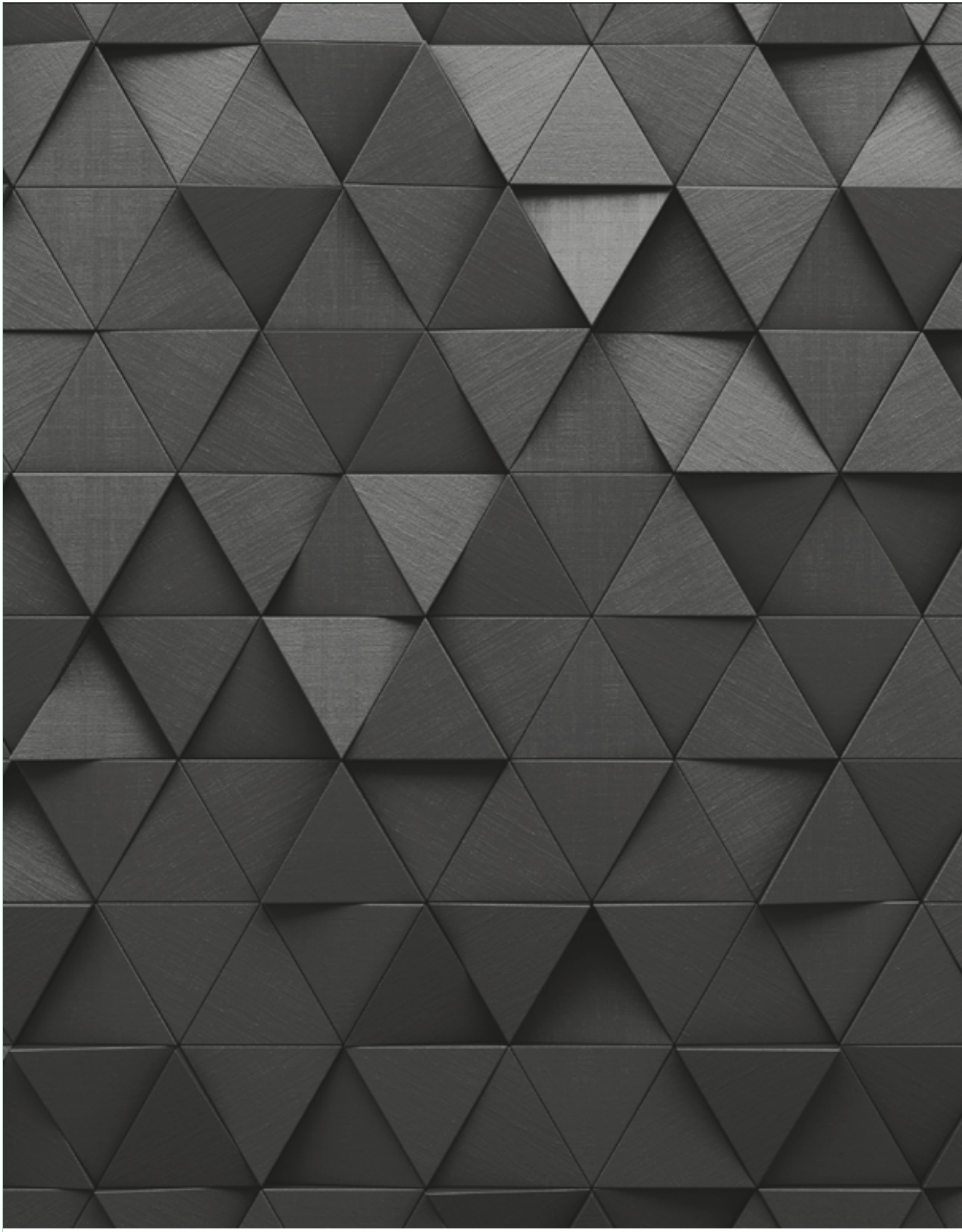
22 These 13 platforms are the GAFAM and Airbnb, Oracle, Paypal, Salesforce, SAP, Videndi, Yahoo, and Zoom. See Mario Mariniello & Catarina Martins, "Which platforms will be caught by the Digital Markets Act? The 'gatekeeper' dilemma"(2021), https://www.bruegel.org/2021/12/which-platforms-will-be-caught-by-the-digital-markets-act-the-gatekeeper-dilemma/.

