Keio University Global Research Institute (KGRI)

Great Thinker Series

"How Can and Should the Platforms be Governed? Assessment of EU Digital Services/Markets Acts"

Version 1.0

January 2023

Lawrence LESSIG

Discussant: Jiro KOKURYO

This is a revised transcript of Prof. Lawrence Lessig's KGRI Great Thinker Series on June 24, 2022.

Content

Introduction

Haluna Kawashima
Project Associate Professor, KGRI, Keio University
Good afternoon, everyone. Welcome to the Keio University Global Research Institute's Great Thinker Series. Today we will talk about how can and should the platforms be governed and an assessment of the EU Digital Market Act and Digital Services Act. Before we begin, let me briefly introduce Professor Lawrence Lessig, today's guest speaker. Professor Lawrence Lessig is the Roy L. Furman Professor of Law and Leadership at Harvard Law School. Prior to returning to Harvard, he taught at Stanford Law School, where he founded the Center for Internet and Society. He also clerked for Judge Richard Posner on the Seventh Circuit Court of Appeals and for Justice Antonin Scalia on the Supreme Court. Professor Lessig is a founder of Equal Citizens and a founding board member of Creative Commons. He is also a member of the American Academy of Arts and Sciences. Professor Lessig is known as an author of numerous books read worldwide—in Japan, too—such as "Code" and "Remix" and as a critical player in reforming the theories and practices on network space order. After two tentative attempts to invite Prof. Lawrence Lessig to Japan to our campus, which were turned into online conferences in 2019 and last December, it is an extreme delight for us to have a face-to-face dialogue with Professor Lessig today. To start the events, we have the great pleasure of inviting Professor Kohei Ito, the President of Keio University, to give an opening speech. [Japanese] Please.

Kohei Itoh
President, Keio University
Last December, I actually attended online this KGRI Great Thinker Series, presented, of course, by Professor Lawrence Lessig. The title of the symposium was "The Change in the Media and Democracy in the Digital Society." It was so timely, and even though it was given online, I was so impressed by the contents of Professor Lessig's talk. Of course, it was cutting-edge and also eye-opening on ideas at the forefront of how we connect and how we should really think about the connection between our everyday life and the constitutional law and the digital society. But also, I was so impressed by his style of presentation. The entire presentation was performed in a way where he was standing in front of the background material, and whatever was shown behind him flew by very naturally as he spoke. Speech is a very important element of teaching at Keio University, so Professor Lessig's presentation was both academic excellence and also presentation excellence. It was really the textbook presentation, and I could really see the forefront of how social science is developing. So I'm very happy to meet Professor Lessig in person today. I'm very much looking forward to this talk on the relationship between war, media, and also digital society. So, with this, I would like to introduce and welcome Professor Lessig. Please.

Main Talk

Lawrence Lessig
Roy L. Furman Professor of Law and Leadership, Harvard Law School
I am grateful for the welcome and the opportunity to visit Keio University again. The first time I visited was 20 years ago, and we've tried many times to arrange a return. But COVID stopped that return over the last three years. I'm so happy that we were able to make it work this time.

When I came this time, I was given an assignment. I usually give assignments, I don't usually receive assignments. But I was happy to receive this assignment. The assignment was to reflect upon the European Union's strategy for regulating digital platforms. In particular, the Digital Services Act, which is on the cusp of being adopted, as is the Digital Markets Act now.

In the context of American politics, one is told never to answer the question asked and only ever answer the question you wish had been asked. But alas, I am a failed politician, so I will accept the assignment and answer the question asked. But I want to answer it in a way so as to allow us to think about the problem of governance generally. Because these particular statutes point, I fear, in the direction of a failure of governance in the digital age. We need to learn about the nature of that failure and respond to it. Quickly.

Here's the background: Twenty-five years ago, for about a nanosecond, I was special master in the *United States v. Microsoft Corp*. case. (Or, at least, I remember I was. Wikipedia doesn't actually mention that I was, but I do have a distinct memory about it, so I will assume that, in fact, I was.)

That case became the most under-appreciated case in Internet history. There was a single principle in that case that became foundational for Internet policy. That principle was this: Do not use your power, the power of monopoly, to protect yourself from your competition. That was the objective of the prosecution in the Microsoft case: To avoid the then present monopoly—Windows 95—from leveraging that monopoly as it did against innovators from the future.

