RUTGERS LAW RECORD
The Digital Journal of Rutgers Law School
lawrecord.com
Volume 47 **2019-2020**

THE INTERNET OF THINGS – THE INTERNET OF THINGS OR OF HUMAN OBJECTS? MECHANIZING THE NEW SOCIAL ORDER

BRUNO ZELLER, LEON TRAKMAN AND ROBERT WALTERS[1]

Like the printed book, the Internet of Thing [IoT] has also changed the perception of reality and conceptions of social interaction. It has changed the levels of how information is perceived and viewed. For many people, it is the sharing of mostly personal information via social networks that extends from a personal face-to-face interaction to a global communication; a form of communication that is accessible to many in an instant and retransmitted to a global audience. With the speed and volume of transmission(s), the Internet has created a different social construction of reality and has assisted the spread of knowledge; however, it has also been the source of misinformation.

This article highlights and defines the multiple perceived realities by participants in the IoT. It explores the Internet as being a source of an inspiring knowledge revolution. However, it will also consider challenges to this notion. The article goes on to explore the responsibility of mega-corporations, which "control" access and channel information into mass consumer markets, their regulatory power to do so, and growing expectations for intervention by regulators. It juxtaposes the rationale that the IoT epitomizes a "free marketplace in ideas" and the argument that it is "free" to subjects whose personal data is distributed over a predominantly underregulated IoT.

[1] Bruno Zeller B. Com, B. Ed, Master of International Trade Law (Deakin), Ph.D (The University of Melbourne). Professor of Transnational Commercial Law, University of Western Australia. Adjunct Professor Murdoch University and Sir Zelman Cowen Centre, Victoria University, Melbourne
Leon Trakman B. Com, LLB (Cape Town); LLM, SJD (Harvard). UNSW Professor of Law and Former Dean, Faculty of Law, University of New South Wales, Sydney.
Robert Walters LLB (Victoria), MPPM (Monash), Ph.D Law (Victoria), Lecturer Victoria Law School, Victoria University, Melbourne, Adjunct Professor, European Faculty of Law, The New University, Slovenia, Europe

The central focus of the article is to address the tension between corporations' and data users' economic interest to secure access to personal data, and the right to legal protection of the subjects of that data. The hopeful, yet idealized, aspiration is to accentuate the need for society and in particular, legal regulators, to better comprehend the worrisome damage that arises from exposure of personal information over the Internet. This article proposes that democratic institutions assist in bridging the gap between the objectives of mega-data corporations and society's desire for ready Internet access without forfeiting their autonomy.

Table of Contents

1. Introduction

The world is again confronted with a significant challenge in transmitting, collecting and disseminating knowledge. This challenge is not new. It finds it's parallels in the 15th century when Gutenberg invented the printing press.[2] The printing press made it possible to print books faster than the old wooden blocks, decreased the prices for the European middle class, and provided the text in their own language as well.[3] Hence, knowledge spread more rapidly across Europe, as information could be transmitted, collected and importantly, disseminated through the then innovation medium of the printing press.[4] This development was arguably instrumental in the realization of the Renaissance, Reformation, Age of Enlightenment, and Scientific Revolution in Europe.[5]

History has demonstrated that, while social organizations are a product of human activity, how they function, and change is constant in nature yet variable in operation.[6] As Berger and Luckman note, "[A]ll socially constructed universes change, and the change is brought about by the concrete actions of human beings."[7]

The IoT in the Age of Digitalization has undoubtedly changed the reality of everyday life.[8] It has challenged the scope of an idealized global free market economy.[9] The IoT has underscored the commercial value of individuals' personal information to data surveillance corporations like Facebook and Google, and its social importance and perceived value to end user-data consumers.[10] The IoT has also demonstrated the vulnerability of data subjects, whose personal data is exposed over the internet

---

[2] *See* DIANA CHILDRESS, JOHANNES GUTENBERG AND THE PRINTING PRESS 1-29 (Twenty-First Century Books 2008).
[3] *Printing Press*, HISTORY (Oct. 10, 2019), https://www.history.com/topics/inventions/printing-press.
[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] *See* PETER L. BERGER & THOMAS LUCKMANN, THE SOCIAL CONSTRUCTION OF REALITY 134 (Penguin Books 1966).
[8] Pascal Brier, *The Digital Shift Has Happened: A Transformation in Three Dimensions*, ALTRAN, https://www.altran.com/as-content/uploads/sites/8/2018/09/brochurea5_digitaltransformation_web-1.pdf (last visited Dec. 28, 2019).
[9] *Id.*
[10] *Id.*

and who are themselves subject to manipulation based on that data.[11] This manipulation is most evident by mega-data corporations, such as Facebook, providing the data of millions of users to Cambridge Analytica for deployment to influence voters in the 2016 US Presidential Elections and the UK referendum on Brexit.[12] This abuse of personal data is accentuated by the fact that data has increasingly become the most valuable resource, globally.[13]

The tension between the economic interests of surveillance corporations in accessing personal data and protecting the personal information of the subjects of that data on the IoT has not gone unnoticed. The full text of the G20 leaders meeting in Japan in July 2019 explicitly recognizes this transcendent and global challenge:

> Cross-border flow of data, information, ideas and knowledge generates higher productivity, greater innovation, and improved sustainable development, while raising challenges related to privacy, data protection, intellectual property rights, and security. By continuing to address these challenges, we can further facilitate data free flow and strengthen consumer and business trust. In this respect, it is necessary that legal frameworks, both domestic and international, should be respected. [14]

These challenges of unchecked data flow across national borders are not wholly unique. Their antecedence traces back to the trade in goods and services within and among geographically diffused communities. Recording responses to these challenges was a self-ordered medieval Law Merchant, loosely identified with today's self-ordered internet.[15] Similar to data surveillance corporations seeking to trade across national boundaries and avoid local regulators, their purpose was to facilitate merchant trade beyond the restrictions of local princes.[16] The Law Merchant relied on merchants to self-regulate the sales of goods and services at fairs, guilds and markets in the then known world, not unlike

---

[11] *See generally* Carsten Maple, *Security and Privacy in the Internet of Things*, 2 J. CYBER POL'Y 155 (2017).
[12] *Id.*
[13] *The world's most valuable resource is no longer oil, but data*, THE ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.
[14] *Full Text of the G20 Osaka Leaders' Declaration*, THE JAPAN TIMES (Jun. 29, 2019), https://www.japantimes.co.jp/news/2019/06/29/national/full-text-g20-osaka-leaders-declaration/#.XhX-I5NKg_W.
[15] Leon E. Trakman, *From the Medieval Law Merchant to E-Merchant Law*, 53 UNIV. OF TORONTO L. J. 265 (2003) [hereinafter Trakman, *From the Medieval Law*].
[16] *Id.*

Facebook and Google regulating the trade in data in freely operating markets across a far wider world today.[17] Hence, parallels can be drawn between the medieval commerce conducted at cosmopolitan markets and "21st Century e-commerce Law Merchant" conducted on Internet platforms.[18] Disparities in knowledge among merchant sellers and buyers, is similar to disparities in understanding among data providers and their data users.[19] Typically, medieval customers who could not read or write in Latin were forced to rely on more knowledgeable suppliers to explain the alleged attributes of those goods and services. Just as data users rely on data corporations to treat them fairly and provide just data services, these disadvantaged buyers relied on merchant sellers to provide services equally and fairly (*ex aequo et bono*) at a fair or "just price."[20] Medieval customers also relied on "learned ones", notably in the Church, to advise them on unfair consumer transactions.[21] Similarly, data subjects rely on consumer websites and blogs to advise them about the unfair practices adopted by data surveillance entities, miners and hackers.[22]

Finally, the methods of dispute resolution and avoidance in the medieval and in the "now" data Law Merchant have comparable attributes.[23] Just as medieval merchant judges sought to resolve disputes between merchant traders, buyers and sellers, the judicial system is used by data subjects

---

[17] ANA M. LOPEZ-RODRIGUEZ, LEX MERCATORIA AND HARMONISATION OF CONTRACT LAW IN THE E.U. 87 (Djoef Publ'g 2003) ("For several hundred years uniform rules of law, those of the law merchant, were applied throughout the market tribunals of the various European trade centers." (footnote omitted)); Leon E. Trakman, *The Evolution of the Law Merchant: Our Commercial Heritage*, 12 J. MAR. L. & COM. 1, 5 (1980) ("The only law which could effectively enhance the activities of merchants [was] . . . suppletive law, i.e., law which recognized the capacity of merchants to regulate their own affairs through their customs, their usages, and their practices.") [hereinafter Trakman, *The Evolution*].

[18] Trakman, *From the Medieval Law*, *supra* note 15; Harold J. Berman & Felix J. Dasser, *The "New" Law Merchant and the "Old": Sources, Content, and Legitimacy*, *in* LEX MERCATORIA AND ARBITRATION 21, 61 (Thomas E. Carbonneau ed., 1990); Lawrence M. Friedman, *Erewhon: The Coming Global Legal Order*, 37 Stan. J. Int'l L. 347, 356 (2001) (ascribing the origins of the modern lex mercatoria to the customs of medieval merchants); Ralf Michaels, *The True Lex Mercatoria: Law Beyond the State*, 14 IND. J. GLOBAL LEGAL STUD. 447 (2007) (identifying the Law Merchant as "truly" transnational law operating beyond the nation state).

[19] ROBERT LOPEZ, THE COMMERCIAL REVOLUTION OF THE MIDDLE AGES (Cambridge U. Press 1976) (analyzing the Law Merchant's transnational identity).

[20] *See* Leon Trakman, *Ex Aequo et Bono: Demystifying an Ancient Concept,* 8 CHI. J. INT'L. L. 621, 642 (2008) [hereinafter Trakman, *Ex Aequo*].

[21] *See* LOPEZ-RODRIGUEZ, *supra* note 17, at 87; Trakman, *The Evolution*, supra note 17, at 11-15.

[22] *See* Zack Whittaker, *Online security 101: Tips for protecting your privacy from hackers and spies*, ZDNET (Sept. 11, 2018, 9:18 AM), https://www.zdnet.com/article/simple-security-step-by-step-guide/.

[23] *See* Trakman, *Ex Aequo*, *supra* note 20, at 629.

bringing class actions against providers who hold, sell or otherwise use personal information. Such modern disputes over the collection, sale and use of data is illustrated by the 2018 class action lawsuit brought against Facebook and Cambridge Analytica, in which users alleged that the companies engaged in the illegal use of the personal data of over 30 million US citizens.[24] The international nature of the internet has also increased the likelihood that data disputes relating to contract and intellectual property rights will be exposed to international commercial arbitration,[25] and tort rights to international commercial arbitration, between data collectors, miners and processors on the one hand and data users on the other.[26]

Part 2 will explore the tension between the economic interests of data collectors and processors to the interest of Internet users in protecting their personal information. It will also examine the schism between the public interest in the free flow of data and the protection of privacy rights. Part 3 will conceptualize the "new reality" associated with the IoT and present insights into its construction and application across a digitalized society. Part 4 will address the expansion of this new reality, including the collection and processing of personal data and the use of that data to manipulate the subjects of that data, such as influencing voting patterns. Part 5 will analyze the function of governmental regulators in institutionalizing this new reality. Part 6 with evaluate the relationship between data protection and anti-competitive conduct. Part 7 will discuss the conception of surveillance capitalism and its application to personal data. Part 8 will propose a plan to balance vitality self-regulatory capacity of the IoT, contrasted against the growing need to maintain the security of the billions of persons who function within a global data community. Part 9 will evaluate the potential to

---

[24] *See* Owen Bowcott & Alex Hern, *Facebook and Cambridge Analytica face class action lawsuit,* THE GUARDIAN (Apr. 10, 2018, 11:45 AM), https://www.theguardian.com/news/2018/apr/10/cambridge-analytica-and-facebook-face-class-action-lawsuit.

[25] *See* Leon Trakman et al., *International Arbitration in Data Protection and Privacy Law – is it Relevant?,* TRANSNATIONAL DISPUTE MANAGEMENT (forthcoming 2019).

[26] *See* Paul M. Schwartz & Daniel J. Solove, *Reworking Information Privacy Law: A Memorandum regarding Future ALI Projects about Information Privacy Law*, DUKE L. (2012), https://law.duke.edu/sites/default/files /images/centers/judicialstudies/Reworking_Info_Privacy_Law.pdf.

internalize the IoT to include the data users as subjects rather than objects of it. Part 10 will conclude by reflecting on the pathway ahead of the IoT for data surveillance entities, those are who are subject to such surveillance, and those who regulate that surveillance.

2. Public Access to Data versus Data Privacy

The IoT has changed the perception of what is disseminated publicly. As a result, it has created expectations of users of the multi-faceted information which is available on the Net. This has led to divergence over the reality expected by its multilayered users. The most obvious discord is observable in relation to personal data that is uploaded onto the IoT. Corporations, such as Facebook and Google, have learned that this information is valuable because it is sellable; however, personal data subjects would prefer to keep this information private and protected.[27] This has led to a contest over the ownership and control of such data. Data corporations that are experts in capturing information on the Net, have claimed the novel status of ownership over information as a merchantable object. Consequentially, they have claimed "ultimate jurisdiction over that stock of knowledge in its totality."[28]

Their assertion is increasingly disputed. Lawrence Trautman describes the mission of tech-giants as "to give people the power to build community and bring the world closer together."[29] He notes, in support of this contention, Facebook's assertion that, "[our] top priority is to build useful and engaging products that enable people to connect and share with friends and family through mobile devices, personal computers, and other surfaces."[30] However, the new reality is that, in building "useful and engaging products," Facebook also controls both the product and its content.

---

[27] *Aimee Picchi, Facebook: Your personal info for sale*, CBS NEWS (March 21, 2018, 12:04 PM), https://www.cbsnews.com/news/facebook-your-personal-info-for-sale/.
[28] CHILDRESS, *supra* note 2, at 125.
[29] *See* Lawrence J. Trautman, *Governance of the Facebook Privacy Crisis* 1, 9 (Mar. 31, 2019) (unpublished manuscript) (citing Form 10-K (Annual Report) for Facebook, Inc., for the fiscal year ended Dec. 31, 2017, https://www.sec.gov/Archives/edgar/data/1326801/000132680118000009/fb-12312017x10k.htm) [hereinafter Trautman, *Governance*].
[30] *See* Trautman, *Governance*, *supra* note 29.

The unfortunate result of such control by mega-corporations is that a dark side has emerged, namely, a conflict between privacy and the desire for profit-making by companies like Facebook and Google. Zuboff termed these new phenomena as arising from the *Age of Surveillance Capitalism*:

> Total information tends toward certainty and the promise of guaranteed outcomes. These operations mean that the supply and demand of behavioral futures markets are rendered in infinite detail. Surveillance capitalism thus replaces mystery with certainty as it substitutes rendition, behavioral modification, and prediction for the old 'unsurveyable pattern.[31]

A tension exists between the profit making/securitization of commerce and the autonomy/privacy of the data subject. Albrecht has aptly observed that "[i]f data is the new oil, then data protection is the new environmental protection."[32]

This tension is accentuated by the fact that "the digital realm is overtaking and redefining everything familiar, even before we had a chance to ponder and decide."[33] One problem that results is a conflict between the right to collect and transmit data and data subjects not wishing their personal data to be shared with others on the IoT. Another tension exists between data collectors and subjects on one side and on the other, third-party users such as miners and hackers who access personal data for profit, pleasure, victimization, vindication, or some combination of these motivations.[34] The resulting tension within this new reality is not only between corporations that profit from the use of data and the subjects of that data. It is also between the downstream users of personal data. Not only do corporations want access to that data, but so do those users.

A consequential attribute of the new reality is the "knowledge gap" between vulnerable data subjects, whose personal data is made available on the net on the one hand, and data surveillance

---

[31] *See* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 497 (2019).
[32] DEMOCRACY: IM RAUSCH DER DATEN (Indi Film Produktion 2015) (referencing Jan Philipp Albrecht, the rapporteur to the EU Parliament in the legislative procedure for the EU General Data Protection Regulation).
[33] ZUBOFF, *supra* note 31, at 497.
[34] *See generally* Richard L. Pell, *Third-Party Data Collection and Consent in Mobile Applications*, LEXOLOGY, https://www.lexology.com/library/detail.aspx?g=5ed6a338-f459-4480-b82a-c5f37db27ab3 (last visited Oct. 14, 2019).

miners, hackers and other users on the other hand.[35] The knowledge gap is that most data subjects are not able to understand how their personal data is accessed and used in a complex technological world.[36] This "knowledge gap" is not unlike the imbalance between those who could not read in the Middle Ages and relied on others like Church pastors to do so for them. Surveillance corporations like Facebook purport to bridge this knowledge gap by claiming to protect their data platforms from attack in order to protect their users, data subjects, from victimization.[37] Whether data surveillance capitalists, so named by their critics, seek to protect themselves at the expense of the subjects of their data is hotly contested.[38] Whatever view is adopted, data surveillance corporations like Facebook and other tech-gaints are not immune from unauthorized access to user's personal data.[39] Facebook warned that "security breaches and improper access to or disclosure of our [Facebook's] data or users' data, or other hacking and phishing attacks on our systems, could harm our reputation and adversely affect our business."[40] Accordingly, Facebook warned, in the alleged public interest:

> Our industry is prone to cyber-attacks by third parties seeking unauthorized access to our data or users' data or to disrupt our ability to provide service. Any failure to prevent or mitigate security breaches and improper access to or disclosure of our data or user data, including personal information, content or payment information from users, could result in the loss or misuse of such data, which could harm our business and reputation and diminish our competitive position. In addition, computer malware, viruses, social engineering (predominantly spear phishing attacks), and general hacking have become more prevalent in our industry, have occurred on our systems in the past, and will occur on our systems in the future. We also regularly encounter attempts to create false or undesirable user accounts, purchase ads, or take other actions on our platform for purposes such as spamming, spreading misinformation, or other objectionable ends. As a result of our prominence, the size of our user base, and the types and volume of personal data on our systems, we believe that we are a particularly attractive target for such breaches and attacks. Such attacks may cause interruptions to the services we

---

[35] *See* Michael A. Cacciatore et al., *Another (Methodological) Look at Knowledge Gaps and the Internet's Potential for Closing them,* 23 PUB. UNDERSTANDING SCI. 367, 367-377 (2014).
[36] *Id.*
[37] *Facebook's Privacy Principles,* FACEBOOK, https://www.facebook.com/about/basics/privacy-principles (last visited Dec. 21, 2019).
[38] See Lawrence J. Trautman & Peter C. Ormerod, *Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things*, 72 U. MIAMI L. REV. 761 (2018); Lawrence J. Trautman, *Managing Cyberthreat,* 33(2) SANTA CLARA COMPUTER & HIGH TECH. L.J. 230 (2017).
[39] Facebook, Inc., Annual Report (Form 10-K), at 14 (Jan. 31, 2019).
[40] *Id.*

> provide, degrade the user experience, cause users to lose confidence and trust in our products, impair our internal systems, or result in financial harm to us.[41]

Generally, Facebook's emphasis on its global stature and need to protect data consumers is, arguably, self-serving and does very little to balance the need of users with Facebook's business plan. However, its stress on the vulnerability of the net to security violations is also a credible part of a new reality. "Hackers" have evolved into sophisticated market players who profit from securing and selling data, not least of all to competitor data providers.

However, the devastating effect of data surveillance, at least initially, rests centrally with mega-data corporations. The social harm of the "instagramification" of data by data surveillance corporations, is a reduction in the attention span of the most vulnerable data users—children.[42] Studies provide evidence that the cycle of instant access and reaction to data encourages reflexive rather than reflective action by data users who respond to data barrages beyond their comprehension, which both mechanizes and diminishes their social interactions.[43] An example of the continuing reduction of real-life social interaction is the ease with which data users can upload videos of other people's real life experiences on YouTube. This new access to a social media looking glass is comparable to a supermarket tour in which shoppers wander through the supermarket looking at what is on sale. As freelance journalist Arian Lobe comments, this isolating practice depicts a digital society in which online users, arguably considered junkies, look at anything that is available on the net, irrespective of whether that online information has any social value other than acting as a looking glass.[44] At work is

---

[41] *Id.*
[42] *See* Mark Bridge, *Our Instagram Society Could Alter Children's Brain, Scientists Warn,* THE TIMES (June 7, 2019, 12:01 AM), https://www.thetimes.co.uk/article/our-instagram-society-could-alter-children-s-brains-warn-scientists-dhcfvrs22.
[43] *See* Neue Zurcher Zeitung, e-Paper (June 25, 2019), https://epaper.nzz.ch/; FEUILLETON, REVUE FEUILLETON 17 (June 16, 2016).
[44] *See* Arian Lobe, *Teleshopping 2.0: What's Nicer Than Shopping? Watch[ing] others shopping*, NEUE ZÜRCHER ZEITUNG (June 24, 2019), https://www.nzz.ch/feuilleton/teleshopping-20-nix-kaufen-nur-schauen-auf-youtube-ld.1489560.

the new and sometimes unduly protracted activity of teleshopping without any real and pervasive purpose.[45]

The worrisome new reality is that the IoT is not only a place of study and learning, but also a place in which anything, even trivial information, can be uploaded and fed to billions of users across a net-fixated global community. In effect, the IoT has evolved into a pastime that is replacing, to some extent, meaningful social discussion and reflection. It is an experience in which the data user is obsessed with the IoT, not unlike a voyeur peering through the curtains to see what is going on in the next apartment.