23 See Damien Geradin, "What is a Digital Gatekeeper? Which Platforms should be Captured by the EC Proposal for a Digital Market Act?" (2021), https://ssrn.com/abstract=3788152.

24 Article 16 and 17 of the Responsibilities Guideline specifically require platforms to act in accordance with the Anti-monopoly Law and the Anti-Unfair Competition Law. However, this is not really an additional obligation.

25 See OECD, "Ex ante Regulation in Digital Markets – Background Note," DAF/COMP(2021)15, December 1, 2021.

26 See Phillip E. Areeda & Herbert Hovenkamp, *Antitrust Law: An Analysis of Antitrust Principles and Their Application*, New York: Wolters Kluwer (2020), 260-262.



WHY REGULATION OF DARK PATTERNS IS HERE TO STAY

BY
MIHIR KSHIRSAGAR

Tech Policy Clinic Lead, Center for Information Technology Policy, Princeton University.

01 INTRODUCTION

Consumer protection regulators across a variety of jurisdictions are taking on the challenge of combating online "dark patterns" through targeted enforcement actions and new rule-making initiatives. Broadly speaking, dark patterns are user interface techniques that benefit an online service by leading users into making decisions they might not otherwise make. Some dark patterns deceive users, while others exploit cognitive biases or shortcuts to manipulate their actions. But businesses

complain that authorities' newly found attention to the issue of dark patterns risks targeting legitimate persuasion techniques that have been long used in the marketplace. Alternatively, they complain that dark patterns are a squishy or amorphous concept and that the lack of standards creates an unacceptable degree of regulatory uncertainty. This article examines the future of dark patterns regulation for the tech industry and explains why the issue is not a passing fad. I argue that businesses should prepare for continued scrutiny of their practices and should develop proactive mechanisms to address regulatory risk.

02

FRICTIONLESS DESIGN PROMOTES INTERESTS OF SERVICES OVER CONSUMER CHOICE

The early days of the Internet promised a marketplace that minimized the cost of price discovery and empowered consumers with information to make rational, intelligent choices. Needless to say, this semi-mythical frictionless world has not come to pass. Instead, online services seized on insights from behavioral researchers to develop digital interfaces to manipulate consumers in a variety of different settings. Harry Brignull, a user experience designer who coined the term dark patterns, used it to name and shame "tricks used in websites and apps that make you do things that you didn't mean to, like buying or signing up for something."[2]

Three core drivers inform the strategy of using dark patterns. First, there is a strong incentive for services to protect margins by increasing switching costs. Interface designs that obscure true costs or inhibit price discovery benefit the service at the expense of consumers. Second, designers have the ability to quickly run large-scale micro-experiments that optimize for presenting information that creates the least amount of friction for the choices that benefit the service. For example, studies have shown how the use of A/B testing could introduce dark patterns that inhibit obtaining meaningful consent if the sole metric of performance is the click-through rate. Third, the longevity of the customer relationship for online services is quite short. [X percent of customers switch every y years.] As a result, there are fewer incentives to build long-term loyalty and more incentives for firms to prioritize extracting value early in the relationship.

Several research studies document how dark patterns have proliferated across online services as a profitable strategy. Dark patterns may start with the advertising of a product or service, and can be present across the whole customer path, including sign-up, purchase, and cancellation. And dark patterns are not just limited to purchases. Consumers encounter dark patterns when making choices to consent to the disclosure of personal information or to cookies, or when interacting with services and applications like games or content feeds that seek to capture and extend consumer attention and time spent.

The different types of dark patterns observed by researchers can be separated into two themes that affect the choice architecture facing users: (a) interfaces that modify the set of choices available to users; and (b) interfaces that manipulate the information that is available to users. The main feature of dark patterns is that they take advantage of consumers' cognitive shortcuts (heuristics and biases) in their decision-making processes. By doing so, dark patterns unfairly influence people's choices — the core concern of consumer protection laws. When confronted with dark patterns, consumers are manipulated, deceived, or coerced into accepting something that they would not have chosen if that were a free and informed choice.