That monopoly, of course, arose when the company Microsoft, through the MS-DOS operating system, established itself as the platform for innovation in the PC market. And as that platform evolved into Windows, Windows extended its reach beyond the operating system into the application layer of the PC market. At the time, the operating system was dominant. Microsoft thought it had perpetual control over the development and innovation in the PC market, but what it feared was that as this stack extended to include the Internet, there was a promising new competitor. That competitor was the combination of a browser and a programming platform that promised to extend across all platforms. The fear Microsoft had was that its operating system would become just one of many and, therefore, its monopoly power in the

PC market would be contracted. The idea was controversial. But whether you think it was plausible or not, what's clear is that Bill Gates believed it was possible. And through his "Internet Tidal Wave" memo, he raised a “five-alarm fire” inside Microsoft, to get the company to defend itself against this new competition.

Microsoft defended itself in a very particular way. Its objective, the evidence showed, was to crush the competition. To “take away their oxygen supply and crush them.” And it is from this intent that the "United States v. Microsoft Corp." case was born.

The case was fueled importantly by the victims of this “fight” against competition. Those competitors feared this dominant player. That reality was a strategic mistake. Microsoft had made their competitors their enemies, rather than making them their friends. This is a subtle joke, but it's a serious point that we need to recognize in the context of the current nature of the Internet market. Microsoft aimed to crush the ecology of competition, and venture capitalists responded to that very aggressive effort. They first responded by never funding anything anywhere near Microsoft's monopoly. Just ask WordPerfect about the consequence of running against a Microsoft platform. Microsoft intended to crush the competition, and that aggressive response was not going to last.

So, in 1992, when Bill Clinton became President, he brought into his administration a key troika of thinkers about the nature of innovation. Al Gore, who, of course, famously invented the Internet. Well, not really. He never said he did, but that's how he was mocked. Reed Hundt, who became the Chairman of the FCC. And Joel Klein, who became the Deputy Attorney General charged with antitrust. These three decided it was important to do something against the aggressive actions of Microsoft, to do something to save the Internet from a future dominated by Windows. It’s kind of astonishing in retrospect to recognize that the American government would do this. It was an extraordinary thing to do to take on America’s most successful technology company. At the time, technology companies were the key to the future of the economy in America. I didn't think so at the time, but I was naive. Back then, when I was relatively young, it was naive to think there was anything special about the US government standing up to technology.

But it's important to recognize, because if we step back from where we are today, in 2022, and ask the question: When was the last time the United States government took on a major technology company through an antitrust action? And the answer is, in 2022, we can say the last time was United States v. Microsoft Corp. in 1998. That in the past 25 years or so, there's been only one major antitrust case in this critically important context of the economy. And because it was so long ago, the important principle of that case has been forgotten: "Do not use your power to protect yourself from the competition, whether that power is used aggressively to crush your competition, or it is used not so aggressively to buy your competition." It is misuse of market power that ought to be policed by the government. But

when the government won its case in 2001 against Microsoft, and Microsoft stood down, the lesson we should take from that victory is the opportunity it opened up for innovation. Because there's a slew of companies that then were born and expanded and took off then because of the freedom established by that important legal principle. Yet, unfortunately, very quickly antitrust was forgotten.

I remember attending an event with Barack Obama at the Googleplex. Google loved Barack Obama. Silicon Valley loved Barack Obama. And the Democrats, in turn, loved the Internet. The consequence of that love fest was a refusal to deploy antitrust in the context of technology platforms. Antitrust was told to stand down. And the consequence of that is the problem the world now sees. Because the platform for culture, commerce, and politics has become dominated by a few giants. And these are smarter giants. They are kinder giants. If you challenge them, they don't crush you. They buy you out. This is the new business model, a business model where everybody gets rich, while the super-rich become super powerful. The only losers in this new equilibrium are the people who would press an innovation that would challenge the dominant business model of the platform — and not give in to those in power now.

So, what is that dominant business model that now remains unchallenged because antitrust does not guarantee that the innovators who would challenge it have an opportunity to challenge it without being crushed through acquisition? Think back to 2003: there is competitive health at each of the three layers of the platform. The hardware layer is competitive. The operating system layer has increasing competition from Apple and from GNU Linux. The applications layer has lots of new applications, and the internet layer is extremely competitive as many, many companies are competing for dominance. Yet as that stack evolves to circa 2007, we should recognize conceptually a new layer that gets added to the Internet. We should call that layer a “data layer.”

The data layer in turn becomes the most important layer for value and profit in the context of the Internet. Because with the birth of modern advertising, which Shoshana Zuboff has brilliantly captured with the title "surveillance capitalism," the business model of the internet changes. That model now depends upon engaging and knowing you, the user. The more it knows, the better it performs. There are network effects, of course. There were always network effects with the operating system, which was why Microsoft was able to succeed so powerfully with the dominant operating system. But the network effects on the data layer are huge. Much greater with data, and much more profit is possible.