Furthermore, the IoT is a two-way looking glass. Data surveillance corporations can devise the looking glass for data users, while scrutinizing the intensity of that look and manipulating user reactions to it. the supposed mutual benefit is that data users can view the picturesque scenes created by these corporations inside the curtains and/or window.[46] Surveillance corporations can harvest and use information culled from the nature of that inward look. The result of this two-way looking glass is that surveillance capitalists can maximize on a free market in data the determinative objective reality, subsuming the subjective reality of the individual data user. A related reality is that the looking glass allows others to troll the net in search of data about the surveillance capitalist in order to sell to those in the surveillance market, at the expense of the data providers.[47]

However, the mutually reinforcing free market surveillance of data and the consumption of that data is offset by the fact that data users conceive the free market in data quite differently.[48] On one side there is a demand by consumers to have "what I want, when, where, and how I want it;"[49] a

[45] *See id.*
[46] Olafer Eliasson, *2010: How Is The Internet Changing The Way You Think*, EDGE, https://www.edge.org/response-detail/10373 (last visited Dec. 10, 2019).
[47] ZUBOFF, *supra* note 31.
[48] *Id.*
[49] *See id.*, at 39.

demand surveillance capitalists are pleased to satisfy. Conversely, there is the desire of end users to either hijack the data provider, to misuse the personal information of data subjects, or both.[50] The critical issue is that surveillance capitalists seeking to objectify a free market which they largely control, disempowering a vulnerable data community, which sometimes includes themselves. The result of the deep socialization that comes from data surveillance is the need to establish the pathway to a new reality that redresses deficiencies in the current obstructed and obstructive data pathway.

The tension between the free market in personal data and protecting the data of those who are captive to that market is not unique. However, the challenge today transcends this unstable balance between a free and fair market in data. Nor is today's challenge over whether end users should forego their privacy in interacting with Google or Facebook. It is rather how end users, as human subjects, can coexist with the new reality of Facebook and Google that is unavoidably accompanied by some loss of privacy in exchange for a transformative and informative highway. Simply put, how can global society reconcile that the price of using the IoT is the human, and increasingly socialized, right to privacy? The response, this article proposes, is to investigate how to reconcile three perspectives on how to regulate the use of data. These perspectives include: the community of users whose personal is placed on the net; the extent to which data surveillance corporations, and some users, trade in that personal data; and how regulators can regulate that trade in data.

3. The "New Reality" of the Internet of Things

It is useful to briefly define what is meant by the Internet of Things (IoT), to assist in defining the new reality ascribed to a functional global internet. The International Telecommunication Union described the IoT as "a global infrastructure for the information society, enabling advanced services

[50] *See id.*

by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies."[51]

Based on this conception, one could assume that the IoT will enable speedy transmitting of information, not only between data surveillance corporations and end users, but also among those end users. This development is not unlike the Gutenberg print, in which books became accessible to the reading populace allowing scholars, such as Copernicus, to publish their studies allowing others to learn. However, the IoT has opened a complex new economic vista for data providers engaged in the global transmission of data. Zuboff aptly observes: that "[n]ew economic logics and their commercial models are discovered by people in a time and place and then perfected through trial and error."[52] Simply put, data providers like Google can progressively capture personal information that is placed on the net, including personal data.

An important distinction needs to be drawn between two realities occupied by consumers: face-to-face communication and instant access to data in a virtual world, absent of direct communicative discourse. One reality resides in consumers simply sharing information with one another. For example, a consumer asks a friend where they shop and why, while also providing information about those shopping experiences. Another is that consumers can share such information over the net. The result is that consumers can benefit from information provided to them through all channels of communication.

What has changed is the expanding content of personal data under surveillance over the net. This cause of such change is the practice by corporations – the inventors and owners of the net – to devise instruments that secretly control, trap, and record data, which rather than being shared, is used to change behavior. This new reality is growing, both perceptibly and precipitously.

---

[51] *Overview of the Internet of Things: Recommendation ITU-T Y.2060*, THE INT'L TELECOMM. UNION (June 15, 2012), https://www.itu.int/rec/T-REC-Y.2060-201206-I.
[52] ZUBOFF, *supra* note 31, at 497.

Once data is placed online, data subjects have hardly any control over the processing of their personal data. Data processors, in turn, render that denial of control permanent due to the ubiquitous character of the Internet and the lack of specific individual rights in relation to it.[53] However, this reality extends beyond the divide between dominant data processor and data subjects whom they subordinate. The new reality relates to an invasion into what might be called the "intimate personal space" of data subjects. That is the new battlefield in which the utility of internet regulation is being fought.

The new reality of personal invasion still encapsulates an old reality in some respects. The new power struggle between an open access internet and the protection of personal sensitive data is akin to the previous reality of a dominant employer taking advantage of dependent employees. The contest now is that surveillance capitalism is parasitic and self-referential, but not unlike an employer exploiting a mass of employees. However, the new reality does more than revive Karl Marx's old image of capitalism as a vampire that feeds on labor. Operating well beyond employers exploiting their employees, "surveillance capitalism through the internet feeds on every aspect of every human's experience."[54] Zuboff ominously observes:

> Surveillance capitalism operates through unprecedented asymmetries in knowledge and the power that accrues to knowledge. Surveillance capitalists know everything *about us,* whereas their operations are designed to be unknowable *to us*. They accumulate vast domains of new knowledge *from us,* but not *for us*. They predict our futures for the sake of others' gain, not ours. As long as surveillance capitalism and its behavioral futures markets are allowed to thrive, ownership of the new means of behavioral modification eclipse ownership of the means of production as the fountainhead of capitalist wealth and power in the twenty-first century.[55]

[53] *See* Mariusz Krzysztofek, *'The Right to be Forgotten' on a Swing,* 27 EUR. BUS. L. REV. 865, 865-866 (2016).
[54] ZUBOFF, *supra* note 31, at 9.
[55] ZUBOFF, *supra* note 31, at 11.

Critics of the growing dominance of surveillance capitalism, like Berger and Luckmann, prioritize the paramountcy of our personal lives: "[C]ompared to the reality of everyday life, other realities appear as finite provinces of meaning, enclaves within the paramount reality … and modes of experience."[56] In essence, we now operate on two levels of reality.[57] The first, is the reality of our own lives operating outside the internet.[58] The second reality is generated by the internet, without our shared understanding or full appreciation of the hidden power of the ubiquitous IoT.[59] The question is whether these two realities can coexist, or whether we are enslaved by an IoT that subordinates our own personal realities. The challenge is to determine and reconcile these conflicting realities. Berger and Luckmann, in their 1966 publication, "The Social Construction of Reality", explain their conception of the movement between these two realities as a "shock."[60] "As I move from one reality to another, I experience the transition as a kind of shock. This shock is to be understood as caused by the shift in attentiveness that the transition entail."[61] This shock, arguably today, is the current realization that our privacy is becoming the victim of technological machines that intrude upon every part of our personal lives. While data surveillance capitalism conceives of their technological machinery of as affirming our personal lives, critics view that machines as unremitting intrusions on human and social life.[62]

However, despite the separation between new technological modes of engagement and traditional norms and rules of communication, the common denominator is how the IoT interfaces with face-to-face communication. Both methods of communication are still at the core reality of

---

[56] BERGER & LUCKMANN, *supra* note 7, at 39.
[57] *Id.* at 35.
[58] *Id.*
[59] Shanyang Zhao, *The Internet and the Transformation of the Reality of Everyday Life: Toward a New Analytic Stance in Sociology*, 76 SOC. INQUIRY 458, 469-70 (2006).
[60] BERGER & LUCKMANN, *supra* note 7, at 115.
[61] *Id.* at 35.
[62] Shoshana Zuboff, *Big other: surveillance capitalism and the prospects of an information civilization*, 30 J. OF INFO. TECH. 75, 76 (2015) [hereinafter Zuboff, *Big other*].

everyday life that are shared, willingly or otherwise, by protagonists and antagonists of the technological machines that influence the quality of that life.[63] Berger and Luckmann use the analogy of the rising and falling of a curtain to denote how a person is "transported" from one world to another.

> As the curtain rises, the spectator is 'transported to another world', with its own meaning and an order that may or may not have much to do with the order of everyday life. As the curtain falls, the spectator 'returns to reality', that is, to the paramount reality of everyday life by comparison with which the reality presented on the stage now appears tenuous and ephemeral, however vivid the presentation may have been a few moments previously.[64]

This transportation across worlds is perhaps too stark. The new reality arises, not by a new world order replacing an old one, but by the transition of changes in communication, sometimes radical in nature, across a spectrum of reality.[65] That changing spectrum is reflected in transitioning from face-to-face only communication, to the incremental inception of published books to newspapers, to the World Wide Web of online data, and surveillance directing the everyday life of data users.

The issue, then, is to evaluate the evolving reality of everyday lives. That reality extends beyond Berger and Luckmann's order of reality of the replacement of an old with new order of communication. At the same time, the transitioning of that reality is less than a protracted shift in modes of communication and more than a fleetingly transformation to a new order connected to the IoT. The reality, therefore, is that there is not only one curtain in the world of the IoT, as there are many actors who adopt their own variants of reality. It is this multiple reality of life which needs defining, as surveillance capitalists, regulators and individuals in society see the reality of everyday life differently, exacerbated by chasms in defining the reality of life ascribed to the IoT.

---

[63] *Id.*
[64] BERGER & LUCKMANN, *supra* note 7, at 39.
[65] *See* Zhao, *supra* note 59, at 458.

4. Addressing the new Reality

The new reality in the IoT is associated with its pervasive impact upon everyday life in which the internet is used, but differently.[66] The issue is that "everyday life is divided into sectors that are apprehended routinely, and others that present me with problems of one kind or another."[67] The argument of instant transition is that, as soon as individuals engage with the IoT, they are subordinated to the rules of its technological "machinery" or to the lack of such rules. The problem is in how this transitioning reality is absorbed into everyday life. Many people absorb that reality by rendering it into part of their personal identities, while diverging on how they do so.

This transition in personal identity does raise deleterious social and attendant legal responses, beyond divergences in our individuated endorsement of the expanding surveillance of our everyday lives. That deleteriousness includes the social realization that the data subject's propertied right to retain the confidentiality of personal data has increasingly become a casualty in the accessibility, of personal information to the public domain. The result is that private data is subjugated, ever more invasively and pervasively, through surveillance over the IoT.[68] That invasive and pervasive reality is building an ever deepening and disturbing divide between the provision of, and access to, personal data and the use and abuse of that data. The proposition is not that the personal information of data users is equally accessible to data surveillance corporations. The divide between access to and the abuse of personal data is contextualized differently, including by data users, based on their different knowledge bases, and understanding of Internet access, data use, and threats to their data privacy. The drivers are also influenced by the ideological and economic proclivities of surveillance capitalists that

[66] *See id.* at 469-70.
[67] BERGER & LUCKMANN, *supra* note 7, at 37.
[68] ZUBOFF, *Big Other*, *supra* note 62, at 76.

are associated with "free" more than "fair" market rationalizations. And it is exactly in addressing divergence over the nature and limits of these normative factors with which privacy laws are grappling. For Zuboff, these contextual differences are unexceptional:

> [T]here is nothing unusual about the prospect of capitalist enterprises seeking every kind of knowledge advantage in a competitive marketplace, the surveillance capitalist capabilities that translate ignorance into knowledge are unprecedented… surveillance capital derives from the dispossession of human experience, operationalized in its unilateral and pervasive programs of rendition: our lives are scrapped and sold to fund their freedom and our subjugation, their knowledge and our ignorance about what they know.[69]

The problem is that the reality of the IoT is viewed differently by those who regulate it, use it and multinational companies like Facebook and Google that materially control it. The real issue, as Zuboff sees it, is that:

> the cards have been reshuffled; the rules of the game have been transformed into something that is both unprecedented and unimaginable outside the digital milieu and the vast resources of wealth and scientific prowess that the new applied utopianists bring to the table.[70]

However, today's functional reality was not an instant or complete transformation from a competitive market to a digital society that subjects human subjects to the un-precedented digitalization of their personal identities.[71] Consumers have long functioned within uncompetitive markets dominated by large-scale corporations, well before the entry of Google and Facebook into global markets.[72] What is supportable is that, before the advent of the net, the "most important experience of others takes place in the face-to-face situation, which is the prototypical case of social interaction."[73] The prototypical case of social interaction through the IoT does diverge physically

---

[69] ZUBOFF, *supra* note 31, at 498.
[70] *Id.* at 499.
[71] *Id.*
[72] Lina Kahn & Sandeep Vaheesan, *How American became uncompetitive and unequal*, WASH. POST (June 13, 2014), https://www.washingtonpost.com/opinions/how-america-became-uncompetitive-and-unequal/2014/06/13/a690ad94-ec00-11e3-b98c-72cef4a00499_story.html.
[73] CHILDRESS, *supra* note 2, at 43.

from face-to-face communication.[74] Social interaction after the IoT takes place in front of a screen, through "machine communications" that are controlled by the IoT.[75] In both face-to-face and machine communication, the underlying rationale is the same, to facilitate interaction.[76] However, the nature of social interaction has changed radically.[77]

We have moved perceptibly, but not exhaustively, away from a two-way face-to-face meeting to interacting with the mechanical world in which the devices of mega-corporations like Facebook are linked, not to the reality of one individual, but to many different realities in any given society.[78] This new reality involves a passive remote connectedness between data controllers and data subject. Interaction within the IoT is significantly controlled by mega-data corporations that create and run online platforms, as the very means of interaction over the net. These platform creators are also the real data regulators, in which companies like Goggle, not government regulators, run the data media. The further reality is that governments are reluctant to provide comprehensive "guidance" on the scope of data protection in a global setting in which trade in goods and services is dominated primarily by a corporatized, not a socialized, data market.[79]

However, there are shifts in both the free market ideology and human rights foundations of data protection. These shifts are also clear evidence of changing perceptions, not only subjectively in the perspectives of individual consumers, but also within the objective reality of societies that prioritize unchecked exposure to the internet. Still, the prioritization is never static. Nor is it insulated from public opinion over when the IoT intrudes on the quality of personal life.

---

[74] *See id.*
[75] *See id.*
[76] *See id.*
[77] *See id.*
[78] *See id.*; *See also* AJ Agrawal, *Millennials Are Struggling With Face to Face Communication: Here's Why*, FORBES (May 4, 2017 7:24 PM), https://www.forbes.com/sites/ajagrawal /2017/05/04/millennials-are-struggling-with-face-to-face-communication-heres-why/#111b25bc26e8.
[79] *See* ROBERT WALTERS ET AL., DATA PROTECTION LAW: A COMPARATIVE ANALYSIS OF ASIA-PACIFIC AND EUROPEAN APPROACHES (Springer ed. 2019).

However, despite these shifts in reality, it is the personal data that lies at the keystone of all internet activities and within the contemplation of data providers and less evidently, government regulators and data users. Without access to personal data, surveillance capitalism would be starved of the very essence of its being, namely, the access to data expressing the everyday life of individuals.[80] It is in reaction to that reality that governments, along with society as a whole, are struggling to address, and also redress.

The underlying contest is between protecting data access without wholly disregarding data protection. It is a contest inhering in the tug of war between a liberal and social democracy. What has changed are perceptions of that which is real about the evolving IoT, and how that reality diverges from past realities. One intensifying reality is the proposition that communication between consumers of information is only real in a face-to-face situation, but as soon as that communication becomes anonymous over the IoT, the reality of that face-to-face communication retreats.[81] What dissipates is:

> the anonymity of the typifications by means of which I apprehend fellowmen in face to face situations [which] is constantly 'filled in' by the multiplicity of vivid symptoms referring to a concrete human being.[82]

However, the transition in reality in moving significantly away from the face-to-face communications between "fellowmen" to internet communication directed by internet providers to users on masse.[83] What has changed is that the communication is less between users than between the IoT and a mass of users which dominates daily life. What has also changed is that the contemporaries directing the communication are not fellowmen anymore; they are the IoT, or what

[80] John Naughton, *'The goal is to automate us': welcome to the age of surveillance capitalism*, THE GUARDIAN (Jan. 20, 2019 2:00 AM), https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook.
[81] WALTERS ET AL., *supra* note 79, at 47.
[82] BERGER & LUCKMANN, *supra* note 7, at 47.
[83] WALTERS ET AL., *supra* note 79, at 47.

might be termed 'public opinions' generated by the IoT which influences the reality of everyday life.[84] The threat to social engagement does not stem from the shift to communication between people and machines. The threat is rather that the conversation is directed away from people conversing to internet machines spewing out information about everyone and anyone's information that happens to be on the net. What the evolving IoT has undermined is that "social structure is the essential element of the reality of everyday life."[85] It is that structure involving participants in everyday life that needs to be revitalized in the face of the anonymity of surveillance capitalism that directs traffic in personal data over the Internet.[86]

Centrally in issue is the capability of the IoT to maximize upon the effects of habituation in which the repetition of activities is constituted into a pattern "which can then be reproduced with an economy of effort."[87] The IoT is the perfect tool to make repetition into a pattern, to entrench it as a habit, and to use it as an instrument which shapes the reality of everyday life. Moreover, as a habit, it provides a direction and hence minimizes the specificity of decision making. As such, the machine formulated patterns of the IoT replace, to a great extent, the face-to-face patterns that formulate the personalized realities of everyone's life.

The problem is that habituation which is driven by innovation and human activities precedes the institutionalization of those repetitive patterns. The result is that habituation requires ensuing direction which is facilitated by rules and regulations of the guiding or directing institution. As the innovation, in this case the IoT, always precedes the protection and order which is formulated by law, these regulatory institutions always postdate that innovation: hence the variable movement from the habituation of repetitive patterns to legal institutionalization requires a change in reality in all levels of

---

[84] *See id.*
[85] *Id.*, at 48.
[86] *See id.*.
[87] *Id.* at 71.

society, from surveillance capitalists, to data users, to the regulatory state. The attendant reality is that the social order as we know it today is still in the process of construction. As a result, if regulators are to prevent that process of construction from evolving into a permanent and irreversible reality, a responsive institutional order. If regulators are to encompass data users as determinants, rather than supplicants, of the social order in virtual reality, there is need for regulatory action at the earliest time. Berger and Luckmann have recognized that an inclusive social order, namely one that includes human subjects, already exists in both objective and subjective reality.[88]

The IoT has not changed this fact; and every individual in society "simultaneously externalizes his own being into a social world and internalizes it as an objective reality."[89] Alternatively conceived, objective reality eventuates when all participants in the virtual "social world" will have realized the ability of the IoT to connect, that is, to create a social network.[90] At the same time, it is necessary to understand the obstacles in attaining this interconnected social world. The reality of the net is that information sharing takes place on a far wider scale than ever before, such as being a "follower" of a message which can attract thousands of followers - a phenomenon not experienced before the IoT.[91] This objective reality of the net has become a subjective event as the technology driving the IoT has been internalized into becoming the reality of everyday life. This internalized reality is best expressed by the observation that two or more people are often far more engrossed in looking at their mobile phones, rather than engaging in face to face conversation. In effect, society has accepted the IoT as creating a new reality in which individuals can enjoy effective and meaningful personal lives outside the framework of face-to-face interaction.

---

[88] BERGER & LUCKMANN, *supra* note 7, at 149.
[89] *Id.*
[90] *See id.*
[91] *See id.*

However, there are still areas in which the reality of the individual, the surveillance capitalist, and the regulators of that surveillance diverge materially: hence, the reality of everyday life is not yet adequately defined. In issue is the scope the protection accorded to personal data on the IoT. The starting point is to delineate the reality of everyday life based on the level of protection which governments and regulators have introduced in order to protect personal data; and the adequacy of that protection.