03

INTERNATIONAL REGULATORY RESPONSES

There are few mechanisms for market self-correction in the use of dark patterns. In some egregious cases, especially across repeated interactions, consumers can become wise to improper influence methods. But this can breed a general distrust of all businesses that hurts honest marketers in the wake. There are also limited incentives for competitors to highlight their advantages of transparent pricing and persuasion tactics. But those instances are few and far between, as many online markets for products and services share attributes that allow them to settle into an equilibrium that thwarts user intentions.

As a result, several jurisdictions around the world are working on regulatory responses to address the problem of proliferating dark patterns online. These responses fall in two categories — privacy regulations that address the use of dark patterns in the context of obtaining consent for the use of personal information, and updating consumer protection regulations to clarify the application of longstanding prohi-

2 Harry Brignull, https://www.deceptive.design/.

bitions against deceptive or unfair practices in the online context.

In Europe, the new Digital Services Act ("DSA") imposes restrictions on services that use their online interface (either through structure, design, or functionality), to impair users' ability to make free, autonomous, and informed decisions or choices (Article 13a). The DSA seeks to empower users to make decisions about critical matters without being subjected to practices which exploit cognitive biases (Recital 39a). The DSA provides specific examples of prohibited practices such as: (a) giving unequal visual prominence to any consent options when asking the user for a decision; (b) repetitively requesting or urging the recipient to make a decision such as repeatedly requesting consents to data processing where consent has previously been refused (especially in the form of a pop-up that interferes with the user experience) or has been refused through the use of automatic refusal configurations; (c) urging a user to change a setting or configuration after the user has already made a choice; or (d) making the procedure to cancel a service significantly more cumbersome than signing up to it.

In China, the regulators have floated various proposals to regulate the use of dark patterns. For example, they have proposed a requirement that there should be a one-click closing button for pop-up advertisements, start-up playback, video insertions, and other such interstitial advertising. They have also suggested requiring companies to collect and maintain data about their algorithmic recommendations for personalized advertising to allow the government to evaluate if those algorithms might be manipulating users.

> ***As a result, several jurisdictions around the world are working on regulatory responses to address the problem of proliferating dark patterns online***

Meanwhile, the Australian Competition & Consumer Commission ("ACCC") released its third digital platform services inquiry report that investigate measures to mitigate the use of dark patterns. Separately, on the issue of obtaining meaningful consent, the ACCC is considering more stringent criteria for what constitutes consent to prevent firms from relying on dark patterns to trap unwary consumers.

In the United Kingdom, the regulators are actively studying the impact of dark patterns and online choice architecture more generally. The Competition and Markets Authority ("CMA") published two papers in April 2022 discussing and summarizing evidence on online choice architecture and how it potentially causes harm to consumers. Common examples of choice architecture include the order of products in search results, the number of steps needed to cancel a subscription, or whether an option is selected by default.

The CMA contrasts well-designed websites, apps or digital services built with consumers' interests in mind that will help consumers choose between suitable products, make transactions faster, and recommend new relevant products or services, with choice architectures that hide crucial information, set default choices that may not align with consumer preferences, or exploit consumers by drawing attention to scarce products. The CMA has a multi-prong strategy to tackle abuses. First, it will challenge choice architectures that mislead and harm consumers or undermine their trust and confidence in online markets. Second, it will use a combination of behavioral science, data science, and other methods to determine the prevalence of harmful practices. Third, it will engage in bilateral and multilateral engagement with other authorities and regulators to develop effective strategies to regulate harmful conduct. Fourth, it will raise consumer and business awareness of such practices.

04
UNITED STATES

The United States, home to the largest online markets by value, has been slower to react to problems created by dark patterns. But now the traditional regulatory preference for a wait-and-see approach is giving way to a growing recognition that some type of response is required. At the federal level, the proposed DETOUR Act, aims to regulate the use of dark patterns by large online platforms. The Federal Trade Commission ("FTC") held a workshop about dark patterns last year and is in the process of updating its online disclosure guidelines that is likely to contain guidance on avoiding dark patterns. It has also brought several cases recently that focus on the use of dark patterns. At the state level, there are a series of enforcement actions by state attorneys general applying their unfair and deceptive practices doctrines to the online context, as well as rulemaking proceedings in the privacy realm that ensure that services are appropriately obtaining consumer consent without resorting to using dark patterns to trick users.