Surveillance capitalism in turn creates a slew of new businesses trading on these data. Yet there are just four dominant companies on the Internet platform and one in real space. All have built a machine of surveillance; that surveillance is produced through the data they collect.

These data are not just found. It's not just as if these companies are passively sitting and watching what we do the way a webcam at the side of the road might be able to count how many white cars drive by. Instead, the platform is active. It's poking and tweaking and asking us questions. It is rendering us emotionally vulnerable, reaching down the brain stack to leverage our insecurity so that we reveal more. This is the business model of Facebook and Instagram. And as they make us feel insecure or unengaged, we engage more, we do more, and we reveal more — so that they see more, so that they can sell better ads. This is the cycle of surveillance capitalism. And it is the most important dynamic in the modern context of the Internet.

Some people speak as if this surveillance is all bad. Apple has become the most prominent advocate of the idea that surveillance is all bad. Here's a minute clip from Tim Cook's speech at the Computers, Privacy, and Data Protection Conference.

> *A little more than two years ago, I spoke in Brussels about the emergence of a data industrial complex. As I've said before, if we accept as normal and unavoidable that everything in our lives can be aggregated and sold, then we lose so much more than data. We lose the freedom to be human. Earlier today, we released a new paper called "A day in the life of your data." It tells the story of how apps that we use every day contain an average of six trackers. This code often exists to surveil and identify users across apps watching and recording their behavior. Right now, users may not know whether the apps they use to pass the time, to check in with their friends, or to find a place to eat may, in fact, be passing on information about the photos they've taken, the people in their contact list, or location data that reflects where they eat, sleep, or pray.*

Some speak at the opposite extreme, as if it's all good — as if all of this infrastructure of tracking is essential and productive in the context of the Internet. Facebook has taken this position. And at the time Apple was attacking the tracking built into these technologies, Facebook started to sell the idea that this tracking was good. That it was good for society. This was a very clever little video that they released at the time.

> *People have ideas. Ideas are all around. You watch them, buy them, ride them into town. And yet, for every big idea that rose to wild acclaim, there are so many more that never found their fame. And some might seem bizarre to you, and some are only for a few, but many are small businesses that simply lack the tools to find excited people who will stop and say, 'That's cool!' There's an idea for everyone, and you'll love yours. She'll love hers, too. These two get served up coffee because they adore the brew. If you're the type who needs to cruise or likes your bags in vivid hues, behold, it's there. These bikers got some new headwear. Small businesses and people make connections so profound, and all because personalized ads help good ideas get found.*

Between these two extremes, though, we should see that, in fact, this tracking, this surveillance, has some good and some bad both. And we can see this, I think, by focusing on the uses of these data.

I want to offer a matrix of these uses. On one dimension, we're going to distinguish between uses that benefit the user of the platform and uses that harm the user of the platform. Across the other dimension, we're going to think about uses that benefit society and uses that harm society.

With this matrix, we can pick the easy case first: Uses that benefit the user and benefit society. My favorite example of this is my Amazon account, which surveils what I do, and based on what I do and what I buy, it recommends to me things that I would want to buy. The things it recommends turn out to be things that I do want to buy. It's giving me something—giving me information—because of its surveillance of how I use its platform. And so, unless we're against books or against reading or against commerce in general, we should recognize this is a use that benefits both me and benefits society.

Then there are uses that harm the user but benefit society. We can imagine technologies being developed right now to make it easy to identify predators who are using the platform to harm, for example, children. That use, of course, benefits society — to be able to identify those predators, even if that use harms those predators. They're worse off. They would prefer a world where they were not so easily identified. But that, too, is facilitated by the ability to surveil and engage in analysis based on surveillance.

And then there are cases that harm the user and harm society. One tragic story about gaming culture is a story about a certain class of gamers who simply can't control themselves: People who spend such an extraordinary amount of money on gaming — they're called "whales" — that they're basically subsidizing the platform for everybody else. These gamers are identified through surveillance; the fact that they are exploited is a fact that it's harmful to them and to society. The fact that surveillance leads to identifying and exploiting them is something that society, in general, should oppose.

These are relatively easy cases. The fourth is the most interesting case: Uses that benefit the user but harm society. What is that class of cases?