5. The regulators and the objective Reality

Governments as regulatory institutions are captive to two realties; a society that is impacted by access to data and those who provide that access. The pressure which these two constituencies exert on the institutions of government is, by definition, the impetus in creating the reality of regulation as constructed by governments. Consequently, government regulators do not create the reality through which to direct their interrelationship with the environment which they regulate. They rely rather on social and corporatized patterns of conduct, such as relate to an IoT, upon which to frame their regulating institutions. As such, institutional regulation is unlike the world of reality experienced by the individual within a given society. This is so because the regulatory institutions of government exist only as a consequence of the reality as perceived by those parts of society that exert pressure on governments to expand, limit, or simply change, the regulatory structure. Hence, government regulation works on a reality of compromise in which shifting patterns of behavior by governments respond to changing patterns of corporate and social behavior.

As an example, data companies that are dissatisfied with the options and sanctions imposed by regulatory institutions tend to attempt to immunize themselves from those institutions they perceive as interfering with their business models. A response is that the creation of a guiding reality for government regulation does not apply to only one participant in the relationship between

government and data companies, but to all participants in society who interact on the net. The purpose is to render the relationship between data companies and human participants impartial, that is, without favoritism accorded to some only. The purpose therefore is not to protect only highly vulnerable data subjects, nor those who are most aggressive in representing their own interests. It is to protect data users in general from having personal data exposed to public scrutiny without their consent.

A central consideration remains over the extent to which regulators ought to rely on patterns of conduct among surveillance corporations and data users, and how regulators ought to reorder those patterns. In issue is whether habituation drives the institutions by which governments regulate data corporations and their customer, or whether government institutions create, direct and hence reconstitute the boundaries of such habituation. Berger and Luckmann describe the nature and function of an institution that controls human conduct, not limited to government institutions, in this way:

> Institutions by the very fact of their existence control human conduct by setting up predefined patterns of conduct, which channel it in one direction as against the many other directions that could theoretically be possible. It is important to stress that this controlling character is inherent in institutionalization as such, prior to or apart from any mechanisms of sanctions specifically set up to support an institution.[92]

Berger and Luckmann's view is that institutions assume responsibility for "setting up predefined patterns of conduct."[93] In that regard, these institutions establish the direction of further habituation, rather than the contrary. While Berger and Luckmann do not deny that patterns of conduct among those engaged in such conduct influence institutional regulation, they attribute a controlling function to governing institutions.[94] The result is that institutional regulators are also the source of "mechanisms" that sanction patterns of conduct that diverge from such institutionalization.

---

[92] BERGER & LUCKMANN, *supra* note 7, at 72.
[93] *Id.* at 72.
[94] *Id.*

Berger and Luckmann's views ought, nevertheless, be subject to important qualifications. Institutional regulators act, not only reactively in response to patterns of behavior of data surveillance corporations. Regulators also act, at least in part, proactively in imposing institutional constrained based on pre-set ideological preferences, such as according to a spectrum of both free and fair market values. Both proactive and reactive constituents of institutionalization therefore contribute to the regulatory framework, whether systemically, incrementally, and sometimes inconsistently.

The harmony ~~mediation~~ between Berger and Luckmann's view and our view of institutionalized regulation lies in the shared proposition: that patterns of conduct in society may well precede institutionalized regulation; however, government regulators select among legally permissible and impermissible patterns of conduct according to their preferred construction of those patterns.[95] Applied functionally to the IoT, patterns of conduct in disseminating information emerged at the outset in a largely unregulated information highway. However, that highway initially consisted primarily of the collection and display of whatever data was available for display over the then internet.

Since its inception, patterns of conduct on the net have changed, in the development of corporate surveillance and more recently, government action based on concern about its invasive use and impact on personal data.[96] The important current question, a means to identify the next stage along the spectrum of reality, is how government regulators, acting separately or together, will regulate the IoT in the immediate and intermediate future. How will they control patterns of corporate (and other) behavior deemed to exceed the free exchange of information, and the public's right to know? Subsumed within this question is the manner in which governments will regulate patterns of corporate behavior to protect personal data in particular. In issue will be the criteria governments employ to so decide, such as the nature and extent of the perceived data infraction and limitations in the capacity

[95] BERGER & LUCKMANN, *supra* note 7, at 72.
[96] *See id.*

of data users at large to scrutinize the nature infractions upon their personal data. Other important criteria for regulators in determining when and how to regulate measures adopted by data surveillance capitalists, including their regulatory costs in requiring them to remediate their surveillance measures, the social impact of such regulatory measures, and their effectiveness in sanctioning socially deleterious patterns of surveillance of personal data.[97]

These issues are central to the EU in promulgating its 2018 General Data Protection Regulation **(**GDPR). The key purpose of the GDPR regulations is to protect individuals from the abuse of their personal data which is, detrimental to their levels of comfort with their present reality. Krzysztofek has recognized this new reality created by the IoT, by stating that "data subjects have hardly any control over processing activities of their personal data anymore, once they are online due to the ubiquitous character of the Internet and the lack of specific individual rights."[98]

Responding to this new reality was something that the European Commission ("Commission") had been seeking to address since 2012.[99] Its added incentive was to make Europe "fit for the digital age", in addition to enabling data subjects regain control of their personal data.[100] The further impetus for the GDPR was the realization that state, acting individually or collectively as institutions, faces the stark reality that self-regulation of the market is an illusion and has not worked at all effectively to date.[101] Polanyi has observed that the State needs to construct "a network of measures and policies [which] are integrated into powerful institutions designed to check the action of the market relative to labor, land, and money"[102] and now personal data. This action is needed as

---

[97] *See* ZUBOFF, *supra* note 31.
[98] Krzysztofek, *supra* note 53, at 865-66.
[99] Press Release, European Commission, Agreement on Commission's EU data protection reform will boost Digital Single Market (Dec. 15, 2015) (on file with author).
[100] *Id.*
[101] Andrew Rossow, *The Birth Of GDPR: What Is It And What You Need To Know*, FORBES (May 25, 2018, 7:32 AM), https://www.forbes.com/sites/andrewrossow/2018/05/25/the-birth-of-gdpr-what-is-it-and-what-you-need-to-know/#57e8141355e5.
[102] KARL POLANYI, THE GREAT TRANSFORMATION: THE POLITICAL AND ECONOMIC ORIGINS OF OUR TIME 79 (2nd ed. 2001).

an institution has "a reality of their own, a reality that confronts the individual as an external and coercive fact."[103]

The problem is the effectiveness of the data regulatory measures adopted by states and how they can be improved. In contention is the balance between regulatory measures that serve as instruments that preserve the economic utility of the IoT while protecting the social rights of those who are subjected to it.[104] That balance, at worst, is precipitous in challenging the financial incentives of data collectors, processors and miners in largely unregulated global data markets.[105] At best, that balance is impeded by obstacles that regulators face in determining the social, social and ultimately, legal nature and applicability of human rights protection accorded to data subjects.[106] If Zuboff is correct, institutional regulations of the IoT have had very little effect in tethering surveillance capitalism.[107] She writes:

> "[w]hen it comes to surveillance capitalist operations, the 'market' is no longer invisible, certainly not in the way that Smith or Hayek imagined. The competitive struggle among surveillance capitalists produces the compulsion toward totality."[108]

Zuboff's assertion is that, in place of free access to the net, is competition among internet providers to secure ever more extensive control in collecting, processing and mining data. This contention is especially evident when internet providers like Facebook and Google construct a reality different from the one envisaged by individuals, as well as by State institutions. The rationale

---

[103] CHILDRESS, *supra* note 2, at 76.
[104] Kate Fazzini, *Europe's sweeping privacy rule was supposed to change the internet, but so far it's mostly created frustration for users, companies, and regulators*, CNBC (May 5, 2019, 9:34 AM), https://www.cnbc.com/2019/05/04/gdpr-has-frustrated-users-and-r.
[105] *Data mining for profit and manipulation*, JAPAN TIMES (Mar. 22, 2018), https://www.japantimes.co.jp /opinion/2018/03/22/editorials/data-mining-profit-manipulation/#.XaZt7edKjfY.
[106] *See* Bruno Zeller et al., *The Right to be Forgotten—the EU and Asia Pacific Experience (Australia, Indonesia, Japan and Singapore)*, 1 EUR. HUM. RTS. L. REV. 23, 23-37 (2019).
[107] ZUBOFF, *supra* note 31.
[108] ZUBOFF, *supra* note 31, at 497.

supporting this contention is that multinational Internet corporations have become institutions themselves, not controlled by any state, nor by data consumers that function beyond any one State.[109]

The ominous reality is that data corporations are the principal regulators of the Internet, not state regulators and certainly not data consumers.[110] The reality is not whether states determine whether the individual will adhere to data protection legislation, but rather whether data miners – those with the profit motive – can be controlled by state institutions that are adequately informed by patterns of behavior employed by surveillance capitalists.[111] The huge task for regulators is to regulate an IoT that has moved rapidly from user determination on an information highway to control data excised by corporations that create often unexpected and sometimes destructive roadblocks and barriers over every inch of that highway. The result is that surveillance capitalism directs rather than responds to social action, creating obstacles for governments attempting to constrain that unchecked surveillance. For some, the "social world [is] in the process of construction, containing within the root of an expanding institutional order."[112] In effect, the social world dominated by the IoT represent a shift from institutional legal ordering to institutional data surveillance ordering.[113] The IoT is institutionalized by a competitive corporate order whose aspirations are distinct from, not replicated by, the society of data users.[114] Nor, too, is the IoT effectively regulated by states seeking to mediate between data corporations that choose the mechanisms by which to manage and trade in personal data and data subjects who seek to limit the use of those mechanisms and trade.[115]

The reality is that the coercive power of surveillance capitalism over the individual's personal data is still maintained, but the mega-data corporations exercising that coercion have become

---

[109] See Robert Walters, Bruno Zellers & Leon Trakman, *Personal Data Law and Competition Law – Where is it Heading?*, 39 EUR. COMPETITION L. REV. 1, 5-12 (2018).
[110] *See id.*
[111] *See id.* at 16-17.
[112] CHILDRESS, *supra* note 2, at 75.
[113] ZUBOFF, *supra* note 31, at 497.
[114] *See id.* at 497.
[115] *See* Walters, Zeller & Trakman, *supra* note 109.

alarmingly entrenched.[116] Mechanisms of social control implemented by surveillance corporations reflects their subjective aspirations, rather than patterns of social behavior directed at protecting the personal space of individuals.[117] Nor do they defer to attempts by state regulators to construct an objective reality; instead, they defy such attempts.[118]

Berger and Luckmann argued in 1966 that "[t]he more conduct is institutionalized the more predictable and thus the more controlled it becomes."[119] However, this argument is less sustainable today, notably with powerful multinational tech giants commanding the flow of data over the internet by surreptitious means directed at duplicitous ends. Individual data subjects are still subject to institutional constraints: but these constraints rest with tech-giants that determine their effectiveness in their own images. Berger and Luckmann propose an effective means of promoting regulatory order through coercion. "If socialization into the institutions [of regulation] has been effective, outright coercive measures can be applied economically and selectively."[120] However, applying coercive measures "economically and selectively" to remediate the excesses of largely unregulated surveillance capitalists is economically, socially and politically fraught. The core issue is not whether the coercive mechanisms are applied economically and selectively, but from whose perspective they are "economical". If that perspective is identified with surveillance capitalists, the for social ends is decided by favoring their economic benefits. Social ends that conflict with their corporate good are, effectively, sublimated.

There is no better example of the tension between the interests of data corporations and societal interests in protecting personal data than the ongoing tension between the privacy of data

---

116 ZUBOFF, *supra* note 31, at 497.
117 *See* Deborah Cornwall, *Google on contempt charge over reviews*, THE AUSTRALIAN (July 8, 2019, 1:00 AM), https://www.theaustralian.com.au/nation/google-on-contempt-charge-over-reviews/news-story/a91b54fb41c5578acfbeba5387eb4969.
118 *See id.*
119 *See* BERGER & LUCKMANN, *supra* note 7, at 80.
120 *See id.*

subjects and breaches of that privacy attributed to Facebook over the past 5 years. This privacy issue continues to multiply and constitutes a major governance issue. For example, the Federal Trade Commission (FTC) lists 450 pages of correspondence between Facebook and the FTC for the period March 10, 2011 through March 20, 2018.[121] In addition, *The New York Times* reports that "Facebook and the Federal Trade Commission [FTC] are discussing a settlement over privacy violations that could amount to a record, multibillion-dollar fine."[122] This followed a 2011 agreement where Facebook "agreed to settle charges that it had deceived consumers on privacy."[123] By late March 2019, Facebook was accused of violating the Fair Housing Act.[124] Additional unauthorized Facebook user records continue to surface.[125] In July 2019, the FTC fined Facebook 5 billion dollars for violating the privacy of millions of its users by providing their personal information to Cambridge Analytica, a now defunct company engaged in political marketing.[126] Some view that penalty is no more than a slap on the hand.[127] Others view it as the demonstrated willingness of government regulators to penalize

[121] E-Mail from Edward Palmieri, Counsel, Facebook, to Reenah Kim, Federal Trade Commission (Jan. 22, 2015, 6:04 AM) (on file with author).
[122] See Cecilia Kang, *Facebook Fine Could Total Billions if F.T.C. Talks Lead to a Deal*, N.Y. TIMES (Feb. 14, 2019), https://www.nytimes.com/2019/02/14/technology/facebook-ftc-settlement.html.
[123] Natasha Singer, *Why the F.T.C. Is Taking a New Look at Facebook Privacy*, N.Y. TIMES (Dec. 22, 2018), https://www.nytimes.com/2018/12/22/technology/facebook-consent-decree-details.html.
[124] *See* Katie Benner, Glenn Thrush & Mike Isaac, *Facebook Engages in Housing Discrimination With Its Ad Practices, U.S. Says*, N.Y. TIMES (Mar. 28, 2019), https://www.nytimes.com/2019/03/28/us/politics/facebook-housing-discrimination.html; *See also* Josh D. McKinnon & Jeff Horwitz, *HUD Action Against Facebook Signals Trouble for Other Platforms*, WALL ST. J. (Mar. 28, 2019), https://www.wsj.com/articles/u-s-charges-facebook-with-violating-fair-housing-laws-11553775078.
[125] *See* Sarah Frier, Matt Day & Josh Eidelson, *Millions of Facebook Records Found on Amazon Cloud Servers*, BLOOMBERG (Apr. 3, 2019, 1:23 PM) https://www.bloomberg.com/news/articles/2019-04-03/millions-of-facebook-records-found-on-amazon-cloud-servers.
[126] *See* Julie Carrie Wong, *Facebook to be fined $5bn for Cambridge Analytica Privacy Violations- reports*, THE GUARDIAN (Dec. 7, 2019, 6:12 PM), https://www.theguardian.com/technology/2019/jul/12/facebook-fine-ftc-privacy-violations.
[127] *See* David Cicilline (@davidcicilline), TWITTER (July 12, 2019, 2:09 PM), https://twitter.com/davidcicilline/status/1149787832275410944 ("It's very disappointing that such an enormously powerful company that engaged in such serious misconduct is getting a slap on the wrist.").

surveillance capitalists for institutionalizing patterns of behavior wholly in their own financial interests.[128]

Governmental challenges to data corporations now also include the creation of regulatory bodies.[129] The Wall Street Journal reports that "the U.K. government plans to create a regulatory body to force the removal of harmful content from the internet, one of the most far- reaching proposals from a host of countries trying to put a tighter leash on global technology companies."[130] New global regulations now seem to be a virtual certainty, but how pervasive and effective they will be remains speculative.[131]

It is nevertheless true to argue that the uncertainty is how to reconcile the market-based ideology directed as expanding profit and increasing access to data balanced against societies' ambition to protect personal data and limit its erosion. The challenge to finding that balance is identified with the parallel contest between an autonomous IoT and its - as yet largely unchartered - territorial waters. The fact is that most users of internet applications and devices struggle to understand how they work, given the lack of an effective interface across those applications and devices. This, in turn, leads to lack of legibility in how data is being processed, why and by whom it is processed, where and for how long it is being stored.[132]

It is therefore not surprising that the State as an institution is at odds with the reality as perceived by surveillance capitalism and why it struggles to command the necessary control over all

---

[128] *See* Emily Glazer, Ryan Tracy, & Jeff Horwitz, *FTC Approves Roughly $5 Billion Facebook Settlement*, Wall St. J. (July 12, 2019), https://www.wsj.com/articles/ftc-approves-roughly-5-billion-facebook-settlement-11562960538?mod=hp_lead_pos1.
[129] *See* Sam Schechner & Parmy Olson, *Facebook, Google in Crosshairs of New U.K. Policy to Control Tech Giant*, WALL ST. J. (Apr. 8, 2019), https://www.wsj.com/articles/u-k-moves-to-end-self-regulation-for-tech-firms-11554678060.
[130] *Id.*
[131] *See* Jamie Condliffe, *The Week in Tech: Facebook Is Desperate to Shape Tech Regulation. Should it?*, N.Y. TIMES (Apr. 5, 2019), https://www.nytimes.com/2019/04/05/technology/big-tech-regulation.html.
[132] *See* Lachlan Urquhart, Tom Lodge & Andy Crabtree, *Demonstrably Doing Accountability in the Internet of Things,* 27 INT'L. J. L & INFO. TECH. 1, 4 (2019).

participants in the IoT. Not surprisingly, Zuboff coined the new reality the surveillance capitalism, as is discussed immediately below.[133]

6. Surveillance Capitalism

It is of value to define, albeit briefly, what Zuboff understands to be surveillance capitalism. She notes at the very beginning of the book a new economic order that claims human experience as a free raw material for hidden commercial practices of extraction, prediction, and sales.[134] The origin of a new instrumentarian power that asserts dominance over society and present startling challenges to market democracy.[135] This paper accepts Zuboff's definition recognizing that it is not the only definition given by scholars. What is undisputed is that the tech-giants understood long ago the economic potential of the IoT. Like the siren calls, their marketing teams proclaimed to IoT consumers that they, the source of social surveillance, more truly represented the public at large:

> Our ultimate ambition is to transform the overall Google experience, making it beautifully simple, almost automagical, because we understand what you want and can deliver it instantly.[136]

Arguably, this self-aggrandizing proclamation explains that surveillance capitalists like Google and Facebook have long understood that their control over the means of production serves to modify consumer behavior.[137] An example of changing behavior arising from the star spangled upward spiral of the data surveillance revolution is that comments posted on Facebook would, in many cases, not be replicated in face to face communication. It is the inhibiting factor of having a direct response or rebuff for invasive and offensive statements which the IoT has removed. Zuboff puts it, at least in

---

133 ZUBOFF, *supra* note 31.
134 Noah Kulwin, *Shoshana Zuboff on Surveillance Capitalism's Threat to Democracy - The Harvard Business professor discusses her new boo*k, INTELLIGENCER (Feb. 24, 2019), http://nymag.com/intelligencer/2019 /02/shoshana-zuboff-q-and-a-the-age-of-surveillance-capital.html.
135 *Id.*
136 *Google Management Discusses Q3 2011 Results – Earnings Call Transcript,* SEEKING ALPHA (Oct. 13, 2011), https://seekingalpha.com/article/299518-google-management-discusses-q3-2011-results-earnings-call-transcript.
137 *Understanding User Behavior with Google Analytics*, GOOGLE, https://support.google.com/analytics /answer/7126596?hl=en (last visited Nov. 7, 2019).

part, by stating: "Machine processes replace human relationships so that certainty can replace trust."[138] In effect, surveillance capitalists constructed their own reality of a "private knowledge kingdom."[139]

Importantly, the results produced by those machines is "certain" primarily in ensuring expanding internet intrusions into personal space and through it, the security of the space which individuals within an user society, occupy.[140] The "trust" in conversation that is lost, is not only in data collectors and processors depersonalizing the source of conversation between individuals, but also in a loss of the environment in which any conversation occurs. Not only do data corporations provide access to information on the IoT; they provide the institutional medium through which paparazzi seeking, often without self-identification, to invade the sensitive space of others, and in extreme cases, to stalk and even torment victims who are largely silent, unable to answer.