A recent case from the New York Attorney General's office ("NYAG") illustrates how enforcement authorities might seek to reign in egregious practices. (Disclosure: I worked in that office from 2016 to 2019.) In 2022, the NYAG obtained a settlement with Fareportal – a large online travel agency — that resolved its use of deceptive practices to manipulate consumers to book online travel. The investigation focused

on how Fareportal, which operates under several brands, including CheapOair and OneTravel, used a series of dark patterns to pressure consumers to buy tickets for flights, hotels, and other travel purchases. Specifically, Fareportal exploited the scarcity bias by displaying, next to the top two flight search results, a false and misleading message about the number of tickets left for those flights at the advertised price. It manipulated consumers through adding 1 to the number of tickets the consumer had searched for to show that there were only X+1 tickets left at that price.

Another design feature Fareportal introduced exploited the bandwagon effect by displaying how many other people were looking at the same deal. The site used a computer-generated random number between 28 and 45 to show the number of other people "looking" at the flight. It paired this with a false countdown timer that displayed an arbitrary number that was unrelated to the availability of tickets. Similarly, Fareportal used these false scarcity indicators across its websites and mobile platforms for pitching products such as travel protection and seat upgrades, through inaccurately representing how many other consumers that had purchased the product in question. In addition, the NYAG charged Fareportal with using a pressure tactic described as "confirmshaming" to make consumers accept or decline purchase a travel protection policy to "protect the cost of [their] trip" before completing a purchase. Finally, the NYAG took issue with how Fareportal manipulated price comparisons to suggest it was offering tickets at a discounted price, when in fact, most of the advertised tickets were never offered for sale at the higher comparison price. The findings from this investigation illustrate why dark patterns are difficult for consumers to identify or avoid. As a result, absent firm regulatory action, such tactics risk becoming entrenched across different travel sites who have the incentive to adopt similar practices.

Another design feature Fareportal introduced exploited the bandwagon effect by displaying how many other people were looking at the same deal

A recent multistate enforcement action against Intuit, which sells the TurboTax service to file taxes, took the service to task for obscuring free filing options to drive traffic to paid product. The investigation documented how Intuit used confusingly similar names for the free and paid products and took active steps to prevent consumers from finding the lower cost option by hiding hid the free site from search engines. Importantly, TurboTax let users make a "choice" to take paid option. But the enforcement authorities cut through that defense by highlight how this was a false choice because it was presented only after users had invested considerable time on their platform entering data, and they were not likely to change their minds after investing that time. Intuit settled the allegations for $141 million that restored funds to 4.4 million duped customers. Another recent multistate action, led by the D.C. Attorney General, is litigation that concerns Google presentation of its location tracking settings that the states allege obscures that information collection and inhibits the ability of consumers to control who has access to sensitive information.

05
COMPETITION ISSUES

The concept of dark patterns is also gaining purchase in competition actions. For example, private plaintiffs have successfully used allegations involving dark patterns in antitrust class actions to advance past the motion to dismiss stage. In *Klein v. Facebook* (N.D. Cal. 2022), plaintiffs alleged that Facebook's misleading privacy practices duped users to turn over information and entrench Facebook's dominant position in the relevant market. Specifically, the plaintiffs argue that Facebook's "No, Thanks" to information sharing prompt led users to believe that they had control over how Facebook could use their purchasing data when, in reality, Facebook was collecting and selling that data through its use of web beacons. Similarly, they assert that the "Like" button and "view tags" secretly transmitted data to Facebook. The core competition claim rested on the allegation that by selling increased amounts of data to third parties while representing to users that it was keeping data private, Facebook increased its user base and its profits. In other words, Facebook's deception allowed it to prevent sophisticated rivals from entering the market and thereby avoided competing on the merits. The court found this claim was sufficient to survive the dismissal motion.