To recognize this class of cases, we're going to introduce a concept that I've talked about before: "brain hacking." This concept was inspired by the extraordinary technologist Tristan Harris, who left Google to start the Center for Humane Technology to make understandable to the rest of us the emergence of an incredibly important science within Silicon Valley. That science is the science of engineering attention to overcome the resistance that people would

naturally have to the use of digital technologies so that they spend more of their time using digital technologies. That engagement, therefore, becomes more profitable for the platforms.

This science—engineering attention—does its work by exploiting evolution, exploiting the ways that we happen to have evolved. So, we have evolved to be particularly susceptible to random rewards, and so this becomes a dynamic of the engineering platform to make it, so we become more addicted because of its random rewards or because we are particularly bad at resisting bottomless pits of content: the perpetual scroll. That's something we can't draw ourselves away from easily.

The platforms exploit this fact to engineer the platform to make it so that we will engage with the platform more. All of this engineering is with the aim of gathering more data about us for the purpose of selling ads to us.

This gathering itself has effects on us. So, think about the effects of the Facebook News Feed. That news feed has individual effects: It triggers and feeds certain addictions and depressions. Depression is particularly significant in certain classes and demographics, in particular young teenage girls. But it also has social effects, as it is architected to isolate and make us vulnerable as a way to drive more engagement with the platform.

As Zeynep Tufekci writes, "These companies are in the business of monetizing attention and not necessarily in ways that are conducive to health or success of social movements or the public sphere." In particular, they've discovered, through this science of attention, that the most successful way to drive our attention when it comes to democracy or politics is to exploit the politics of hate. Because it just turns out that we humans are more engaged and more willing to engage if we can be polarized and ignorant about the underlying issues that we are being engaged in. In the United States, the most extreme example of that dynamic, of course, was the embarrassment of January 6, when thousands of Trump supporters were led, not just by the President but also by social media, to believe that their election had been stolen and that they needed to rise up in a patriot-like way to revolt against this deep corruption of their government. This was, of course, a collective disaster, but for the media companies, this strategy was, individually, the most profitable strategy for them.

This is the externality we should recognize that social data produces. It is an externality that society needs to take account of. It is in this sense that I want to suggest we can see the NewsFeeds as uses that benefit the users — in the sense that the users are voluntarily choosing to subscribe to their Facebook NewsFeed rather than the Wall Street Journal or New York Times. But it harms society collectively because of the ways these platforms drive us to behave collectively.

But though this analysis is brilliant, I think is also a mistake. To frame it all as awful is not quite true. Some of it is awful, and some of it is not. But what make it awful is not a function of the surveillance. It is a function of its use. So that leads to an obvious question: Can we distinguish among these various uses and respond in a regulatory way based on that use? Can we be targeted in our response — to assure that surveillance does not produce negative social effects while allowing it to produce positive commercial, economic, and social effects?

That's the question that drives me to be interested in the assignment given me here today. Because in the context of the EU, we've seen an extraordinary range of regulatory innovations to address the problems presented by this platform of technology.

One not on my list, but with which I want to start with is GDPR. GDPR was the first major internet regulation. The Digital Services Act and the Digital Markets Act will complement GDPR. In thinking of these three together, I'm going to make three points to place them in context and see what's missing in what they've propose.

The first point is just simply: Wow. A functioning government. From the perspective of the United States, such a thing is totally and completely unimaginable. The idea that the governments would address privacy and digital services, and digital markets in a comprehensive and sensible way is fantasy in the United States. Because the government of the United States is essentially dysfunctional—non-functional—and it will not address these problems that it has created any time in the foreseeable future.

So, the first point to recognize is the gift the Europeans are giving the world by actually demonstrating reflectively sensible and serious engagement with the problems this platform has created — problems which have been created, in my view, because of the failure of the United States to carry through on the Microsoft principle, which would have stopped these platforms become from becoming the dominant negative forces that they have become. That then is the first point. Wow.

The second point is a little bit more qualified: The EU regulations are understandable, given the way we lawyers think about these problems. And from the way we lawyers think about these problems, the particular solutions they advance are smart and understandable. But I want to say that even though they're understandable, they are not wise. They are not wise strategically — because I fear they will produce a wholly predictable response, and that response is one that none of us should be eager to incentivize.

So, let's think about these points. I'm going to talk briefly, first, about the one I'm not asked to talk about—GDPR.

GDPR is grounded on the idea that individuals own their data and that their data should only be used with permission. This is a regulatory structure familiar to lawyers. We call it empowerment and choice. We empower the consumer, and we give the consumer choice. In the American context, empowerment and choice is like motherhood and apple pie. No one could be against it, because for us, empowerment and choice are an unambiguous good.