The capacity of surveillance companies to create an environment in which conversation is stultified is not unlimited. Every society, with its distinctive legal framework, creates its own coercive reality. As an example, the EU protects individuals from having their personal data mined and used without their consent.[141] In contrast, Singapore is now debating whether companies are required to seek their customers' consent to use personal data for business reasons, such as for data analytics.[142] Demonstrating the erosion of data privacy was the 2010 declaration by Facebook's CEO, Mark Zuckerberg, that privacy was no longer a social norm and CEO would relax the company's privacy entitlements.[143]

---

[138] ZUBOFF, *supra* note 31, at 351.
[139] ZUBOFF, *supra* note 31, at 352.
[140] *Id.*
[141] *See GDPR Consent Examples*, PRIVACYPOLICIES.COM (Sept. 25, 2019), https://www.privacypolicies.com/blog/gdpr-consent-examples/.
[142] Ng Jun Sen, *How should personal data be used and shared by firms? New rules on data protection up for review*, TODAY (May 22, 2019), https://www.todayonline.com/singapore/how-my-personal-data-used-new-rules-data-protection-review.
[143] *See* Bobbi Johnson, *Privacy no longer a social norm, says Facebook founder,* THE GUARDIAN (Jan. 10 2010), https://www.theguardian.com/technology/2010/jan/11/facebook-privacy.

The data surveillance environment is a constantly changing virtual reality that comprehensive social response. Economists well appreciate the slow emergence of "creative responses" within society at large in response to reality capitalism that replicates its self-created heritage and spurns social disapproval of its transcendence. Resistance to creative responses to social and economic changes is not limited to today's surveillance capitalism. Schumpeter wrote, decades ago:

> Creative response shapes the whole course of subsequent events and their long run outcome [Hence] creative response changes social and economic situations for good … This is why creative response is an essential element in the historical process. … We are dealing with a process whose every element takes considerable time in revealing its true feature and ultimate effects.[144]

Schumpeter is well justified in maintaining the impact of historical change upon the social and economic "good", and by recasting, indeed sometimes reconstituting, social reality. Surveillance capitalism, with the invention of the IoT, has forced a change in social behavior. This, in turn, has forced the institutions of the State to play catch up with the ascending new reality of the IoT in response to social changes brought by surveillance capitalism. The GDPR is an early response, and warning signal, of the impact of the machinery of the IoT upon social interaction in everyday life. Typifying this response is the decision of the EU Court of Justice in *Google Spain SL v Agencia Espaniola de Protection de Datos.*[145] in applying the GDPR to protect ninety applicants seeking their anonymity over the internet, by granting them the "right to be forgotten". That decision demonstrates the GDPR's institutionalized response directed as preserving each person's private space. It also represents the first significant judicial censure of the invasive intrusion by surveillance capitalism upon the autonomy of the person.

---

[144] *See* JOSEPH SCHUMPTER, THE ECONOMICS AND SOCIOLOGY OF CAPITALISM 412 (Richard Swedberg ed., Princeton University Press 1991).
[145] *See* Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), 2014 ECLI:EU:C:2014:317 (May 13, 2014).

Google Spain has been followed by courts outside the EU, but without comparable legal consequences. As an example, the New South Wales Supreme Court in Australia issued a contempt of court order against Google.[146] It ordered Google to take down defamatory comments posted by online trolls.[147] Google, ignored the court ruling and did not even attempt to respond to, or otherwise contact, the court.[148] Part of the new reality, as demonstrated in this case, is that corporate institutions have become so economically and socially empowered, that state institutions are often ineffective in attempting to regulate their excesses.[149] The fact is that Google cannot be sent to jail. An Australian court cannot, and Australian legislatures will not, impose meaningfully legal sanctions upon a global entity engaged in a trade which knows no national boundaries.[150] However, even this deference to corporate giantism may be changing. In its 2019 report on the digital platforms inquiry, the Australian Consumer and Competition Commission (ACCC) "clearly called out" the behavior of internet giants, identified the personal information they should be disallowed from collecting, and recommended the establishment of a new regulatory body to monitor their digital platforms.[151] Whether the Australian Government will confront such tech giants as Google and Facebook with effective regulatory responses, in the absence of comparable developments elsewhere and beyond the EU's GDPR, remains to be seen. What is likely are Joseph Schumpeter's words, that change will only reveal its true features over time, and one might add, after concerted and tenacious effort.[152]

---

146 Michaela Whitborn, *Google faces contempt charge for failing to remove defamatory reviews*, SYDNEDY MORNING HERALD (July 7, 2019, 12:15 AM), https://www.smh.com.au/national/google-faces-contempt-charge-for-failing-to-remove-defamatory-reviews-20190706-p524q3.html.
147 *Id.*
148 *See* Cornwall, *supra* note 117.
149 *See* Cornwall, *supra* note 117.
150 *See generally Australia: Sanctions 2020*, ICLG.COM (Nov. 10, 2019), https://iclg.com/practice-areas/sanctions/australia.
151 *See* Nassim Khadem, *Crackdown on Facebook, Google looms as ACCC hands down its final report into digital platforms*, ABC NEWS (Jul. 26, 2019, 4:08 AM), https://www.abc.net.au/news/2019-07-26/government-threaten-google-facebook-with-digital-regulation/11348858.
152 SCHUMPTER, *supra* note 1444, at 412-83.

Protecting personal data from data surveillance also hinges less on social resistance to that surveillance, than to regulatory responses to the IoT as a mode of communication. Social interaction over the IoT often does more to feed than respond to capitalist behavior; hence, the real clash is not between individuals within society and surveillance capitalists, but between the State – its institutions – and data surveillance corporations. This clash is accentuated by the fact that society has reduced face-to-face contact in preference for machine communication systems, such as those facilitated by tech-giants.[153] Important is the readiness of data consumers to endorse the wonders of inexpensive access to the internet and their lack of resources to protect their personal information from the invasive capabilities of those that manipulate that information.

Zuboff mounts the argument that:

> [O]ver the centuries we have imagined threats in the form of state power. This left us wholly unprepared to defend ourselves from new companies with imaginative names run by young geniuses that seemed able to provide us with exactly what we yearn for at little or no cost.[154]

The reality is that, if society at large is unable to defend itself from mega-tech corporations that replace the regulatory powers of the state, how can society protect itself from the coercive power of authoritative corporations whose supranational authority over their data subjects prevails over the authority of the state?

A pertinent distinction to draw is that, in past decades, people's power was used to defend the privacy and human rights of individuals within society as a reality of their everyday lives. Zuboff justifiably contends that a smaller percent of the population is prepared to face off against corporations; they simply cannot afford the legal costs.[155] A bigger proportion has already adjusted to

[153] *See generally* Katy Steinmetz, *Teens Are Over Face-to-Face Communication, Study Says*, TIME (Sept. 10, 2018), https://time.com/5390435/teen-social-media-usage/.
[154] ZUBOFF, *supra* note 31, at 53.
[155] *Id.*

the evolving reality of the IoT; they ignore or tolerate the cultural misappropriation of their personal data for the promised connectivity.

Arguably, the desire of participants in everyday society to communicate all the details of their personal experiences on a public platform, such as what they ate for lunch, both feeds on and serves as a rich source of data mining. In essence, the past reality which was marked by curiosity and questioning in social interactions is replaced by the "masterful rhetorical misdirection"[156] generated by surveillance corporations in which individuals serve as their means of generating a profit. In effect, society has accepted that "our lives [are] plundered for]behavioral] data."[157]

An emerging response to data users succumbing to global data surveillance is the argument that mega-tech corporations should be reconstituted along national and regional lines.[158] For example, Stephen Scheeler, past Managing Director of Facebook, Australia, acknowledged the argument for the technology platform to be broken up globally.[159] A supporting rationale is that there is more economic value in breaking Facebook up than running it as a single company.[160] In reality, it does not matter materially whether Facebook is one single company or not. The source of its income is still the same, namely, a platform on which to harvest information and sell it on to interested parties. Interesting, too, is the contention, that data regulations should be withdrawn, and that no moderation of information should take place.[161]

What is also questionable is the contention that breaking up Facebook will reduce the need for the regulatory oversight directed at it as a single global corporation. The ironic reality is that

---

[156] *Id.* at 51.
[157] *Id.* at 53.
[158] *See* Pippa Chambers, *Facebook Australia MD Stephen Sheeler resigns*, ADNEWS (Feb. 13, 2017), http://www.adnews.com.au/news/facebook-australia-md-stephen-scheeler-resigns.
[159] See id.
[160] *See* Leo Shanahan, *Business case for splitting Facebook*, THE AUSTRALIAN (July 8, 2019), https://www.theaustralian.com.au/business/media/business-case-for-splitting-facebook/news-story/f6056e34e3d747969765c955d9a31490.
[161] *Id.*

regulations directed at data surveillance companies is discernible globally, regardless of the place of incorporation. As a result, the regulatory framework may well increase, not decrease, if mega-tech corporations move away from a single company model.

A contrary proposition is that tech giants operating in smaller company structures will be able to conduct more focused surveillance, as general sampling will be replaced by in-depth concentration on the collection of data. The capacity of tech-giants to influence and exploit the construction of a new reality based on corporate segmentation is therefore likely to remain contestable, regardless of whether data platforms are segmented or otherwise divided. The next section will analyze the process that has evolved in constructing the evolving reality of corporatized surveillance.

6.1 The process of constructing the reality

Next, we ask, if democratic institutions are to prevail, how can they transcend the intransigence of surveillance capitalism? How, too, can those institutions survive the mutation of social communication and redress disparate social expectations of the IoT?[162] Importantly, can democratic institutions survive "changes [in] the nature of capitalism by shifting it in the direction of those it is supposed to serve"?[163] The issue linking these different questions is whether surveillance capitalists are still bound within reciprocal relationships with their data user populations through continuing but changing democratic institutions.

Viewed pessimistically, democratic institutions already subserve to the ever-expanding power of surveillance corporatism. Illustrating this expansiveness is the realization that, as much as individuals aspire for privacy from mega-tech corporations, they sometimes also want to protect their privacy from those seeking to expose privacy violations by those self-same corporations. As the world

---

[162] *See* Friedrich A. Hayek, *The Use of Knowledge in Society,* 35 AM. ECON. REV. 519–30 (1945), https://www.econlib.org/library/Essays/hykKnw.html (on self-ordering); *See also* ZUBOFF, *supra* note 31, at 52; *See also* PAUL OSLINGTON, ADAM SMITH AS THEOLOGIAN 61-77 (2011).

[163] Zuboff, *supra* note 31.

learned that Cambridge Analytica (CA) had expropriated the personal data of millions of Facebook users, a millionaire financial associated with CA, Aaron Banks, sued the journalist who broke the "story", arguably to discourage the release of the documentary on CA, the Great Hack.[164] So conceived, Banks' alleged purpose was to protect his reputation and personal damage arising from public disclosure of his association with CA.[165] However, in initiating suit Banks implicitly also sought to protect CA's "secrets" on how it used surveillance to exploit its personal data.[166] The inference is that the exploitation of data encompasses both surveillance corporations invading the private space of data subjects and data subjects exploiting the corporate space occupied by surveillance enterprises.[167] A response is that leadership in addressing such challenges ought to emanate from surveillance corporations that exploit personal information, even if that exploitation leads to counter exploitation from the targets of such surveillance.

The challenge ahead is in exploring how surveillance capitalism can initiate change, protecting data subjects from sustained, excessive and debilitating surveillance of an individual's personal space.[168] Can mega-corporations can become responsible initiators of social actors? Can they tell and replicate stories about the prospective abuse of personal data and how to avert them? Can Google and Facebook inform an IoT dependent society about the risks of having their personal information

---

[164] Ellie Harrison, *Netflix threatened by Brexit funder Arron Banks over The Great Hack documentary*, INDEPENDENT (July 22, 2019), https://www.independent.co.uk/arts-entertainment/tv/news/netflix-the-great-hack-documentary-brexit-arron-banks-legal-lawsuit-a9015291.html; *See generally* Charlotte Tobitt, *Carole Cadwalladr will defend 'true' claims about Brexiteer Arron Banks in libel battle*, PRESS GAZETTE (July 15, 2019), https://www.pressgazette.co.uk/carole-cadwalladr-will-defend-true-claims-about-brexiteer-aaron-banks-in-libel-battle/.

[165] *See generally* Charlotte Tobitt, *Carole Cadwalladr will defend 'true' claims about Brexiteer Arron Banks in libel battle*, PRESS GAZETTE (July 15, 2019), https://www.pressgazette.co.uk/carole-cadwalladr-will-defend-true-claims-about-brexiteer-aaron-banks-in-libel-battle/.

[166] *See* Emma Graham-Harrison**,** *Brexit funder Arron Banks threatens Netflix over Great Hack documentary*, THE GUARDIAN (July 20, 2019, 11:59 EDT), https://www.theguardian.com/uk-news/2019/jul/20/arron-banks-netflix-threat-great-hack-documentary.

[167] Jathan Sadowski, *Companies are making money from our personal data- but at what cost?*, THE GUARDIAN (Aug. 31, 2016, 9:00 EDT), https://www.theguardian.com/technology/2016/aug/31/personal-data-corporate-use-google-amazon.

[168] ZUBOFF, *supra* note 31.

disclosed and how to limit those risks? Importantly, can these mega-corporations still profit from pursuing such socially responsible action, at what cost, and who must bear that cost?

Sadly, the prevalent reality is of a society of data users that has already unquestioningly accepted the exploitative technology of a depersonalizing IoT as the new way to live and appears to be unwilling or unable to reduce their connectiveness from the world-wide web to return to a face to face reality.[169] But institutions and society are in the process of understanding that, not all information is, or deserves to be treated as irreparably immortal. Schwartz and Pfeifer note that, as far as governmental institutions are concerned, a "Luxembourg Court felt that. . . [f]ree flow of information matters, but not as much, ultimately, as the safeguarding of dignity, privacy, and data protection in the European rights regime."[170]

The impetus to redefine the reality of life in the age of the IoT is also unlikely to emanate from recanting surveillance capitalists. The source of such redefinition emanates from social action, to which legal regulators respond as a measure of responsible and socially responsive governance. The predictable response to this social and regulatory reality is for data surveillance corporations to dismiss the social source of regulation as no more than a historical aberration. This the result of the judicial ruling against Google for violating a person's right to be left alone, in *Google Spain*.[171] After *Google Spain* was decided, Google leaders sneered at the decision.[172] When asked about *Google Spain* at a tech conference, Sergey Brin responded: "I wish we could just forget the ruling."[173] However, the balancing power of the legal institution in that case was to demonstrate that neither the determining legislators,

---

169 *See Policy Brief: IoT Privacy for Policymakers*, INTERNET SOCIETY (Sept. 19, 2019), https://www.internetsociety.org/policybriefs/iot-privacy-for-policymakers/.
170 *See* Paul Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy*, 106 GEORGETOWN L. J. 115, 131 (2017).
171 *See* SCHUMPTER, *supra* note 144, at 412 (on Google Spain).
172 *See* Greg Sterling, *Google Co-Founder Sergey Brin: I Wish I Could Forget The "Right To Be Forgotten,"* SEARCH ENGINE LAND (May 28, 2014), https://searchengineland.com/google-co-founder-brin-wish-forget-right-forgotten-192648.
173 *See id.*

nor the court acceded to the unilateral exercise of power of a corporation acting with indifference towards the protection of personal information.

What remains speculative at this time is the capacity of legal institutions to extract the reality of life from the commanding presence of surveillance corporations, extending it to the life of a society which those corporations have exploited. In determining whether legal institutions have such capacity, it is necessary to determine whether data users and data subjects in particular have the knowledge to initiate and applaud such regulatory action. "[N]o part of institutionalization of data protection can exist without the particular knowledge that has been socially produced and objectivized with reference to this activity."[174]

The problem in data subjects and law makers responding to surveillance capitalism is that such surveillance is not socially produced; its "existence [is] in a social world defined and controlled by [corporations] and [their] body of knowledge."[175] However, a social world that is controlled by surveillance corporatism cannot be institutionalized unless the source of that control mutates, or is forced to mutate, through regulatory action. Hence, surveillance capitalism will only succeed and be part of the socially accepted reality when it becomes a social product and when that product is derived from socially accepted norms. We must keep in mind that we live in a global village where socially accepted norms vary in response to changing, including external norms that a data using society internalizes. Functioning in that global village, in effect, corporate capitalism itself can be the "spark" that induces a change in social norms, in effect leading to a radical shift in a new social reality adopted by a social response to such corporate action.[176]

---

[174] BERGER & LUCKMANN, *supra* note 7, at 85.
[175] BERGER & LUCKMANN, *supra* note 7, at 85 .
[176] FRANCESCA BRIA, SOCIAL MEDIA AND THEIR IMPACT ON ORGANISATIONS: BUILDING FIRM CELEBRITY AND ORGANISATIONAL LEGITIMACY THROUGH SOCIAL MEDIA 164-65 (Imperial C. London, 2014).

The IoT is the tool at hand: it was created by surveillance companies that brought the extent of its eavesdropping, however unintentionally, to public knowledge and attention.[177] The result is the social and regulatory scrutiny of such conduct based on what kind and level of surveillance is socially acceptable. There is no significant social debate that the mechanical tools devised and applied by Google and Facebook are "nothing less than spawning a new variant of capitalism."[178] These are already part of everyday reality that have superseded many functions of pre-existing daily life.

What is debatable is whether the kind and level of data surveillance is permanent or irreversible. In contention is whether the consuming public and institutional regulators will accept it, reserve judgement about it, or actively challenge it. The contest between data society, legal institutions and corporatized capitalism therefore revolves around how much of the corporate business model will be institutionalized and accepted as the reality of everyday life. Berger and Luckmann reasoned that this sedimentation is "only a small part of the totality of human experience [that] is retained in consciousness."[179] They reasoned further, that:

> Intersubjective sedimentation can be called truly social only when it has been objectivated in a sign system of one kind or another, that is, when the possibility of reiterated objectification of the shared experience arises.[180]

They maintained, in support, and elaborated that "language provided the means of objectifying new experiences."[181] The fact that machines have their own language and functions can be viewed as a language which Facebook and other functionaries on the IoT use to replace traditional languages,

---

[177] Christine Bannan, *The IoT threat to privacy*, TECHCRUNCH (Aug. 14, 2016), https://techcrunch.com/2016/08/14/the-iot-threat-to-privacy/.
[178] John Naughton, *'The goal is to automate us': welcome to the age of surveillance capitalism,* THE GUARDIAN (Jan. 20, 2019), https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook.
[179] BERGER & LUCKMANN, *supra* note 7, at 85.
[180] BERGER & LUCKMANN, *supra* note 7, at 85.
[181] BERGER & LUCKMANN, *supra* note 7, at 86.

such as French or English.[182] The objectifying inference is that the IoT becomes a global language embodying a communicating reality that expands to all who "speak" it and are subject to its "speak."[183] However, this universal language, grandly conceived, is truly subjective in its creation and application.[184] It is troubling that to those who devise and operate the machinery of that global language of the IoT are the directors of corporate capitalism. There is confirmation about data users of the machinery of the global IoT language.[185] There is debate over whether the primary determinants of that "speech" are also the source of the subjugation of those data users and the implications of new technologies is the trade-off to the right to privacy.[186] On

the one side, therefore, is the fact that to date, the mechanical speech of the IoT has largely won its immediate struggle to preserve free use of the Internet. It has not done so for the public good, but for its corporate and shareholder profit-making. On the other side is social suspicion about how that surveillance "speech" interfaces with the reality of data protection and privacy of data subjects. There is further debate in a data using society between those who support an unregulated internet to secure ongoing access to its intrigue, and those who demand that it complies with socially acceptable and defined conceptions of respect for human subjects and their private space.[187] Some predict that these debates will lead to the demise of the internet as we know it today, with new counter-Orwellian consequences. Presented starkly:

> The internet will disappear. There will be so many IP addresses … so many devices, sensors, things that you are wearing, things that you are interacting with, that you won't even sense it. It will be part of your

[182] Fredric Paul, *What programming languages rule the Internet of Things?,* NETWORKWORLD (Jan. 31, 2019), https://www.networkworld.com/article/3336867/what-programming-languages-rule-the-internet-of-things.html.
[183] *See generally id.*
[184] John Seabrook, *The Next Word: Where will predictive text take us?,* THE NEW YORKER (Oct. 14, 2019), https://www.newyorker.com/magazine/2019/10/14/can-a-machine-learn-to-write-for-the-new-yorker.
[185] *See generally id.*
[186] Carly Nyst, *Two sides of the same coin – the right to privacy and freedom of expression,* PRIVACY INT'L (Feb. 2, 2018), https://privacyinternational.org/blog/1111/two-sides-same-coin-right-privacy-and-freedom-expression.
[187] Richard Godwin, *How the internet if changing language as we know it (ikr lol)*, THE GUARDIAN (Oct. 11, 2019), https://www.theguardian.com/books/2019/oct/11/how-to-speak-internet-online-writing-richard-godwin.