The key issue for the competition analysis is to separate tactics that involve legitimate price discrimination from those that discriminate using undisclosed factors to on manipulate the consumer. Indeed, some services have turned to private versions of dark pattern rulemaking by applying anti-discrimination principles to protect their consumers. A prominent example of this tactic is American Express' anti-steering rules that prevented merchants from steering consumers to lower cost payment systems at checkout. The multistate enforcement action challenging those rules failed at the Supreme Court because the Court found that the authorities had not properly accounted for the benefits to consumers from such rules. (Disclosure: I worked on behalf of American Express in the enforcement action.) This issue resurfaces in the actions challenging the role of the Android

and iOS app stores in imposing rules to protect consumers from manipulation by third party services. Apple's changes to iOS requiring more transparent information collection, for example, has led to significant benefits to consumer welfare as consumers can begin to exercise meaningful choices concerning their privacy.

06
FUTURE CHALLENGES

As dark patterns regulations progress, there are undoubtedly going to be some difficult line drawing exercises between legitimate persuasion and improper coercion. But this is not that different from the line drawing around unfair and deceptive business practices. Guidelines and settlements can provide the type of clarity legitimate businesses need to avoid running afoul of regulators. Some of the more egregious uses of dark patterns revolve around the need to obtain meaningful consent for data practices. Privacy regulations that go beyond the notice & consent framework should hopefully alleviate the pressure on seeking the initial sign-up as regulators focus more on how data is used and shared.

At a higher level, businesses can protect themselves by using ethical design principles that focus on fair and transparent information disclosures. They can also develop interfaces that account for differences in particular vulnerable users to ensure that they comprehend the choices presented to them. In addition, they should encourage and then respect consumer-focused technological innovations to counteract harmful patterns such as browser-based that send automated signals from users about their information collection preferences.

One key defense that is likely to be litigated extensively rests on the argument that the services have a right under the First Amendment to engage in unfettered promotional activity. Historically, courts have been reluctant to have First Amendment principles override traditional state power to protect consumers, believing that rules that promote an honest and transparent marketplace do not impose a significant cost on protected speech activity. But the current Supreme Court is more willing to credit the free speech interests of corporations. And, because some of the fixes for dark patterns are not simply about requiring more speech by way of additional disclosures, there are likely to be stronger First Amendment arguments. As enforcement authorities litigate these challenges, evidence of actual consumer confusion is pivotal to determining if the regulations are a proportional response to misleading or deceptive speech.

In summary, efforts to reign in dark patterns are likely to be a significant issue in the regulation of the tech industry for many years to come. The enforcement authorities' core motivation to create a level playing field for businesses to operate in a fair and transparent manner should be a welcome development for businesses interested in developing long-term relationships with their consumers.

As dark patterns regulations progress, there are undoubtedly going to be some difficult line drawing exercises between legitimate persuasion and improper coercion

ABOUT US

Since 2006, **Competition Policy International** ("CPI") has provided comprehensive resources and continuing education for the global antitrust and competition policy community. Created and managed by leaders in the competition policy community, CPI and CPI TV deliver timely commentary and analysis on antitrust and global competition policy matters through a variety of events, media, and applications.

As of October 2021, CPI forms part of **What's Next Media & Analytics Company** and has teamed up with **PYMNTS**, a global leader for data, news, and insights on innovation in payments and the platforms powering the connected economy.

This partnership will reinforce both CPI's and PYMNTS' coverage of technology regulation, as jurisdictions worldwide tackle the regulation of digital businesses across the connected economy, including questions pertaining to BigTech, FinTech, crypto, healthcare, social media, AI, privacy, and more.

Our partnership is timely. The antitrust world is evolving, and new, specific rules are being developed to regulate the so-called "digital economy." A new wave of regulation will increasingly displace traditional antitrust laws insofar as they apply to certain classes of businesses, including payments, online commerce, and the management of social media and search.

This insight is reflected in the launch of the **TechREG** Chronicle, which brings all these aspects together — combining the strengths and expertise of both CPI and PYMNTS.

Continue reading CPI as we expand the scope of analysis and discussions beyond antitrust-related issues to include Tech Reg news and information, and we are excited for you, our readers, to join us on this journey.

Scan to Stay Connected!

Scan here to subscribe to CPI's **FREE** daily newsletter.

CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit **competitionpolicyinternational.com** today to see our available plans and join CPI's global community of antitrust experts.

CPI COMPETITION POLICY™ INTERNATIONAL