But I'm against it. I'm against empowerment and choice because of what empowerment and choice actually, or practically, will always look like. If you take the terms of service for the major internet services that people now use, these are the terms of services for these services. They are endless and incomprehensible. Microsoft's terms of service would take more than an hour to read, Spotify's would take about 36 minutes, Pokémon GO 35–36 minutes, and so forth. We empower people with "lawyer speak" that they can spend their life reading, and once they've read it, we stand back and say, "Have they understood it? Do they understand the implications of it? Do they understand the interactions between these different choices they've made with respect to these different platforms? Do they understand what happens when these platforms become co-owned? Do they understand anything about the practical privacy consequences of the choices that they have been ostensibly empowered to make through this empowerment and choice architecture?"

My answer to these questions is obviously no. And I could go on for hours about why I think this is a bad structure. But that is not my assignment today. So I'm going to put that to one side, and I want to move to the second one and think about a similar question in this context too.

Some of us in the United States, when we think about the Digital Services Act, are impressed that Europeans would be so sophisticated in their response. The Washington Post had an editorial where they said "US legislators should give themselves an easy assignment: read the European Union's Digital Services Act." That's something only someone who's never read the Digital Services Act can say, because there's nothing "easy" about reading the Digital Services Act. It's a massive regulation, and it's a significant burden of regulation even if its objectives are ones we should all praise. This platform of regulation recognizes a point that's become obvious to everyone: Digital services affect society — often well but often awfully. The DSA is focusing on the awful part, what we could think of as the "bad speech" produced by these platforms. By "bad speech," they're thinking about the illegal content produced on these platforms —bad advertising and disinformation. And the solution to this bad speech that is distinctive and different from the solution, or the non-solution, in the United States, is make the intermediaries responsible for dealing with this bad speech. This is different from the regime in the United States. In the United States, under the Communications Decency Act, these platforms have immunity from responsibility for this bad or harmful speech. The EU is flipping that responsibility: If you profit from the speech, you are responsible for the speech. And so under the DSA, there is first a conditional liability exemption —these platforms are

immune only if they don't know about the harmfulness of their content. But once they've been made aware, their exemption from liability disappears. Once they know, they've got to take steps to address this bad speech.

This is another principle that's significant, but importantly but very different: the DSA will require algorithmic disclosures so that we have a better understanding of exactly how these platforms are affecting us and driving us to behave through this engagement model. It will also establish a much greater regime of transparency to deal with complaints, in particular, complaints about speech that has been suppressed. And critically, the DSA will impose very serious penalties for platforms found to be violating these laws. These penalties have been crafted to make it no longer economically viable for companies that choose to operate within Europe not to obey these principles. Because if they do fail to obey these principles, Europe can leverage its enormous power to take up to 10%, in some cases, of their revenues. These are the broad principles embedded in this important rtegulaiton.

Then, there are some very interesting details. The first is a commitment to the principle that there's no general obligation to the police. There might be bad speech. The DSA says you are not obligated to look for it. If you are made aware of it, you might have to do something to maintain your immunity, but you don't have to police. Secondly, and critically important, the burden the regulation imposes is a function of the size of the platform. So, the burden to Google will be greater than the burden of a new version of Google, which is an essential qualification to ensure that we don't protect the dominant platforms from new forms of competition. The consequence then is to shift censorship into a purely private space. The government is not in the business of exercising judgment or requiring judgment on its behalf, but the platforms can exercise that censoring judgment.

Now we can do a similar analysis for the DMA. The critical idea behind the DMA is that it rejects the Chicago School of antitrust. That school was started by Robert Bork, a very famous right-wing academic, then judge, then failed nominee to the Supreme Court. Bork birthed this conception of antitrust by saying that antitrust should stop worrying about facilitating competition and instead worry solely on the question of consumer welfare. Yet this idea became a completely Orwellian conception of consumer welfare — because the total focus of the approach was to ask about the short-term consequence of mergers or competitive behavior on consumer prices. That means the doctrine ignores the structural or strategic long-term effect of mergers or the like. It just asks whether, in the next period, consumer prices will be low. That approach has come to dominate the American legal system. It has become the Justice Department's approach to antitrust, which is why, after the Microsoft case, we saw no antitrust enforcement in the United States.