> presence all the time. Imagine you walk into a room and the room is dynamic.[188]

In so positing, Eric Schmidt does not envisage the end of the internet, but rather a process of unshackling it from devices such as computers and phones.[189]

The more immediate reality is whether the all-embracing technology that data corporations use to operate the internet will preserve its current reality, mechanically and with limited social intervention. A challenge in its construction and operation, therefore, will depend not wholly on the socialization of the IoT, but on the machine-made environment in which we interact, not on a personal level, but with machines. The individual will become the subject of a message which is entrusted to, or captured by, the IoT. In essence, what is a human reality will be indistinguishable from that is machine reality. The control of information and the power to dictate how we act will be left to the programmed machines that will continue to have the power to influence and "guide" human thinking and activities. Hence it is important to understand what is meant by surveillance capitalism that is identified with data corporations.

6.2 What is Surveillance Capitalism?

Zuboff views surveillance capitalism as a "profoundly antidemocratic social force or a market driven coup from above."[190] It is a social force because it influences the decision making of society by concentrating exclusively on knowledge imbedded in a surveillance system which is not open to public scrutiny. Once devised and operationalized, that corporatized social force is rendered structurally independent from the people it regulates and from competing institutions. As such, the IoT becomes a coercive instrument for the mechanical regulation of human subjects, such as by

---

[188] *See* Chris Matyszczyk, *The Internet will vanish, says Google's Eric Schmidt*, CNET (Jan. 22, 2015, 6:00 PM), https://www.cnet.com/news/the-internet-will-vanish-says-googles-schmidt/.
[189] *Id.*
[190] ZUBOFF, *supra* note 31, at 513.

processing personal data of multiple subjects indiscriminately, even if that processing has a devastating effect on some data subjects.

Recently, Max Schrems, an Austrian data privacy campaigner, brought an action against Google accusing it "of 'coercing' users into accepting their data collection policies. The complaint strikes at the heart of the big tech companies' business model: providing 'free' online services in exchange for user profiling based on collecting of user data."[191]

Zuboff is not apologetic in describing surveillance capitalism as attempting to achieve "excusive concentrations of knowledge and power that sustain privileged influence over the divisions of learning in society; the privatization of the central principle of social ordering in the twenty first century. . .is a form of tyranny that feeds on people but is not of the people."[192]

Arguably this is the counterpart of learning before the Gutenberg printing revolution which challenged the control of knowledge and learning that the Church had exerted over the community at large. The power of learning rested exclusively in the hands of the Church; and only when printing was discovered was the power of learning uncoupled from the institution and, by implication handed to the people.

Arguably, Zuboff's views are not universally accepted, as it is a bleak picture she is painting. The emancipation in learning from the Church is also not a prototype template for emancipation from a dominating IoT. However, current reality has indicated that Facebook and Google are extremely reluctant to give up their business model. No doubt, too, the access of individuals in society to instant information is an irresistible inducement for them to forsake the principle of personal privacy. Many users of the IoT are not concerned about the business model of the tech giants, as long as their instant

---

[191] *See* Derek Scally, *Max Schrems files first cases under GDPR against Facebook and Google*, IRISH TIMES (May 15, 2018), https://www.irishtimes.com/business/technology/max-schrems-files-first-cases-under-gdpr-against-facebook-and-google-1.3508177.

[192] ZUBOFF, *supra* note 31, at 513.

access data through Google and Facebook works, and they can maintain contact with the world at large. Tech-giants will nevertheless need to change their business model to ensure that the internet becomes more invisible. The peril is in surveillance corporations extracting all information from the real world in which we live and relocating it in the virtual world that hungrily devours it all. Zuboff notes that the surveillance capitalist wants "your bloodstream and your bed, your breakfast conversation, your commute, your run, your refrigerator, your parking space, your living room."[193] The phase has already largely been accomplished. Now, surveillance corporations have dived into the new depths of information. They have uncovered new booty, the ultimate patterns of the self, that is, the reality in which every individual's experiences can be entrapped.[194]

> These supply operations are aimed at your personality moods and emotions your lies and vulnerabilities. Every level of intimacy would have to be automatically captured and flattened into a tidal flow of data points for the factory conveyor belts that proceed toward manufactured certainty.[195]

The central challenge ahead is to address the ever-growing demand of tech-companies to identify and capture information sources that are likely to maximize their income, to extract it by mechanical means, and to perfect that extraction process until all information that is profitable is controlled and used to the full advantage of the corporate extractor and hoarder of information.[196] For tech-companies to maintain their competitive advantages, they must be able to sell the highest quality prediction product. They also need to tap the source of that data, namely, from the real world of users of the IoT whose behavior they wish to predict and influence, if not direct.[197]

The means by which tech-companies shape the new order of control is by extending their machine-based extraction architecture into the real world that is the current reality of everyday life.

---

[193] ZUBOFF, *supra* note 31, at 201.
[194] *Id.*
[195] *Id.*
[196] ZUBOFF, *supra,* note 31, at 202.
[197] *Id.*

Their greatest ally is the predilection of the majority of data consumers to support the encapsulation of an ever-widening data spread; and the ability of surveillance corporations to predict a positive end user response to that spread. The fact that the majority of internet users who favor a free market in data is declining, serves as a real incentive for data collectors to market the social benefits of their services in order to re-entice a doubting public.[198] One means of data corporations to assess social attitudes towards the market in data is by enhancing their clandestine surveillance machinery and its analysis of those social attitudes.

The problem is that the method of shaping behavior to suit the profit motives of surveillance companies is attacking the very essence of society. The effectiveness of surveillance attacks is increasingly directed, not only at the geometrically increasing mass of personal data, nor even the analysis of points of connection between that data and behavior of data subjects within that mass. It is also directed at manipulating the behavior of the data subjects within that mass.[199] The purpose is not only to "know thy mind" but also to influence how whose minds work, such as to influence data subject's voting patterns. The result is that "the material infrastructure that performs extraction-and-execution operations begin[s] to function as a coherent whole,… produc[ing] a twenty-first-century means of [behavioral] modification."[200] Zuboff quoting the research director of Gartner who made the collateral point that mastery of the IoT will serve as a "key enabler in the transformation of business models from guaranteed levels of performance to guaranteed outcomes."[201] At that point, social control through the internet will have become virtually complete, and outcomes will be both predicable and assured. Participants in society will evolve into data objects, fully directed by data mechanisms that not only capture their personal identifies and behavioral patterns, will also capture

198 *Id.*
199 *Id.*
200 *Id.*
201 *Id.*.

reactions to the vicissitudes of everyday life, and more still. The invasive online machinery employed by surveillance corporations will enhance their market share by examining patterns of behavior across data samples drawn from databases that will be progressed to a far grander scale. Surveillance operatives will use such data far more extensively, to predict everything we do, well beyond buying patterns in discrete economic sectors. They will encapsulate our social behavior in multiple contexts, along with the anger, humility, submissiveness, or other tendencies we display.

The challenge is to develop legal mechanisms by which to respond to these intrusions on our human lives, indeed, on our humanity. As Berger and Luckmann argue, "every viable society must develop procedures of reality maintenance to safeguard a measure of symmetry between objective and subjective reality."[202]

The target of a reactive society is to join the expanding pushback from regulators to ensure that the mining of data does not continue to violate our personal privacy, and that the mining of data complies with slowly evolving legislation and court decisions that remediate inroads on our humanity. The social and legal target are tech-giants that have succeeded in creating a virtual reality. They used human targets whose behavior is entirely predictable because everything material that is known about them is part of a mechanical algorithm molded in corporate hands to virtual perfection.

The ultimate question is whether we are, and are likely to continue, to act like ostriches, burying our heads in the sand, while tech-giants are seeing, eating and living off the rich land taken from us. Are we ostriches, without knowledge and appreciation of what they are doing? Or are the inferences arising from these rhetorical questions over-generalized, or simply too pessimistic?

It is undeniable that corporate surveillance now does more than harvest the reality constructed out of what people produce. Corporate controllers of the IoT are now reforming their business models, not only to predict human behavior, but also to modify how data targets reach important

[202] BERGER & LUCKMANN, *supra* note 7, at 166-67.

social and political determinations.[203] How data targets voted in the US presidential election and in the BREXIT referendum, both in 2016 is a clear demonstration of the power of the IoT.[204] They are reconstituting the very theory underlying social construction prefaced on ever more accurate prognostications on human interactions and exchanges. Arguably, too, this virtualization of the tech world has extended beyond even Berger and Luckmann's visualization of institutional redirection of patterns of social behavior,[205] to the dictation of those very patterns.

Our argument is that, as long as the institutions represented by the State are focused on safeguarding and enforcing privacy, surveillance capitalism can at least be restrained, but not totally controlled. Perhaps grounded more in our faith and belief is our earnest conviction that the state will pursue these ends relentlessly in the interests of a common good beyond the good of data surveillance capitalists and their political and economic associates. The reality is that states, all too often, are overly ready to lie down in order to avoid trammeling profitable corporatized data markets in which tech-companies will resist regulation with every billion dollars that is available to them. They will also fear tech-giants deploying their ever more staggering financial reserves to reverse regulatory trends that would otherwise undermine their single-minded intentions.

6.3 Surveillance Capitalism and it influence on the stock of knowledge

Google is the discoverer and one of the lead practitioners and role models for surveillance capitalism. It is reputed to be a notoriously secretive company where executives carefully draft their messages of digital evangelism.[206] Given the social impact stemming from the exploitation of the IoT by such corporate giants Varian's observations are not surprising:

> Nowadays there is a computer in the middle of virtually every transaction [and] now that they are available these computers have several other uses [such as] data analysis

---

[203] Mark Hung, *Leading the IoT: Gartner Insights on How to Lead in a Connected World*, GARTNER (2017), https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf
[204] *Id.*
[205] *See* BERGER & LUCKMANN, *supra* note 7, at 166-68.
[206] ZUBOFF, *supra* note 31, at 64.

> and extraction, new contractual forms due to better monitoring, personalization and customization and continues experiments.[207]

The logical inference is that data programmers will be able to formulate algorithms that draw on multiple points of connection data subject and masses of date relating to them that are readily accessible inhouse databases. It follows that the corporate owner of data detection and behavior modifying machinery frequently have macro-political and socio-economic ends that diverge from data subjects who resist sharing their personal data publicly or selling it to partner companies seeking to influence macro-political and socio-economic events. The user wants to retain their personal privacy and human dignity. The data collector and processor want to perfect its mined data by exploiting the multiple connection points between data subjects and the likely patterns in their behavior.

This is to be understood as meaning that programs are specifically designed to capture information by enticing the usage of the aps, like bees to honey. Data, essentially, has become the raw material which is used to "manufacture" profiles of data users and hence becomes a merchantable good used, for example, in targeted advertising.[208] The issue is that every member of society has a role to play in becoming a participating actor in a data-based society, including tech-corporations, data users and government regulators. But data users, and data subjects among them, have struggled to understand their role in that society. "[B]y internalizing these roles", data corporations have ensured that "the same world becomes subjectively real."[209] However, the role played by all participating members in society, however expansively their "same world" is conceived, differ from data corporation, to state, to individual participant on the IoT.[210] Individuals wish to their maintain privacy.[211] The State drafts legislation to protect privacy but does not provide complete privacy. Data

---

[207] *Id.*; *See* Hal R. Varian, *Beyond Big Data,* NABE (2013), http://people.ischool.berkeley.edu /~hal/Papers/2013/BeyondBigDataPaperFINAL.pdf.
[208] BERNARD MARR, BIG DATA IN PRACTICE: HOW 45 SUCCESSFUL COMPANIES USED BIG DATA ANALYTICS TO DELIVER EXTRAORDINARY RESULTS (Wiley 2016).
[209] *See* CHILDRESS, *supra* note 2, at 91.
[210] *Id.*
[211] *Id.*

collecting and distributing corporations regulate privacy too, through data user contracts with data subjects, and in seeking to limit data privacy restrictions to secure total disclosure and ensure their profitable use of all captured data.[212]

The history of the IoT has demonstrated that, as soon as the invention of the IoT evolved into a social reality "roles appeared as a common stock of knowledge containing the reciprocal typification of conduct[which] is in process of formation, a process that, as we have seen, is endemic to social interaction and prior to institutionalization proper."[213] The issue now is to determine, firstly, whether collectors and processors are still primarily engaged in "social interaction" with governments, data users and data subject.[214] The second issue is whether the rules governing data surveillance are significantly institutionalized.[215] The third issue is to determine whether that institutionalization continues in operation, and how it has changed since inception.[216] The fourth issue, predictive in nature, is whether regulation of data collection will remain largely in the hands of surveillance corporations as the primary source of institutionalization going forward.[217] Berger and Luckmann have responded to these issues, in part, by arguing that, "as soon as actors are typified as role performers, their conduct is … susceptible to enforcement."[218] The inference is that, once data users and consumers assume roles in the IoT, they can be subject to rules governing their performance of those roles.[219] The reality is that, while individuals are ostensibly free to use the IoT, they lose that freedom when surveillance capitalists entice them to "tick" the box that empower them to use that personal data at will.[220] The attendant reality is that the State can only enforce the misuse of personal data if

---

[212] *Consumer Data Privacy Legislation*, NATIONAL CONFERENCE OF STATE LEGISLATURES (Oct. 14, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx
[213] CHILDRESS, *supra* note 2, at 92.
[214] *Id.*
[215] *Id.*
[216] CHILDRESS, *supra* note 2, at 92.
[217] *Id.*
[218] *See* BERGER & LUCKMANN, *supra* note 7, at 92.
[219] *Id.*
[220] *Id.*

that person has not signed or otherwise not accepted the standardized "tick" box interposed by the surveillance capitalist.[221]

The regulatory quandary is that both society, including individuals within it, and regulators of all segments in society are only now acknowledging the emergence of a new reality, based on a different stock of knowledge.[222] Past knowledge, namely privacy, is now being questioned and even attacked for its limited scope; and legal progressive institutions such as the EU's GDPR are at the incipient stage of protecting personal data beyond privacy rights.[223] The institutionalization of this regulatory process is, at best, in its infancy. The traditional machinery that was used to maintain an equilibrium between the forces of corporatism and consumerism, including through contracting, are now materially deficient.[224] Regulating this new technological reality requires innovative tools to reorder a world order dominated by the acquisition and handling within a globalized regulatory regime that is no longer equipped to redirect social change. One regulatory tool by which to facilitate this transformation is through "specific procedures of universe-maintenance [that] become necessary when the symbolic universe has become a *problem*."[225] However conceptually legitimate are these new "procedures of universe-maintenance", the reordering of data processing and usage of the IoT is distinctly restricted, so long as the key actors society - data corporation, individuals, and governmental regulators – are intertwined in a transitional stage of transformation. Far sighted regulations, epitomized by the GDPR, are not yet "complete". So long as they do not reflect the ambitions and roles of all three groups in society, the regulating and regulated universe will not be in equilibrium.

---

[221] *Id.*
[222] COMMITTEE FOR ECONOMIC DEVELOPMENT, REGULATION & THE ECONOMY: THE RELATIONSHIP AND HOW TO IMPROVE IT (2017).
[223] Michael Nadeau, *General Data Protection Regulation (GDPR): What You Need to Know to Stay Compliant*, CSO (May 29, 2019), https://www.csoonline.com/article/3202771/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html.
[224] *Id.*
[225] *Id.* at 123.

It is true that "socialization is never completely successful."[226] Some social actors, notably corporate data providers that inhabit the IoT space, dominate it more than both regulators and an intergenerational society of data users.[227] The result is the capacity of data providers to harness and embellish their power over the IoT more coherently, self-interestedly and definitively.[228] Importantly, the absence of comprehensive legislative and judicial restrictions on data surveillance and personal data usage remains institutionalized by corporate elite who, with their growing entourage with commercial customers, control the virtual world.[229] The main obstacle to such one-sided self-regulation is that, in the absence of externalized regulation, surveillance capitalists demand the privilege of unfettered freedom over the manner in which they collect and disseminate knowledge.[230] That demand is based on two bedrock assumptions about surveillance capitalism:

> The first is that markets are intrinsically unknowable.[231] The second is that the ignorance produced by this lack of knowledge requires wide ranging freedom of action for market actors.[232]

The solution is to enhance a spiraling but one-sided reality in response to the knowledge of data users, and to protect their freedom from market abuse.[233] A free market that perpetuates the ownership of data, notably through the originating intellectual property rights of data subjects, is woefully inadequate if surveillance corporations can readily access that data, with or without the consent of data subjects. If data consumers lack knowledge about how the data market operates and how their personal information is captured by data collectors and used by data processors, they are ill-equipped to resist mega-corporations that extract their consent through promises of continued and "free" access to corporatized websites. So long as data subjects are excluded from the essential

---

[226] *Id.* at 124.
[227] *Id.*
[228] *Id.*
[229] ZUBOFF, *supra* note 31, at 495.
[230] *Id.*
[231] *Id.*
[232] *Id.*
[233] *Id.*

dialectic around access to and the use of their personal data, they will fulfil the corporate image bestowed on them – of individuals who lack the knowledge, indeed capacity, to understand a data world that only surveillance capitalists can regulate effectively. The reality is that, if data subjects are excluded from the machinations of the IoT, surveillance capitalists will continue to secure or disregard the intellectual property of data subjects for commercial purposes and without paying for the use of that property. They will downstream that information to data miners and processers; and to end users such as hackers pursuing personal or economic advantage, as well as to anywhere-anytime curiosity seekers. Upstream and downstream data miners who are keen to avert litigation will be reassured that the data subject no longer has an intellectual property right in that data and has in the main consented by contract to its downstream use.[234]

We do not suggest that the free and efficient flow of goods, and hence the use of scarce resources, should be summarily suppressed to protect personal data. Data corporations could not exist without having profit generating products. Data users would incur direct user fees should data surveillance companies downstream their reduced profit-margins. A nuanced approach to data mining is therefore necessary. Sensitive personal data should necessarily be protected. Data access that serves as a supermarket in which users determine what staple products in purchase and place on their shelves, ought not to be subject to pervasive personal data protection. Nor should governments have an unfettered power to displace the free market in goods or services over the internet. This rationale for a measured supermarket in data services is not exceptional. As Adam Smith noted: "[no] statesman who should attempt to direct private people in what manner they ought to employ their capitals

[234] Leon Trakman, Robert Walters, Bruno Zeller., *Is Privacy and Personal Data set to become the new Intellectual Property?,* INT'L. REV. INTELLECTUAL PROP. AND COMPETITION L. (2019).

would… assume an authority which could safely be trusted, not only to no single person, but to no council or senate whatever..."[235]

The second issue, that the operation of markets is intrinsically unknowable by data consumers and governmental regulators, well preceded the invention of the IoT. What is distinctive, but also not a unique development, is that mega-tech corporations today wish to act with virtually unchecked freedom and to write their own textbooks on permissible corporate behavior. The source of this self-defining market autonomy, and the purported exclusion of governments from this private sector, is reaffirmed in neoliberal economic theory, well before the creation of the IoT. Friedrich Hayek laid the foundation for a market-privileging economic policy, unchecked by both the "visible" or "invisible hand" of government.[236] What surveillance capitalism has done is replace uncertain with certain market boundaries in data markets and in determining the scope and effect of such surveillance. That pattern of data surveillance has also established discernible patterns of conduct in virtual markets in place of the "unsurveyable pattern"[237] prevailing primarily in face-to-face markets. Importantly too, data surveillance corporations have enabled behavioral modification based on their informed predictions arising from measuring and assessing relevant data. Zuboff aptly refers to CEO, Mark Zuckerberg's boast that Facebook "would know every book, film, and song a person had ever consumed and that its predictive models would tell you what bar to go to when you arrive in a strange city, where the bartender would have your favorite drink waiting."[238] What might have been unthinkable in the face-to-face biosphere is now a virtual reality. As soon as a person arrives in a new country, the mobile phone will immediately receive a message saying, "welcome to Latvia".

---

[235] ADAM SMITH, AN INQUIRY INTO THE NATURE AND CAUSES OF THE WEALTH OF NATIONS 350 (S. M. Soares ed., MetaLibri Digital Library 2007).
[236] ZUBOFF, *supra* note 31, at 496.
[237] ZUBOFF, *supra* note 31, at 497.
[238] *See* Ashlee Vance, *Facebook: The Making of 1 billion users*, BLOOMBERG (Oct. 4, 2012, 7:06 PM), https://www.bloomberg.com/news/articles/2012-10-04/facebook-the-making-of-1-billion-users.