In the DMA, the Europeans have rejected Robert Bork. I wish we would as well. Instead, the DMA embraces a more traditional conception of competition law. Those principles aim at

protecting and encouraging, not surprisingly, competition. They do this by focusing on the behavior of critical gatekeepers, a category of large players — which will include less than ten companies given the way this standard gets defined. And the way the DSA regulates these gatekeepers is to separate out two categories of behaviors: some which are presumptively forbidden and some which are questionable, and which will trigger further regulatory intervention.

The presumptively forbidden are these: the platforms or gatekeepers can't combine data among their different elements or companies that they might own jointly; they can't block third-party competitors with companies that they happen to own; they can't muzzle critics or businesses that they are dealing with who might want to criticize their behavior; they can't mandate single sign-on systems for anybody playing within their particular platform; they can't improperly bundle certain products within their platform that could exist independently and, therefore, competitively; and they can't hide the pricing that they are deploying for elements within their platform from businesses that are engaged in their platform.

All of these together look very much like the regulations imposed on telecommunication companies in the last century, in particular, here , in Japan, to facilitate competition in the deployment of broadband access. We used to call these principles "open access principles," and they were designed to assure competition in the provision of broadband, which in Japan, of course, led to an explosion in broadband at very low prices. This is the same strategy that the Europeans are now adopting for these Internet platforms.

The behaviors that will trigger questions are also not surprising: Business surveillance requiring or surveilling the businesses you're dealing with; lock-in of applications for that platform for those gatekeepers will open you up to further questioning; self-preferencing of your own functions over competitors will open you up for further questioning; blocking competitors, blocking data porting, blocking access to use and search data; and running single app-stores, as opposed to allowing competitive app stores. All of these operate as warning signs that will put the company more clearly into the regulator's scope.

the DSA and the DMA are smart, as we see the problem today. And again, by "we," I emphasize the particular role I play: lawyers. These are smart lawyer responses to the problems that have been identified. But now I want to step out of my role as a lawyer and ask, "Are they wise?"

This is the third part of the argument I want to make. And the answer to that question is this: No, they are not wise. They are not wise strategically, given two factors: 1) the cost of regulation and 2) the reality that code can replace the law.

Let’s start with the costs. What might be better in light of these regulatory costs?

As I've suggested in the context of the GDPR, a better regulation would have been to regulate the uses of data, and to be less obsessed with “empowerment and choice.” In the context of the DSA, there are two points: The first point is to recognize that surveillance itself is not the enemy. The enemy is the business models that build on that surveillance: business models that are destructive of socially important values. The DSA bans surveillance in certain narrow contexts. Surveillance for kids or surveillance for certain audiences that are vulnerable to the effect of surveillance. But my view, is it should have banned much more broadly, at least in the contexts where hate is profitable. News and politics are contexts in which banning this business model would mean ending business models that exploit hate, or that exploit the dysfunction our psychology produces. That strategy would be more effective than policing the particular content that might be produced or not within these contexts.

That's number one. Here’s number two.

Building on the insight of people like Daphne Keller, from the Stanford Center for Internet and Society. Keller looks at the regulatory burden imposed by these statutes and asks, "Is all of this process and documentation worthwhile?" Because obviously, the cost of this lawyer-obsessed system is huge, and its main focus is the adjudication of these single decisions permitting or not permitting content to be available. By asking "is it worthwhile," Keller is asking, “is it better than alternative approaches?”

One way to think about what the alternatives could be is to recognize that this whole lawyer-centric model for adjudicating speech may be mistaken. Evelyn Douek argued for a second wave of regulatory thinking about these internet platforms, one focused not on the particular speech but on the structure of incentives for producing speech that these systems are generating. That approach links back to my focus on the business model of the surveillance as opposed to the particular content or speech within there is surveillance. I agree with Douek: this is the approach we must push.

Okay, that's my view in the context of the DSA. My view of the DMA also has two points. The first point is small, but it's really important to talk about right now. The DMA insists on interoperability, and the first context the DMA for this requirement is with respect to messaging services. But that's a mistake. If you force interoperability with messaging services, you threaten the end-to-end encryption of messaging services as they exist right now. That's not an unsolvable problem, but it's not a problem likely solvable in the short term. Instead, rather than interfere with the security of an end-to-end system, we should step back from that requirement of interoperability.