The disconcerting reality lies in the attribution to Mark Zuckerberg and other Facebook executives that "[w]e are trying to map out the graph of everything in the world and how it relates to each other."[239] This purportedly affirmative publicity for Facebook accentuates, rather than dissipates, the invasiveness of this "mapping" of a person's everything. Further disturbing is to determine the extent to which Facebook "mapping" is institutionalized.[240] Indeed, "how large is the sector of institutionalized activity as compared with the sector that is left un-institutionalized?"[241] The executives of mega-data corporations would like to deliver, or at least internalize, a negative answer, that any institutionalization outside the markets occupied by surveillance capitalists violates the efficiency of the internet as a free market.[242]

These postulations made by, or imputed to, surveillance capitalists, while self-serving, are nevertheless realistic at this juncture. Institutionalizing market order over the internet through external regulation is difficult to accomplish in the face of fragmented perspectives on the justification for and scope of data protection.[243] The fact is that the internet's "relevance structures are shared by groups within the society but not by the society as a whole."[244] The product is the segmentation of the institutional order with "role specific knowledge coming to be reserved to certain types."[245] Viewed reactively, these "certain types" in society encompass groups that, often unwittingly, feed corporations like Facebook with data which it uses to provide profit generating goods and services. What is doubtful, too, is how an institutional order can generate objective knowledge in light of divergent structures of "role specific knowledge" across the entire society.[246] That doubt is accentuated by the inference that surveillance capitalists want to command and control the full specter of learning, both

---

[239] *Id.*
[240] *Id.*
[241] CHILDRESS, *supra* note 2, at 97.
[242] *See* Vance, *supra* note 238.
[243] *Id.*
[244] *Id.*
[245] *Id.* at 100.
[246] *Id.*

in and beyond virtual society, regardless of differences in "role specific knowledge."[247] This is readily apparent in the financial incentives that mega-tech corporations, like Google and Facebook, have in influencing the offline behavior of data users based on their online data records.[248] As Zuboff opines, this command and control "breaks with the old justifications of the invisible hand and its entitlements."[249] Avoiding the invisible hand of government, which Hayek championed, ought not to be replaced by the visible hand of surveillance capitalists who dominate virtual markets in which the vast majority of participants do not engage freely. [250]

Surveillance capitalism in internet markets is distinguishable from the modernity underlying pre-internet markets in key respects. The first modernity in pre-internet markets was in the employment market with involved organic reciprocity between employees and customers of interacting firms. The second market modernity was prefaced upon an interface between labor and money.[251] The third market modernity was embodied in the shareholder-value movement.[252] The fourth modernity eventuated after the invention of the internet.[253] It was created by surveillance capitalism in which human experience constituted a commodity to the business model of surveillance corporations. Cynically articulated, "products and services are merely hosts for surveillance capitalism's parasitic operations."[254] Surveillance capitalists no longer relied on people as consumers because the "users" of their data products were now the raw material for a digital-age production process aimed at new business customers.

---

[247] *Id.*
[248] *See* WALTERS ET AL., *supra* 79.
[249] ZUBOFF, *supra* note 31, at 499.
[250] SOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 497 (2019) *reprinted in* Soshana Zuboff, *The Road to Digital Serfdom? The Visible Hand of Surveillance Capitalism*, PROMARKET BLOG (October 22, 2019), https://promarket.org/road-to-digital-serfdom-surveillance-capitalism-visible-hand/.
[251] ZUBOFF, *supra* note 31, at 514.
[252] *Id.* at 514.
[253] *Id.*
[254] *Id.* at 500.

However, the fourth modernity is not entirely new. The conception of human experience constituting a commodity in the business model of surveillance capitalists is loosely comparable to the commodification of workers already at the second stage of modernity. The distinctiveness of data surveillance from the commodification of workers is that regulatory limitations on what data can be harvested is restricted to personal data; however, consent to the use of that data remains somewhat obtuse.

The fourth stage of post-internet modernity is unique in a key respect. Data corporations that access the responses of data subjects in order to determine the functionality of a product being marketed does not, in itself, violate their personal data. However, once that person's name and identifiable data is used, the threshold of what is acceptable as data usage has been passed. This distinctiveness of this post-internet modernity difference arises from the distinction between data corporations that use personal data anonymously, and by naming or otherwise identifying the data subject without that person's consent. Identifying a data subject by name is increasingly subject to state or regional regulation, such as through the EU's GDPR's protection of the data subject's "right to be forgotten", even though the nature of consent to use that data remains unresolved. The obstacle is to determine not only the nature of consent to use a person's personal information, but also its boundaries. Neil Richard and Woodrow Hartzog espouse three forms of consent.[255] These include unwitting consent, coerced consent, and incapacitated consent.[256] However, legal consent, including consent to use personal data, has developed quite a different meaning: namely expressed or implied consent, or consent by ratification. The Council of Europe has also espoused consent as being freely

[255] Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, WASH. U. L. REV. (forthcoming 2019).
[256] *Id.*

given, specific, informed and unambiguous.[257] The problem to determine, inter alia, is when the consent of a data subject is reasonably given, informed and clear.

Divergence over the nature of consent given by data subjects to use their data has led to an imperfect legal framework that has not contributed adequately to the development of a uniform global reality.[258] Zuckerberg's vision of mega-corporations like Facebook becoming a new global church which will "connect the world's people to something greater than ourselves,"[259] is profoundly overstated. A global church is for praying; the internet does not connect us to any deity, nor should it be so construed. What is more contestable is Zuckerberg's view that:

> For the past decade, Facebook has focused on connecting friends and families. With that foundation, our next focus will be developing the social infrastructure for community -- for supporting us, for keeping us safe, for informing us, for civic engagement, and for inclusion of all.[260]

Arguably, this is a welcomed statement of support for a networking infrastructure that bolsters social connectedness.[261] However, this statement of support is suspect, considering that the control of the flow of information is a construction of a social reality which is removed from those who are mostly affected by it, namely, data subjects. Arguably, social connectedness requires the full involvement of society and its infrastructures - the State – to combine and construct a social reality.[262] As it stands, the current connectedness as brought about by surveillance corporations is like putting the fox in charge of the hen house. The problem is that Facebook on one hand encourages such social

---

[257] Convention for the Protection of Individuals with Regard to the Processing of Personal Data art. 5, Jan. 28, 1981, E.T.S. 108.
[258] COUNCIL OF EUR., CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA 31 (2018).
[259] Mark Zuckerberg, *Building Global Community*, FACEBOOK (Feb. 16, 2017, 3:56 PM), https://www.facebook.com/notes/mark-zuckerberg/building-global-community/10154544292806634/.
[260] *Id.*
[261] *Id.*
[262] *Id.*

engagements, but then mines the information and provides or on-sells it to interested parties, such as the now defunct Cambridge Analytica.[263]

However, there are possibilities offered by Facebook and the IoT generally which are of value and cannot be directly dismissed. Zuckerberg states that Facebook - his company - is socially engaged by assisting in building social infrastructure in two ways:

> The first encourages engagement in existing political processes: voting, engaging with issues and representatives, speaking out, and sometimes organizing. Only through dramatically greater engagement can we ensure these political processes reflect our values.
> The second is establishing a new process for citizens worldwide to participate in collective decision-making. Our world is more connected than ever, and we face global problems that span national boundaries. As the largest global community, Facebook can explore examples of how community governance might work at scale.[264]

These aspirations, especially the second one, are laudatory on their face. More expansive participation by "citizens worldwide in collective decision-making" is wholly warranted, and a goal which this article supports. However, again, Zuckerberg portrays surveillance capitalism as attempting to be the leader of both sides of the IoT revolution: championing global social interconnectedness while subjugating that connectedness to mega-data corporations that direct it.

Zuboff, perhaps too pessimistically in drawing on Orwellian thinking, prophesizes:

> The "seventh extinction" will not be of nature but of what has been held most precious in human nature: the will to will, the sanctity of the individual, the ties of intimacy, the sociality that binds us together in promises, and the trust they breed. The dying off of this human future will be just as unintended as any other.[265]

Arguably, if surveillance capitalism can proceed unchecked, Zuboff could be correct in the prediction. However, as many "oracles" in the past have predicted, the end has not appeared yet. Zuboff bases her views of the demise of surveillance capitalism on the writings of Pippa Norris who points to "a global 'democratic recession' or 'deconsolidation' of Western democracies that were long

---

[263] *Facebook's data-sharing deals exposed,* BBC NEWS (Dec. 19, 2018), https://www.bbc.com/news/technology-46618582.
[264] Zuckerberg, *supra* note 259.
[265] ZUBOFF, *supra* note 31, at 516.

considered impervious to antidemocratic threats."[266] However, Pippa Norris, like many others, uses the IoT to publish and is on Twitter, another product and tool of surveillance capitalism.[267] This is not a criticism of Pippa Norris; it is a realization that virtually nobody can function fully in the current social reality without being in one or another way tied to the IoT.[268] This is an unescapable fact that also ensnares those who criticize it.

This paper argues, differently from Pippa Norris, that we are observing an institutional segmentation, namely, the possibility of socially segregated sub-universes of meaning. On one hand, we embrace the IoT and on the other hand, we also attempt to restrict its excesses. The State currently is engaged in a pattern of conduct within society which produces, or attempts to produce, meanings to such questions as: how to control the appropriation by surveillance capitalism of the IoT and how to constrain the excesses employed by those who engage in such surveillance.[269] The result of state regulation of surveillance capitalism to date is an early creation of an objective reality, with the outcome being pioneering regulations such as the GDPR.[270] However, Berger and Luckmann's cautionary note is very well applicable to the operational phenomena of surveillance capitalism at work:

> A body of knowledge, once it is raised to the level or a relatively autonomous sub-universe of meaning, has the capacity to act back upon the collectivity that has produced it. …The important principle for our general considerations is that the relationship between knowledge and its social base is a dialectical one, that is, knowledge is a social product and knowledge is a factor in social change.[271]

However, Berger and Luckman's comments can extend to very different scenarios. One scenario is that, in a virtual world devised by data corporations and adopted into the knowledge base

---

[266] *See* Pippa Norris, *Is Western Democracy Backsliding? Diagnosing the Risks* (Harv. Kennedy Sch. Fac. Res., Working Paper No. RWP17-012).
[267] *See id.*
[268] *See id.*
[269] *See id.*
[270] *See id.*
[271] BERGER & LUCKMANN, *supra* note 7, at 104.

of that society, the resulting socialized universe can implode on the very society that has adopted it.[272] The second scenario envisage that surveillance capitalists, by collecting data, might acquire knowledge which has the capacity to have a reversionary impact on its very producers, by changing them into supplicants to their own creations.[273] The third scenario is that surveillance capitalists that initiate social change are likely to further imbed themselves as insiders in motivating such change, and in relegating society at large into outsiders in their own social domains.[274] A fourth scenario is that, while knowledge is not a creation of the data miner, those miners can use it to continually manipulate the behavior of society.[275]

Berger and Luckman's scenarios, particularly the fourth one, are readily illustrated by data miners dominating the "dialectic" "relationship between knowledge and its social base", notably in sublimating social discourse to social isolation and by subordinating knowledge to the selective disclosure of information.[276] Its orientation is to satisfy the interests of data users only insofar as doing so furthers its own aspirations, whether fair, competitive and legal, or not. Mega-tech corporations like Facebook absorb knowledge by mining data consisting of the social input of its users.[277] That knowledge is not used as a factor in social change; it is used as a commodity.[278] Mega-tech corporations also employ it to accumulate knowledge as a tool to change and modify *their* own structures in order to entice society to act according to *their* reconstruction of knowledge.[279] In effect, social adherence to their reconstruction of knowledge becomes an artefact which they manufacture and then massage from germination to social compliance.

---

[272] *See id.*
[273] *See id.*
[274] *See id.*
[275] *See id.*
[276] *See id.*
[277] *See* Natasha Singer, *What You Don't Know About How Facebook Uses Your Data*, N.Y. TIMES (Apr. 11, 2018), https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html [hereinafter Singer, *What You Don't Know*].
[278] *See id.*
[279] *See id.*

A further illustration of this data process at work is in distinguishing between a receptible of knowledge, such as book, and a user of knowledge, such as an IoT consumer. Just as a book is a receptacle of knowledge, so is the IoT. However, the distinct difference between them is that, unlike a book, the IoT is not only a receptacle of knowledge. It is also a user of the knowledge it has gleaned from the source of that information which it programs, mechanistically, to entice end users to continue "reading" the story, including in e-books. Edith Ramiz pertinently notes "even the once private act of reading is generating data about us, as e-book companies track not just what we read, but also *how* we read – where we start, what passages we skim, reread, or highlight, and whether we actually finish the book we begin."[280]

Zuboff, in her depiction of surveillance capitalism, examines the information Facebook and other tech giants collect and use as a saleable commodity as noted above.[281] The inference from her depiction of how they use knowledge, beyond serving as a receptacle, is comparable to that of Ramiz.[282]

However, personal data is not only important as the "raw material" used by tech-giants. Tech-giants are increasingly marrying their "client bases" to their "databases" not only to determine how we make decisions, but also to induce us to making decisions they prefer, or are paid to prefer.[283] Many of these tactics are comparable to traditional marketing, such as TV marketing based on its special price and splendid appearance of an advertised car. However, data marketers can also massage our personal data without consent, such as to induce us to vote for a political party.[284] Their purpose is to increase their market by exerting control over how we understand and assimilate information

---

[280] *See* Edith Ramirez, Chairwoman, Fed. Trade Comm'n, Keynote Address at the Technology Policy Institute Aspen Forum: Protecting Consumer Privacy in the Digital Age: Reaffirming the Role of Consumer Control (Aug. 22, 2016), https://www.ftc.gov/system/files/documents/public_statements/980623/ramirez_-_protecting_consumer_privacy_in_digital_age_aspen_8-22-16.pdf

[281] ZUBOFF, *supra* note 31.

[282] *See* ZUBOFF, *supra* note 31.

[283] Singer, *What You Don't Know*, *supra* note 277.

[284] *See id.*

about ourselves, including how we relate or are likely to relate to others.[285] At risk is the privacy and security of our personal information. In contention are data surveillance corporations that engage in uncompetitive practice by unfairly seeking advantage over their competitors. At peril are corporations using ever more sophisticated machinery, clandestinely and tenaciously, to limit detection of their unfair, illegal or undemocratic practices, as to avert social condemnation and legal retribution.[286]

Facebook recently revealed its intention to launch a cryptocurrency called Libra in the first half of 2020.[287] Its purpose is to integrate the impending finance sector of its operations with its already enormous client database and allegedly, "to shake up global finance".[288] The Bank for International Settlements recently noted that such a move would create obstacles in financial regulations that surpass those endured during the financial crisis, as Facebook readily crosses geographical and regulatory boundaries.[289]

The result will be is to force regulators to make tenuous choices. On the one hand, the entry of tech-giants as active participants in the cryptocurrency market will increase global competition at the intersection between cryptocurrency and finance. On the other hand, it will facilitate the incorporation of cryptocurrency companies under its leadership that will wield power beyond that exercised by small countries with ever-receding influence over international finance and currency markets. Considering that tech-giants collect information, which is also needed by financial institutions, it is not far-fetched to predict that tech giants will restrict the flow of data in operating its cryptocurrency sector and attempt to extend its reach to other currency sectors. In particular, tech-

---

[285] *See id.*
[286] *See id.*
[287] *See* Kari Paul, *Libra: Facebook launches cryptocurrency in bid to shake up global finance*, THE GUARDIAN (June 18, 2019), https://www.theguardian.com/technology/2019/jun/18/libra-facebook-cryptocurrency-new-digital-money-transactions.
[288] *Id.*
[289] *See* Thomas Fuster, *Die Technologiekonzerne machen sich im Finanzsektor breit – die Bank der Zentralbanken warnt vor den Risiken*, NEUE ZURCHER ZEITUNG (June 23, 2019), https://www.nzz.ch/wirtschaft/facebook-co-technologiekonzerne-draengen-in-finanzsektor-ld.1490742.

giant currency operators like Facebook can be expected to discount the sale of their data and client databases to affiliates, while selling it at inflated prices to a wider market that excludes their currency competitors. The currency tech-giants, along with their affiliates, will use both their databases and client bases to judge the creditworthiness of their clientele more quickly and more easily than in existing currency exchange and financial markets. In having both customer data and their existing databases at multiple points of connection, they will avoid having to engage in intricate and constrained scrutiny of client creditworthiness in the traditional currency sector.[290] Nor will they face such obstacles as anonymity arising in the current cryptocurrency market.[291]

A libertarian response is that the entry of the tech-giants into the cryptocurrency exchange sector will lead to greater market efficiency that will benefit local, regional and international economies.[292] However, it is arguable that the reverse is more likely, namely that less competition will eventuate.[293] The cost of currency transacting will rise as the tech giants grow more dominant, while the economic viability of others in the currency sectors will recede with increased costs and non-competitive turnover rates. The result, at best, will be competition within a largely oligopolistic cryptocurrency market, or the absence of competition in a monopolistic market, namely, one presided over by Facebook.[294]

The practice of tech giants to control competition by excluding competitors is far from a fantasy. Digital platforms that are controlled and widely operated by tech giants are critical means by

---

[290] *See* Charlie Osborne, *Facebook set to launch own brand of cryptocurrency in 2020*, BETWEEN THE LINES (May 24, 2019), https://www.zdnet.com/article/facebook-set-to-launch-own-brand-of-cryptocurrency-in-2020/.
[291] Fuster, *supra* note 289.
[292] *See* EVEN Foundation, *Cryptocurrency: Threat to the Economy or New Possibilities*, CRYPTODIGEST (Jan. 25, 2019), https://cryptodigestnews.com/cryptocurrency-threat-to-the-economy-or-new-possibilities-bc578ed6876d.; *See also* Ian Bogost, *Cryptocurrency Might be a Path to Authoritarianism*, THE ATLANTIC (May 30, 2017), https://www.theatlantic.com/technology/archive/2017/05/blockchain-of-command/528543/.
[293] Bogost, *supra* note 292.
[294] *See* Dina Srinivasan, *The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy*, 16 BERKELEY BUS. L.J. 39, 74-88 (2019).

which they can enter into new sectors, such as finance.[295] Regulatory and advisory bodies are also increasingly realizing that data which is collected by tech-giants can be used to restrict competition, given that surveillance capitalists like Facebook can collect data at minimal costs.[296] In addition, tech-giants are not under any compulsion to on-sell that data to competitors.[297] The Bank for International Settlements is now warning that, due to the collection of data, mega-tech corporations like Facebook can access the exact financial ability of a customer seeking a loan, which is counter to public welfare and the protection of society in general.[298] Tech-giants will be able to protect themselves effectively from traditional competition in the banking and finance sectors which regulators already appreciate.[299] They will also be able to exploit the gaps in a cryptocurrency market that has not yet matured sufficiently to operate efficiently, but would do so over time within a market in which both parties participate in that process of maturation but one of those parties is a tech-giant.[300] The reality is that Facebook will place that maturation on autopilot on airplanes of its own creation, flying in the direction of its own choosing.