The more important point is this: My colleague Richard Epstein celebrates "Simple Rules for a Complex World." There’s something to that idea that we should celebrate in this context as well. Here, the simple rule is the Microsoft principle. "Don't use your power to protect yourself

from the competition." Here, the monopoly that would be protected is the data monopoly. The question we should be asking in an Epstein-like way is, "Is there a simpler way, a more reliable and less costly way to avoid the monopoly problem in data?" And I think the answer to that is yes. My colleague Zephyr Teachout's book "Break Them Up" is just one of many powerful accounts of this alternative strategy. And the simple alternative strategy is the idea of chopping up these large. Now importantly, a breakup doesn't solve the problems that the DSA is trying to solve. One hundred surveillance capitalists are not necessarily better than five surveillance capitalists. So a breakup doesn't solve the problem of the harmful uses of speech that we might believe exist. But it does solve the monopoly problem. And it solves it in a way that is much more cost-effective than the massive layers of regulation that we imagine will be policing these platforms of power.

Those are the costs. The first critique I am making about the EU strategies is that they are more costly than is necessary or wise given their objective. But the second critique is more fundamental and more important. And I could tweak the EU f I presented the critique like this: Is the EU part of a Web3 conspiracy?

Everybody here knows Web3. My friend Joi Ito wrote a book in Japanese, which of course, I can't read, but which I understand is a powerful account of the importance Web3 to the future of the Internet. I think Web 3 should lead us to think about decentralized autonomous organizations (DAO) as an adjective. And then recognize the way in which there will emergence a class of services that are DAO-like in this way. This emergence is completely predictable because there will be many ways to use code to organize to execute life and business. The rise of Web3 is a predictable dynamic in the context of the evolution of the Internet.

The rise of Web3 is likely to be anti-monopoly, which is one reason people celebrate it. It is likely to break-up part of the power of these platforms. But here's the point I think people are missing: Web 3 is certain to be anti-regulation, in the sense that it will be regulation-insulating. It will make regulation more difficult—not impossible, but more difficult. I remember the good old days of web1 and internet1, where the same arguments were made about how the Internet was going to make regulation impossible. I feel sort of like Yogi Berra, because it feels like deja vu all over again. Once again, we have people telling us that these platforms will be unregulable. Yet again, that's just false. It's never impossible to regulate. But it certainly will be more difficult to regulate with Web3, and the concern I have about the EU strategy is that the strategy is inevitably going to accelerate the move to Web3.

The reason is simply this: Web3 will make it easier to achieve the business objectives of the companies that deploy it without many of the overriding regulatory burdens created by the DMA. So, the question for the EU is, "Why sabotage collective governance?" What we need here is strategic anti-bureaucratic regulation that avoids this consequence. But what we will

get in the face of EU-like regulations is more arguments for Web3, and more incentives to build Web3.

That begs the question I want to leave you with is: Is this really the best we can do? Can't we achieve collective ends without creating an overwhelming incentive to insulate market actors from the reach of collective-ends-governance?

Let me summarize the argument I've tried to make like this: I've offered three thoughts:
1) The United States has failed. It has failed because it has allowed the problem of concentrated power to arise, and has failed because is not going to address that problem anytime soon.

2) The EU has stepped in, and that, in principle, is a good thing, but

3) These interventions are going to press us towards a Web3 reality. The reason it will is that we lawyers have still not understood how code is law — in the sense that code can be better law, or better regulation, for those trying to assure their own business ends. Even if it is worse for the law, code can be better at regulating us, even if the way it regulates us is worse for the objectives of the law.

Thank you very much.

Q&A Session

Haluna Kawashima
Thank you very much, Lessig-san, for your very stimulating talk. One of the key points was the business model, and I would like to invite Professor Jiro Kokuryo to have a dialogue with you because Professor Kokuryo has recently published a new book on alternative business models.

Jiro Kokuryo
Professor, Faculty of Policy Management & Chief Administrator, CCRC, KGRI, Keio University
First, I'd like to, on behalf of everybody, including the people watching, thank you for your powerful talk. As usual, we've learned a lot from you. I just have a couple of very—not-so-simple questions that I'd like to ask you.

I think your point was very clear that what you think is the biggest issue is the business model that profits from brain hacking, if you will—if the expression is right. And you are saying that while the European interventions" for issues are a good attempt at addressing issues, perhaps it's not an adequate approach. What would be the adequate approach? I mean, how can we change the incentive structure so that the root cause can be addressed?

Lawrence Lessig
So that framing of the "root cause" is exactly the right framing. Henry David Thoreau famously wrote, "For every thousand hacking at the branches of evil, there's one striking at the root." And this is the root striker we have to find here. In the context of these brain hacking business models, again, I think that the objective should be to ask whether or not, in the particular context, the incentives of this business model are destructive of social values. And unlike most who critique surveillance capitalism, like Shoshana Zuboff, as I said, I'm actually not universally opposed to surveillance capitalism. I think in capitalism, the surveillance is fine so long as the data is not deployed in ways that are harmful to the individual.

So, if we regulated the use of data, the surveillance that produced that data would be okay. But in certain contexts, like news and politics, and when we know we are dealing with psychologically vulnerable people, the business model that profits from engagement is the problem. So, the root that we should be striking at here is the profitability of that business model.

Now, there are a lot of ways to regulate business models. We do it all the time. For example, the business model of burning coal to produce electricity is one we want to regulate. We don't like that way of producing electricity because it has externalities, and so the way we should be dealing with those externalities is by taxing carbon or taxing the deployment of coal. Those would be effective ways to shift electrical companies away from coal into alternative sources.

The same point is true here: we could be taxing a particular use of data, and if we taxed it smartly, we could make it so a company like Facebook wouldn't be making money by turning people into election deniers who believe that Donald Trump was elected. That use wouldn't pay. And that response, I think, is more likely to be effective than a response that stands back and says, "Oh, is this statement about what happened in the Pennsylvania elections true or false?" Or, "Is this statement about why white nationalism a good incendiary or not?" That approach at the level of the particular statements, I think, is hopeless and certain never to succeed. The only way to address it is to address the underlying cause of this pathology, which is AI trained on maximizing along a dimension that we should not be maximizing.

Jiro Kokuryo
Okay, thank you very much. We should continue thinking about effective ways of how to implement that. I agree with that. My second question is around your almost ambivalent comment on Web3. On the one hand, you seem to be saying, with your final comment, that code is actually the law. It is a powerful statement in that, in the end, we need, I mean, the Internet is connected globally, and any kind of regulation has to be coordinated globally, but we are doing a very bad job at doing that. But of course, the code approach is a very powerful way to implement a global law, but at the same time, you think it's a conspiracy.

Lawrence Lessig
Well, let me be clear about that. What I mean is nobody would think that the EU is actually eager to encourage an infrastructure that undermines its ability to regulate effectively, so why are they doing it? That's my question. And so, the American conspiracy theorist would say, "Oh, it's because there's some conspiracy here." Like they're pretending to be a regulator, but they're actually trying to undermine the power of regulation. But that's more of a joke. The more serious point is, "Why are you adopting strategies that you can see will have the effect of encouraging a push in a direction that will ultimately make it less plausible for governments and democracies to exercise their sovereign power here?" So, you are right to characterize my view here as ambivalent because, on the one hand, I think there are lots of great things in Web3. In particular, I think it's going to be extremely valuable for developing nations and places that don't already have institutions of trust that they can rely upon. This will be very valuable for their entering into a world market in lots of powerful and good ways.

But to the extent that it gets developed as a way to evade inefficient regulation, it's effect will just weaken sovereign authority. And I guess what frustrates me looking back over these 20 years of debates about the Internet is how slow people have been to recognize how they need to internalize the dynamic code will present here.

So, for example, you know this slogan, "Code is law," is wonderfully misinterpreted by all sorts of people "to mean there is no law there's only code." I didn't mean that by "Code is law." What I meant is we need to recognize the way code is operating as law and then decide as a

sovereign people whether we like the way it is operating or not. And if we don't like the legal effect of this code, we need to intervene, find a smart way to intervene, to ensure that it doesn't have that destructive effect. It's never about code alone. It's always about code as one modality of regulation. And the decision sovereigns have to make about whether they like that regulation or not.

I fear that Web3 is going to make it increasingly difficult for sovereigns to exercise their will in ways that might be good, depending on what the particular use is. I wish we just had regulators who were more reflective, recognizing the role of technology in their regulation. Again, you know my talk was very dismissive of lawyers, and I'm allowed to be because I am a lawyer. But what I find is lawyers are very bad at thinking about the technical implication of the interaction here. What we need is a conversation between technologists and lawyers, so the lawyers can propose, and the technologists can come back and say: "Here actually is the consequence of that way of regulating from a technical perspective. Just as we do that with economists. The lawyers propose, and the economists come back and say, "Here's the consequence if that economically." We ought to have the same analysis for technology.

Jiro Kokuryo
Thank you very much, as I'd like to continue this conversation. My staff is saying the time's up, so thank you. If I may advertise: the Keio Global Research Institute (KGRI) is trying to promote dialogue not just internationally but also between engineers and lawmakers—I'm a business major very much interested in the incentive structure kinds of things— so I thank you very much for adding a huge piece of knowledge with us. We'll continue talking, and very much looking forward to having you for another round of sessions. Thank you, professor.

Lawrence Lessig
Thank you very much.

<END>