The aspiration nevertheless is that, with surveillance capitalism entering the cryptocurrency market, available currency services will expand, while the quality and delivery of those services will improve. The further expectation is that competition laws, among others, will sharpen existing regulations in the sector, including the regulation of currency servicing through the IoT.[301] These aspirations are fanciful for the reasons articulated in this article. Currency services are likely to expand, but they will improve only if that suits the tech-giant entering the market. Regulation of the

---

295 Fuster, *supra* note 289.
296 *Id.*
297 *Id.*
298 *Id.*
299 *Id.*
300 *See* Mike Issac & Nathaniel Popper, *Facebook Plans Global Financial System Based on Cryptocurrency*, N.Y. TIMES (June 18, 2019), https://www.nytimes.com/2019/06/18/technology/facebook-cryptocurrency-libra.html.
301 *See* Allan Tan, *Impact of evolving regulation on IoT in financial services*, FUTUREIOT (Apr. 22, 2019), https://futureiot.tech/impact-of-evolving-regulation-on-iot-in-financial-services/.

cryptocurrency market is unlikely to be materially more effective than at present, so long as tech-giants are able to dissuade such regulation. The easiest way to combat extending regulation is for tech-giants to raise fear among regulators regarding financial instability arising from interference, as currency is a highly sensitive sector of the global economy.[302]

Cautious regulators, concerned about not trammeling developments in financial markets, nevertheless warn about the variety and scope of issues that will stem from technocratic inroads on sensitive currency markets.[303] As Federal Reserve Chair, Jerome Powell, pondered and ultimately, warned about Facebook's proposed Libra cryptocurrency:

> … I just think it cannot go forward without there being broad satisfaction with the way the company has addressed money laundering, all of those things. The number of concerns that I list at the beginning, data protection, consumer privacy, all of those things will need to be addressed very thoroughly and carefully.[304]

However, it appears that the door to Libra is not shut. If Facebook can so proceed, it will undoubtedly change, not only data capturing, but also the very nature and operation of financial markets beyond currency exchanges.[305] Financing of multiple customers can be conducted efficiently and expeditiously online. Facebook already has databases of personal and financial data or can readily gain access to that data; and it can also readily devise sophisticated platforms on which to conduct its currency operations.[306] The entire process will be supported by carefully developed algorithms that

---

[302] *See* Rakesh Sharma, *Can Government Regulation Affect Bitcoin Prices?*, INVESTOPEDIA (June 25, 2019), https://www.investopedia.com/news/can-government-regulation-affect-bitcoin-prices/.
[303] *See* Ryan Browne, *Here's why regulators are so worried about Facebook's digital currency*, CNBC (Sep. 19, 2019, 10:25 AM), https://www.cnbc.com/2019/09/19/heres-why-regulators-are-so-worried-about-facebooks-digital-currency.html.
[304] *See* Max Boddy, *Fed Chair Says Facebook Needs to Satisfy Regulatory Concerns Regarding Libra*, COINTELEGRAPH (Jul. 10, 2019), https://cointelegraph.com/news/fed-chair-says-facebook-needs-to-satisfy-regulatory-concerns-regarding-libra.
[305] See John E. Girouard, *What Does Facebook's Libra Mean For The Future Of Commerce And Currency?*, FORBES (Sept. 19, 2019, 10:35 AM), https://www.forbes.com/sites/investor/2019/09/19/what-does-facebooks-libra-mean-for-the-future-of-commerce-and-currency/#614.
[306] *Id.*

assess financial data that is available or added to customer databases.[307] Risks of default, in turn, will be assessed in light of pre-set criteria based on market, client, financing and currency criteria.[308]

The economic and social consequences of tech giants entering the financial sector, albeit precipitously through the cryptocurrency market, are inevitably far reaching and will impact on virtually everyone's daily lives as currency transactions are conducted on trailblazing online platforms. This impact is especially likely as cryptocurrency evolves into a convenient staple by which to buy and sell goods and services across multiple jurisdictions that adopt divergent currency regulations.[309]

Facebook's prospective venture into cryptocurrency also resurrected significant concern that mega-tech corporations are positioned to undermine market competition.[310] One example is the question of how Facebook will withstand antitrust scrutiny of its entry into an inventive entrepreneurialism sector, sustained by companies like Bitcoin. Snowballing controversy about the alleged antitrust practices of surveillance capitalists has attracted mounting governmental concern, and also reactions.[311] These competitive issues are addressed immediately below.

7. From Data Protection to Anti-Competition

The United States, the EU and Australia have all launched inquiries in relation to breaches of competition laws by Google and Facebook in particular. In Australia the Competition and Consumer

---

[307] *See* Jameson Lopp, *How Will Facebook's Libra "Blockchain" Really Work?*, ONEZERO (June 18, 2019), https://onezero.medium.com/thoughts-on-libra-blockchain-49b8f6c26372.
[308] *See* Gary Gensler, *Examining Facebook's Proposed Cryptocurrency and Its Impact on Consumers, Investors, and the American Financial System*, MIT MEDIA LAB (July 18, 2019), https://www.media.mit.edu/posts/examining-facebook-s-proposed-cryptocurrency-and-its-impact-on-consumers-investors-and-the-american-financial-system/.
[309] *See* @cryptonitecj900, *Where will Cryptocurrency be in the next 5 — 10 years?*, HACKERNOON (Oct. 14, 2019), https://hackernoon.com/where-will-cryptocurrency-be-in-the-next-5-10-years-49bb7faf4fb5.
[310] *See* Samantha Chang, *EU Antitrust Boss Flags Facebook Crypto Libra for Monopoly Risks*, CCN (Sep. 5, 2019), https://www.ccn.com/eu-facebook-crypto-libra-monopoly-risk/.
[311] *Id.*

Commission (ACCC) is examining the alleged abuse of market power identified with the alarmingly fast ascent of digitalization, for which regulators remain ill-prepared.[312]

The ACCC recognizes three competition issues arising from Google's market dominance that are potentially subject to litigation, which include: "Google's privacy policy, the fairness of the contract demanded and bundling data from different sources, from Google searches to DoubleClick to Android phones."[313] The success of the ACCC's inquiry, which will depend upon regulatory practice and how data corporations like Google will respond to such regulation, remains unseen. What is certain is that such regulation is unlikely to radically change the reality of data users who are not prepared to live without the services which tech-giants provide.[314] What is needed is a regulatory system that is transparent, that promotes informed social reactions to exploitive data usage, not limited to threats to the security of personal information.

In truth, we have witnessed only the beginning of the power exerted by tech-giants on society at large, individuals within it, and governments trying to cope with its grand-scale advance. Nor are the limits of its advance evident at this time. The hazard of data intrusion on everyday life is also geometrically greater than pre-IoT intrusions.[315] The evolving reality revolves around the sheer volume, variety, intensity and impact of data surveillance on personal and social life. The further reality is the monumental shift in market practice, notably in gauging, measuring and assessing customer data usage directed at gaining a market advantage in an already uncompetitive market.[316] The current number of competitors in financial markets are extensive. However, it is arguable that

---

312 *See* Asha Barbaschow, *ACCC targets Google and Facebook with five investigations underway*, ZDNET (Aug. 13, 2019, 6:08 PM), https://www.zdnet.com/article/accc-targets-google-and-facebook-with-five-investigations-underway/.
313 John Durie, *Digital gaze turns to competition watchdogs, as ACCC readies report*, AUSTRALIAN (June 26, 2019), https://www.theaustralian.com.au/business/technology/digital-gaze-turns-to-competition-watchdogs-as-accc-readies-report/news-story/5422c54d4b95a5ba929732210bc682dd.
314 *See* Matt Stoller, *Australia Strips Google/Facebook to Their Underwear*, BIG (Aug. 6, 2019), https://mattstoller.substack.com/p/australia-strips-googlefacebook-to.
315 *See* Walters, *Personal Data Law, supra* note 109.
316 *Id.* at 11.

mega-tech corporations like Google and Facebook have greater technological capabilities to collect, measure and assess financial data, and to accurately assess customer reactions to new products and services.[317] These factors are all economic justifications for tech giants like Facebook to provide more cost-effective services that supplement, or even displace traditional players in financial markets. The supporting rationale is that, where commercial sectors face market risks, tech giants like Facebook can build algorithms to predict the extent of those risks and how to avert or minimize them.[318]

However, these assertions fail to address the slippery slope along which tech giants, rather than serve as social saviors, dominate global financial markets. Their expansionism could start with cryptocurrencies, progress to banking and finance, and precipitously, to globalized trade in stocks and bonds. Walters, Zeller and Trackman highlight how there is an ongoing need for regulator(s) to balance the economic needs of the country along with innovation and the protection of personal data and privacy.[319] The authors argue that, that balance, is going to be continually challenged and may never be resolved. In other words, the balance between stifling innovation and protecting people's personal data and privacy, walks a thin line, because innovation is becoming increasingly dependent on large scale dissemination, transfer and trade in all forms of data, including personal data.[320] This trade, not only heightens the potential for privacy breaches, but can also be used to obtain a market advantage.[321]

The salient issue is whether surveillance capitalists have created a revolutionary change in captivating our world order through enticing mechanisms, which are also socially threatening to our

---

317 *Id.* at 12.
318 *See* Keith Wright, *How Facebook AI may help to change the way we shop online in the future*, CNBC (Sept. 15, 2018, 10:01 AM), https://www.cnbc.com/2018/09/15/the-key-to-a-facebook-stock-recovery-an-ai-based-attack-on-amazon.html.
319 *See* Walters, *Personal Data Law, supra* note 109.
320 *See id.*
321 *See id.*

daily lives.[322] Have they subjugated our personal, social and economic existence to their data machinery whose functional capabilities are outside our knowledge base and comprehension? Have they displaced the personalized exchange of information which we conduct in a mutually interactive and inclusive marketplace, such as in deciding when to buy or sell a stock or bond?

This is not to suggest that interaction over the internet, even in this new world of tech-giants, is devoid of social interaction in conveying and receiving information. The new tech world is well able to convey and receive information as well as facilitate dialogue with data subjects elevated into being clients.[323] However, the technological invasiveness upon our daily lives does come at a social price.[324] Data information is widely available and accessible because the tech giants so determine.[325]

Exercising control over tech giants through contract is inevitably dictated by those same giants in providing goods and services on a take-it-or-leave-it basis. Government regulation is potentially ignored by mega-corporations, like Google and Facebook, in this new world order, such as Google's failure to appear before, or comply with an order of, the Supreme Court of New South Wales.[326] More economically powerful than many governments, these tech giants have resources to defy regulations that are too costly for governments to enforce.[327] Governments, too, are often fearful of pushing against formidable adversaries that have every reason to resist regulatory intrusion.[328] Further impeding governmental regulation is the absence of uniform, and indeed compatible, compliance

---

[322] Joanna Kavenna, *Shoshana Zuboff: 'Surveillance capitalism is an assault on human autonomy.'*, THE GUARDIAN (Oct. 4, 2019), https://www.theguardian.com/books/2019/oct/04/shoshana-zuboff-surveillance-capitalism-assault-human-automomy-digital-privacy.
[323] JANNA ANDERSON & LEE RAINIE, STORIES FROM EXPERTS ABOUT THE IMPACT OF DIGITAL LIFE 4 (Pew Research Center, 2018).
[324] *Id.*
[325] Kashmir Hill, *I Cut the 'Big Five' Tech Giants From My Life. It Was Hell*, GIZMODO (July 2, 2019), https://gizmodo.com/i-cut-the-big-five-tech-giants-from-my-life-it-was-hel-1831304194.
[326] See Deborah Cornwall, *Google on contempt charge over reviews*, THE AUSTRALIAN (Jul. 8, 2019), https://www.theaustralian.com.au/nation/google-on-contempt-charge-over-reviews/news-story/a91b54fb41c5578acfbeba5387eb4969.
[327] Interview by Terry Gross with Farhad Manjoo, Columnist, N.Y. Times, on Fresh Air (Oct. 26, 2017).
[328] Iain Murray, *Conservatives should resist the urge to regulate Big Tech*, FOX BUSINESS (Dec. 12, 2018), https://www.foxbusiness.com/technology/conservatives-should-resist-the-urge-to-regulate-big-tech.

requirements across a global tech sector. Added to this is the reluctance of regulators to face off against large-scale corporations whose businesses extend beyond the applicable jurisdiction. This reluctance is accentuated by data corporations that are well positioned to disregard legislated and judicial orders, which are directed at protecting the rights of citizens.[329]

The result is that the so-called free internet marketplace, the echo of liberal autonomy in a post-industrial era, is decisively free for those who control it. The opposite is true for a public that is captive to a mega-tech global market from which they are unable to extract themselves in the virtual world to which they are hostage. The illusion of choice is that we each watch and contribute to activities on the internet that interest us the most. This literal truism ignores that how tech giants present this vast volume of information, often overwhelms their captive audience. Even basic precautions, such as parents wishing to control their children's access to the internet, is subjugated by mega-social platforms that withdraw access to, screening software that parents need to protect their children.[330]

The disturbing reality is that targeting children can have massive economic value to internet service providers. After all, children constitute a geometrically growing proportion of internet users. Children also grow into adult users who pass on their proclivities as internet addicts to their children. Whether children become internet junkies out of choice, or whether they do so under the "adult" influence of internet providers, cannot be resolved absolutely. Some children are more vulnerable to abuse of their personal information than others, for reasons unrelated to their access to Facebook, Instagram, or

---

[329] *Data is Giving Rise to a New Economy,* THE ECONOMIST (May 6, 2017), https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy; OECD PRINCIPLES FOR INTERNET POLICY MAKING (2014).

[330] *See* Sonia Livingstone, *Children: A Special Case for Privacy?* 46 INTERMEDIA 18 (2018); J. C. Buitelaar, *Child's Best Interest and Informational Self-Determination: What The GDPR Can Learn From Children's Rights*, 8 INT'L DATA PRIVACY L. 293 (2018).

Twitter's platforms. The common denominator is that, in encouraging access by children, the internet is more likely to harm those children who are most vulnerable.

8. Where next?

There is no debate that the IoT is here to stay and will be further developed. The question is how far it will be allowed to develop to prevent it from drastically impoverishing the social construction of our reality. What is pressing is the need for a new world order that is widely accepted as a means of protecting an information highway that is designed and patrolled by tech corporations who survey road usage and change it to suit their swelling budgets. However, change is important and changes in public opinion towards the large tech dominance of internet markets is within the bounds of reality. The reality is that governments and their regulators will respond to such changes in public opinion if only to be seen to be responsive to maturing public expectations. Inevitably, albeit unevenly. As Hayek stated already in 1978:

> I am operating on public opinion. I don't even believe that before public opinion has changed, a change in the law will do any good … the primary thing is to change opinions.[331]

The role of public opinion in producing such regulatory advances is critical, without which the legitimation of regulatory change will not be achievable. Legitimation is best described as second order objectifications of meaning, where "the function of legitimation is to make objectively available and subjectively plausible the first order objectivations that have been institutionalized."[332] Arguably first order objectivations include the protection of private data which was institutionalized by judgements

[331] *See* Interview by Robert Bork with Friedrich A. von Hayek, Economist, UCLA Centre for Oral History Research (Nov. 4, 1978).
[332] BERGER & LUCKMANN, *supra* note 7, at 110.

protecting the individual's "right to be forgotten."[333] Succinctly observed are two levels of subjective plausibility:

> First, the totality of the institutional order should make sense, concurrently, to the participants in different institutional processes. Second the totality of the individual's life, the successive passing thought various orders of the institutional order, must be made subjectively meaningful.[334]

Berger and Luckmann also stress that legitimation is needed when an institutional order is to be transmitted to a new generation of participants which is observable from the increased availability of IoT services and the disparate reactions of their users to those services.[335] Again, legislative attempts to draft meaningful data protection legislation is the vehicle to move from one variant of IoT reality to the next. The attempt is not to regulate the IoT as such, but to address the clash between objective and subjective knowledge in constituting an institutional order. Knowledge of the wrong actions to adopt within the structure of the IoT has already been established, namely, the unauthorized and secretive usage of data which surveillance companies gather and sell to third parties. This is especially pertinent to data companies that expose sensitive personal data to expropriation, mining and distribution.

These threats which surveillance capitalism impose on participants on the IoT are not only theoretical. They also constitute practical challenges to "the institutional order legitimated by the symbolic universe in question."[336] In issue is the subjugation of the universe of users of the IoT to the universe conjured up by data corporations.[337] The devil in constructing this everyday person's universe lies in the detail, in how to constitute it both conceptually and practically.[338] As Berger and Luckman observed:

---

[333] *See id.*
[334] *Id.*
[335] *Id.* at 11.
[336] *Id.* at 124.
[337] *Id.* at 135.
[338] *See Id.*

> The alternative universe presented by the other society [the users of the IoT] must be met with the best possible reasons for the superiority of one's own. This necessity requires a conceptual machinery of considerable sophistication.[339]

The seemingly impenetrably struggle is for the state to find that institutional line in the sand by which it mediates between surveillance capitalism and data use in constructing the legitimate borders of reasonable data collection and processing.[340] The related struggle for the State is the reality that mega-data corporations may well resist restrictions on access to and use of their data, even if their transmission of data is declared unlawful.[341] They are also likely to resist regulation by further by moving their corporate infrastructures from purportedly regulatory states to other states that are less intrusive.[342]

In some measure, mega-tech corporations will succeed in these evasive tactics for the reasons highlighted by Zuboff:

> Despite the radical prospects of the "ubiquitous claim" that it will "change everything" technology firms in the US have, thus far, continued their run of relative lawlessness, unimpeded by any comprehensive social or regulatory vision.[343]

Even more disturbing that Zuboff's warning, is this view articulated by an IBM executive:

> You know the amount of data being created on a daily basis – much of which will go to waste unless it is utilized. This so-called dark data represents a phenomenal opportunity … the ability to use sensors for everything in the world to basically be a computer, whether it is your contact lens, your hospital bed, or a railway track.[344]

---

339 *Id.* at 127.
340 John Naughton, *'The goal is to automate us': welcome to the age of surveillance capitalism,* THE GUARDIAN (Jan. 20, 2019), https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook.
341 *See id.*
342 This is typified by Facebook's stated intention to relocate 1.5 billion data users of its services from Ireland to Africa, Asia, Australia and Latin America, in order to avoid the EU's GDPR rules of data protection that apply in Ireland. David Ingram, *Facebook to put 1.5bn users out of reach of new EU GDPR privacy law*, THE IRISH TIMES (Apr. 19, 2018), https://www.irishtimes.com/business/technology/facebook-to-put-1-5bn-users-out-of-reach-of-new-eu-gdpr-privacy-law-1.3466837.
343 ZUBOFF, *supra* note 31, at 209.
344 *See* Bryan Glick, *Executive Interview: Harriet Green, IBM's Internet of Things in Chief*, COMPUTER WEEKLY (Apr. 7, 2016), https://www.computerweekly.com/news/450280673/Executive-interview-Harriet-Green-IBMs-internet-of-things-chie.

Society in a sense will simply become an object in an institutionalized data economy. We will all be commodified as the objects, not the subjects of rights; while data surveillance corporations will direct us on how to eat, sleeping and indeed, breathe.

On the positive side, the struggle for the superiority of society over surveillance capitalism has not been finalized. In the end the question will be "who has the bigger stick" and how it might weald that stick. Arguably one of the cornerstones by which to provide society at large with greater autonomy from corporate dominance, is to imbed a determinable definition of a data subject's consent to the collection and use of personal information. If this is achieved, the result is to arrive at a more reliable determination over when personal data is freely available, and when it cannot be used as a commodity because of the absence of the data subject's consent.

A related question is to determine how society at large is to appropriate and internalize individual rights to the protection of their protection of their right to be left alone. Under consideration, here, is to delineate restrictions on surveillance capitalists, such as by delineating the consent to use personal data, and to institutionalize a pervasive conception of consent which extends beyond both domestic laws and the demands of mega-tech corporations.

9. Internalization of reality

Berger and Luckmann have argued that society exists both in an objective and subjective reality; and that this process of realization is composed of three moments, namely, externalization, objectivation, and internalization.[345]

The internalization process is of great importance today as the IoT has already influenced the subjective reality through digital distractions.[346] These distractions are expressed as cognitive

[345] ZUBOFF, *supra* note 31, at 149.
[346] Joseph Firth et al., *The "online brain": how the Internet may be changing our cognition,* 119 WORLD PSYCHIATRY 120 (2019), https://onlinelibrary.wiley.com/doi/epdf/10.1002/wps.20617.

offloading in which information is not retained in our memory because it is stored online.[347] Samuel Greengard warned "[a]lready, serious concerns exist about whether this technology will dumb down society, lead to greater inequality, and expand the digital divide."[348] He then poses the question "[W]hat about the growing problem with digital distraction? . . . How do we approach security and privacy in an era where almost no movement or activity goes unnoticed or unrecorded?"[349]

Of concern is that the IoT has created a machine reality by quantifying success or failure, by providing "likes" or "followers" metrics.[350] In addition, a stream of prompts entices the users to follow "the bouncing ball". In essence:

> Given we have most of our world's factual information literally at our fingertips. This appears to have the potential to changing the way in which we store, and even value, facts and knowledge in society and in the brain.[351]

The central issue is in how to internalize the reality of knowledge and understanding within society in which that reality is multi-faceted and not conceived as a constant or as impervious to differences in understanding. The important point noted by Berger and Luckmann is that, "to be in society is to participate in its dialectic."[352] That social dialectic, in turn, is expressed through an evolving continuum in which society internalizes a dialectic in which individuals are participants.

> In the life of every individual, therefore, there *is* a temporal sequence, in the course of which he is inducted into participation in the societal dialectic. The beginning point of this process is internalization.[353]
>
> Berger and Luckman note further that "internalization in this general sense is the basis, first, for an understanding of one's fellowmen and, second, for the apprehension of the world as a meaningful and social reality."[354]

---

[347] *Id.*
[348] *See* SAMUEL GREENGARD, THE INTERNET OF THINGS (MIT Press, 2015).
[349] *Id.*
[350] ZUBOFF, *supra* note 31.
[351] ZUBOFF, *supra* note 31.
[352] BERGER & LUCKMANN, *supra* note 7, at 149.
[353] *Id.*
[354] *Id.* at 150.

The problem is that the perception of the IoT is not really to understand ones' fellow human beings, but rather to measure one's standing among others, such as through the "likes" and "followers" on Facebook.[355] The unfortunate issue is that a true understanding of the reality of life has been lost, as the verification of messages and spread of fake news intermingles with the actual reality of life.[356] This loss of the reality of life is exacerbated by such examples as a city-country divide in which the city dweller questions whether milk actually comes from cows and not in powder form produced by factories. The issue, in its most simplistic form, is that society and the State have still not reached the objective phase of understanding, let alone passed through the subjective phase. It appears that the State still intends to protect personal data through legal instruments such as the GDPR but remains cognizant of the desire to conduct surveillance of people's movements through mechanisms such as those devised and applied by Facebook.[357]

Berger and Luckmann note it is possible "to conceive of a society in which no further [socialization] takes place after primary [socialization]."[358] The fact is Facebook and corporatized surveillance exert a great influence on how society both interacts and sees the world; a real possibility is that no further socialization will take place. Many people believe to not be connected through Facebook and to not communicate through Twitter, in "grammatical-less" sentences, means to be cut out of life. Berger and Luckmann also discuss a similar possibility, noting that "such a society would, of course, be one with a very simple stock of knowledge."[359] The study by researchers at Oxford, Kings College London, Manchester, Harvard and Western Sydney universities all support this view. Time spent online could

---

[355] *See generally* Tobin Brogunier, *4 Reasons Why Social Media Has Become So Toxic and What to Look for Next*, ENTREPRENEUR.COM (Feb. 22, 2019), https://www.entrepreneur.com/article/328749.
[356] *See generally* Katy Steinmetz, *How Your Brain Tricks You Into Believing Fake News*, TIME (Aug. 9, 2018), https://time.com/5362183/the-real-fake-news-crisis/.
[357] *See generally* Andrew Rossow, *The Birth Of GDPR: What Is It And What You Need To Know*, FORBES (May 25, 2018, 7:32 AM), https://www.forbes.com/sites/andrewrossow/2018/05/25/the-birth-of-gdpr-what-is-it-and-what-you-need-to-know/#57e8141355e5.
[358] BERGER & LUCKMANN, *supra* note 7, at 157.
[359] *Id.* at 157-58.

produce "acute and sustained" alterations to the brain,[360] altering or even reducing the stock of knowledge in society. However, society is far more complex than the IoT and the surveillance capitalist assume. Hence, the maintenance and transformation of subjective reality in contrast to objective reality is never complete and every viable society "must develop procedures of reality maintenance."[361]

Arguably, data protection legislation is the mechanism to safeguard the balance between objective and subjective reality.[362] Berger and Luckmann find that internalizing socialization is not only justifiable but also inevitable.

> Primary [socialization] internalizes a reality apprehended as inevitable. This [internalization] may be deemed successful if the sense of inevitability is present most of the time, at least while the individual is active in the world of everyday life. But even when the world of everyday life retains its massive and taken for granted reality *in actu*, it is threatened by the marginal situation of human experience that cannot be completely bracketed in everyday activity.[363]

It is true that the IoT is perceived as an inevitable development that shapes reality. What is not yet clear is how the IoT is applied to everyday life. Simple observation will show that Facebook users exhibit a tendency toward distraction, such that their face to face "conversation" is split between looking at their devices and continuing a conversation.[364] In effect, the reality of the moment is interrupted by the desire to keep abreast with the world presented by Facebook.[365] In sum, "digital distraction" encourages "cognitive offloading" which means that information does not need to be stored in one's memory because it is stored online.[366]

---

[360] *See* Mark Bridge, *Instagram society could alter children's brains, scientists warn*, THE AUSTRALIAN (June 7, 2019), https://www.theaustralian.com.au/world/the-times/instagram-society-could-alter-childrens-brains-scientists-warn/news-story/313303e905cc6a0eeb13ad7991b198af.
[361] ZUBOFF, *supra* note 31, at 167.
[362] *See Handbook on european data protection*, EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2018), https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf; Steven Chabinsky & F. Paul Pittman, *USA: Data Protection 2019*, ICLG.COM (March 7, 2019), https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa.
[363] ZUBOFF, *supra* note 31, at 167.
[364] Henry H. Wilmer, et. al., *Smartphones and Cognition: A Review of Research Exploring the Links between Mobile Technology Habits and Cognitive Functioning*, 8 FRONT PSYCHOL. 605 (2017).
[365] *Id.*
[366] Benjamin C. Storm, et. al., *Using the Internet to access information inflates future use of the Internet to access other information*, 25 MEMORY 717 (2017).

The storage of personal information online, however, can produce a more insidious result. Cyber- bullying has an important, and arguably misguided, effect in reducing "likes" and "followers," but not necessarily the well-being of victims of social media conducted through Facebook, Twitter or Instagram. A potential solution is to turn off the IoT and concentrate on the face to face communications in which words spoken on Facebook are not repeated or can be rebutted immediately, without having a lasting effect on our brains. It is unsurprising that research shows that:

> Given we now have most of the world's factual information literally at our fingertips, this appears to have the potential to begin changing the ways in which we store, and even value facts and knowledge in society, and in the brain.[367]

The issue is that accessing facts and acquiring knowledge appears to have been overtaken by the structure of the IoT that generates short "takes" instead of reasoned and well laid out information. This is evidenced by the fact that even Presidents can take to twitter to communicate "facts" that, on very close examination, consist of some facts, but also contain "propaganda." It is thus no surprise that the term "fake news" has been created.[368] Accordingly, society has not perceived the taken-for-granted reality of the IoT as a drastic shift from what was perceived to be reality before the IoT. Society has also not treated as drastic the social revolution which arguably is the IoT and the emergence of surveillance capitalism.[369] The likely inference is that society at large does not regard the protection of personal data as being as important as using Facebook or Google, platforms people are not willing to sacrifice. For Berger and Luckmann, an individual's identity is the important driver in constructing personal reality.

> To retain confidence that he is indeed who he thinks he is, the individual requires not only the implicit confirmation of this identity that even casual everyday contacts will supply, but the explicit and emotionally charged confirmation that his significant others bestow on him.[370]

---

[367] Firth, *supra* note 346, at 122.
[368] Donald J. Trump (@realDonaldTrump), TWITTER (Sept. 15, 2019), https://twitter.com/realdonaldtrump/status/1173371482812162048?lang=en.
[369] ZUBOFF, *supra* note 31, at 170.
[370] *Id.*

This confirmation of an individual's identify is a real problem in the creation of reality. Significant others, before the IoT, were those the individual knew or those who knew him. Facebook has changed that reality by elevating everybody reading Facebook messages as being significant others. The "likes" and "followers" and the 'message going viral" are all measuring tools in evaluating one's confirmation of that identity.[371]

However, certain attributes of reality from the 1960s has not changed the reality created by the IoT. In any period in a society "the most important vehicle of reality maintenance is conversation."[372] Conversation still continues. What has changed is how conversation is maintained.[373] Conversation on Facebook is not face-to-face, but conducted through a mechanical instrument, namely, the Facebook reality.[374] It is here where Berger and Luckmann are incorrect in insisting that a "massive" change in reality has occurred through "the accumulation that can afford to be casual".[375] They insist that "the massivity [in change] is achieved by the accumulation that *can afford to be casual* precisely because it refers to the routines of a taken for granted world."[376] The IoT reality is quite different in a material respect to the reality maintained by Berger and Luckmann. Any posting on Facebook or any other media is not "casual": it stays forever, such as when trolls identify comments made by aspiring politicians two or three years before which result in their withdrawal or resignation.[377]

---

371 *The definition of vanity metrics and how to identify them*, TABLEU (last visited Oct. 24, 2019), https://www.tableau.com/learn/articles/vanity-metrics.
372 ZUBOFF, *supra* note 31, at 172.
373 *Messages Matter: Exploring the Evolution of Conversation*, FACEBOOK NEWSROOM (Nov. 16, 2017), https://newsroom.fb.com/news/2017/11/messages-matter-exploring-the-evolution-of-conversation/.
374 *About Messaging*, FACEBOOK, INC. (last visited Oct. 24, 2019), https://www.facebook.com/help/1071984682876123/?helpref=hc_fnav.
375 ZUBOFF, *supra* note 31.
376 *Id.*
377 *See generally* Aimee Picchi, *OK, you've deleted Facebook, but is your data still out there?*, CBS NEWS (Mar. 23, 2018), https://www.cbsnews.com/news/ok-youve-deleted-facebook-but-is-your-data-still-out-there/; *What happens to content (posts, pictures) that I delete from Facebook?*, FACEBOOK, INC. (last visited Oct. 24, 2019), https://www.facebook.com/help/356107851084108.

The routine of the-taken-for granted world also extends communication beyond the trusted personal circle to the world at large. In so doing, personal data is sacrificed for the convenience of being "connected" and "liked" and leads to uncontrolled anonymous postings by people unconnected to the target.[378] As reported in The Guardian newspaper, "Ana had few friends and was lonely. She sought to connect with peers via YouTube, Instagram, Facebook, Snapchat and other platforms only to end up bullied – targeted for sexual innuendo and threats. One comment on her YouTube channel expressed a desire to "have her executed."[379]

Ana was subsequently murdered.[380] Berger and Luckmann, however, have expressed the view that "in order to maintain subjective reality effectively, the conversational apparatus must be continual and consistent."[381] They are justified in stating that the IoT, specifically Facebook, is "continual." However, it is questionable whether that conversation is "consistent." The reality is that the threat of inconsistency cannot be avoided, as the conversation is conducted in an unknown IoT environment, unlike in a face-to-face environment in which conversationalists can participate in a communication [that] is "consistent."

The IoT allows anybody unconnected to the individual's subjective reality to comment through postings, thereby changing the conversational environment from a known one, to the world at large. Subjective reality, Berger and Luckmann add, "is thus always dependent upon specific plausible structures."[382] The problem with that reasoning is that there may no longer be "plausible structures", due the disintegration of the milieu needed to confirm one's identity. Berger and Luckmann respond by arguing that a "plausible structure" is both formal and functional. "One can

---

[378] ZUBOFF, *supra* note 31.
[379] Rory Carroll, *Ireland left horrified by Ana Kriégel's murder in a derelict farmhouse*, THE GUARDIAN (June 23, 2019), https://www.theguardian.com/world/2019/jun/23/ana-kriegel-ireland-horrified-teenage-murder-in-derelict-farmhouse.
[380] *Id.*
[381] ZUBOFF, *supra* note 31, at 174.
[382] *Id.* at 174.

maintain one's Catholic faith only if one retains one's significant relationship with the Catholic community."[383] However, it is not reasonable to insist that the structure of the relationship between Facebook and its users is "plausible". Facebook is not itself a community: it is a mechanism to distribute and record comments, but also a "laboratory" for social transformation. As such, has it replaced the individual's human world with another one created and managed by machines? Or is there "an ongoing dialectic" that continues to unfold throughout the individual's existence in society despite structural changes in communication since the invention of the IoT? Berger and Luckmann prioritize an ongoing dialectic that inferentially prevails over the mechanical displacement of that dialectic:

> There is an ongoing dialectic, which comes into being with the very first phases of [socialization] and continues to unfold throughout the individual's existence in society, between each human animal and its socio-historical situation. Externally, it is a dialectic between the individual animal and the social world. Internally, it is a dialectic between the individual's biological substratum and his socially produced identity.[384]

It is arguable that the world of communication, as envisaged in 1966, remains intact today, despite the advent of the IoT. The basic "dialectic" has not changed, other than the socio-historical context. The IoT and surveillance capitalism have introduced a new social reality based on machine power that has amassed personal information which mega-tech corporations use as a commodity to subtly change social structures.[385] However, this commodification of the human subject's personal space does not foreclose an "ongoing dialectic" nor the continuity of social conversation. Nor does maintaining an ongoing social dialectic preclude the adoption of mechanical measures that, purposefully or otherwise, influence social dialogue.

A residual question is whether formal institution, such as parliaments, can change the structures that underlie social dialogue. Can a parliament influence and limit the effects of the IoT on

---

[383] BERGER & LUCKMANN, *supra* note 7, at 174.
[384] *Id.* at 201.
[385] Jacob Silverman, *How Tech Companies Manipulate Our Personal Data*, N.Y. TIMES (Jan. 18 2019), https://www.nytimes.com/2019/01/18/books/review/shoshana-zuboff-age-of-surveillance-capitalism.html.

social structures, whether by perpetuating, resurrecting, modifying, or abandoning them? Berger and Luckmann respond emphatically: "Parliament can do anything except make men bear children."[386] Is the same response true in relation of Parliament attempting to protect personal data? Only time will tell.

10. Conclusion

The pervasive questions remain: what has been learnt about the evolving reality of the Internet of Things, and how does one address the impact of the IoT on society, as on law? Specifically, what legal framework is needed to protect privacy interest in a hyper-connected future world?

The answer is very little has been learnt, yet. Data consumers continue to use the IoT, entrusting data to it. In effect, they have perceptibly swapped privacy for the ability to be "connected" with everybody. The observation is that a couple or more people at a dinner table often do not communicate extensively with each other, instead opting for community via Facebook and other apps, that is, with the world at large. The sharing of personal information with selected individuals or groups is disappearing. A casualty is the ability to observe and gauge the human responsiveness to communication. Once on the Net, information is there forever and never to be changed. Surveillance capitalism is not interested in vigorous intellectual debates "about life", but on measuring the responsiveness of members of society to advertising, or to the likes or dislikes of ideas. It is not the refined and informed discussion that data surveillance corporations consider important; it is what can be sold and where the economic benefit lies: in mining data.

Change is inevitable. Nor can the IoT be wished away; it is here to stay forever. The development and knowledge of the IoT has a number of consequences. The relationship between reality-defining and reality-producing processes has created a type of inertia among the users of the

[386] BERGER & LUCKMANN, *supra* note 7, at 201.

IoT products developed by surveillance companies. Habitualization and institutionalization in themselves limit the flexibility of human actions. But at the same time, a conflict between the State and surveillance capitalism has arisen. At issue is determining how drafting new legislation will create the equilibrium between data surveillance and the personal data of human subjects which those that conduct such surveillance can access, use and arguably, misuse. At issue, too, is the difficulty of lawmakers to require that data collectors and processors enable the spiraling reality of data exposure to be understood, including those whose personal information is used without consent, anti-competitively, or for illicit and/or undemocratic purposes.

A key issue is that a solution to the lack of public understanding of the new reality is only achievable if society at large, not only corporate self-regulators and legislatures, agrees on how to use the IoT. It is not the internet that destroys humanity; it is rather how we, in society, use that data. It helps that the crucial element of the use of the IoT, namely consent, is being defined and embedded in legislation. Consent is arguably the key to a proper and informed use of the IoT as a mechanism to enhance public knowledge and understanding.

Surveillance corporations are required to secure the informed consent of data subjects to use their personal information, and breaches of those contracts are legally enforced. However, surveillance mechanisms are also means of social intrusion, invading the privacy of users from whom consent is improperly secured or not secured at all. A salient problem is how legal regulators can both detect and resolve the practice of surveillance capitalists transmitting personal data of millions of users for illicit purposes, including violations of social morality. The complexity here is that, while the data surveillance is often conducted globally, social morality is often conceived and construed quite differently from one jurisdiction to the next. Zuboff adopts an insightful view of the impact of the Age of Surveillance Capitalism upon an albeit abstract conception of a transnational moral and political order:

> Age of Surveillance Capitalism will meet the same fate as it teaches us how we do not want to live. It instructs us in the irreplaceable value of our greatest moral and political achievements by threatening to destroy them.[387]

Zuboff's emphasis on surveillance capital threatening the very core of our moral and political life is distinctly pessimistic. However, whether or not she overstates the threat, her message still functionally serves as a warning signal to regulators and human subjects, of a potentially disastrous consequence arising from societal passivity and governmental inaction.

Berger and Luckmann, in their 1966 theoretical work on the social construction of reality well predating the evolution of surveillance capitalism, insist that a change in the social construction of reality will and must happen.[388] However, the question must be asked whether their theory of a social construction of reality is still an applicable model. Has the IoT brought about a social change so profound that the reality of life is constructed by tech-giants, and hence by machines of their creation and operation?

A response to this question is: Why worry what surveillance capitalism gains from their ownership of parts of the IoT if hackers can access really sensitive personal data which the IoT currently cannot prevent. Material changes in the social construction of reality will also eventuate only if both internet users and government regulators realize that personal data and the IoT are not a match made in heaven. Indeed, they are a mismatch that alters society's sense of what is real and important. It is also still true to say that books capture and conserve the reality of the time better and more accurately than the IoT. Karahasan argues that we cannot stop those who attempt to reduce our reality to the "today", but it is false to believe that there is nothing that can be done because books are our protection against barbarians and barbarism.[389] Whether the IoT can protect against barbarism, and as

---

[387] ZUBOFF, *supra* note 31, at 524.
[388] BERGER & LUCKMANN, *supra* note 7.
[389] *See* Dževad Karahasan, *Menschen brauchen Bucher*, NEUE ZURCHER ZEITUNG (June 24, 2019), https://www.nzz.ch/meinung/menschen-brauchen-buecher-sie-verwurzeln-uns-in-der-zeit-ld.1481327.

disemboweling themselves as the perceived source or sponsorship of barbarianism, is an open question. What is arguable, in response, is that the growing social awareness of the barbarization of their personal information constitutes a serious threat to their personal security and social wellbeing. Insofar as this social awareness leads to more restrictive access to, and use of, suspect data platforms, data surveillance corporations are incentivized to respond by modifying their surveillance practices to appease hesitant users of their platforms. However, insofar as social resistance to surveillance of their personal data causes data corporations to lose profits, it is expected that surveillance capitalism will shift from free, to cost-based access to their platforms.[390] This has already occurred in the social media sector, such as in costs associated with use of Instagram,[391] and likely other providers of such services.

A question still remains to be answered: Will real knowledge revert to, and once again, rest with, those who own and write books? The point is that to write books requires a capacity to memorize not just fractions of knowledge, but to understand knowledge that is acquired through life experiences and contemplations, and not by relying on quick grabs on Twitter. The interrelated question is to identify what are the "things" on the Internet of Things. To what extent are we, human subjects, all "things" on the Internet? And are we the "things", not only of data storage and selective distribution outlets, but of other "things" including other individuals who feed on our personal frailties? A disconcerting response is that the moving from an evolving to the overhauling of reality "signals the metamorphosis of the digital infrastructure from a thing we have to a thing that has us."[392] Changing the response to this metamorphosis requires changing how the internet of people distinguish themselves from the internet of things, and how willing governments are to support that distinction.

---

[390] ZUBOFF, *supra* note 31.
[391] Zoe Kleinman, *Ad-free social network Vero to charge subscription fees*, BBC NEWS (Feb. 26, 2019), https://www.bbc.com/news/technology-47375176.
[392] ZUBOFF, *supra* note 31, at 204.

Differentiating between the internet of things and the internet of real person is essential in responding to surveillance capitalism that has moved us, the people, that much closer to being subjects of those tech companies that self-regulate the internet.[393] The enemy is that we are creatures of the internet in part because we habituated, not only by an inclination to learn about life and people, but also curiously about malice towards other communities and individuals, such as based on race, gender and class. We can become increasingly cognizant of our human failings. We can become more aware of those who play to the frailties within us. We can achieve a great deal more if we, as a society of data users, are supported by those who have hitherto exploited our frailties, and by regulators that to date have done little to dissuade such exploitation. That entails regulators, with our support in detecting violations personal data violations, to dissuade surveillance capitalists that, without intervention, will have greater economic incentives to continue to play on our human deficiencies. If they are to benefit, that may well lead to greater access public to higher quality data, more reliable and better serviced data platforms. If they gain at the expense of most of us, that is not a social good worth defending, but one to resist strenuously. The boom is not down on social indignation, nor on legal reaction to ever more inventive surveillance and abuse of our personal lives. Still, that boom is lowering, perceptibly, and in need of raising, including in response to a data-generating world created by a few, for application to many.

[393] *Id.*