INSTITUT DE LA SOUVERAINETÉ NUMÉRIQUE

afnic

INTERNET OF THINGS & DIGITAL SOVEREIGNTY

INDUSTRIAL PROSPECTS AND REGULATORY CHALLENGES

INTERNET OF THINGS & DIGITAL SOVEREIGNTY

INDUSTRIAL PROSPECTS AND REGULATORY CHALLENGES

Coordinated by Bernard Benhamou
Secretary-General of the Institute
of Digital Sovereignty (ISN)

This report was produced by the Institute of Digital Sovereignty (ISN)
in partnership with Association Française pour le Nommage Internet en Cooperation (AFNIC)
and it was coordinated by Bernard Benhamou, Secretary-General of the ISN
bernard.benhamou@souverainetenumerique.fr.

The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.

Mark Weiser, *former chief technology officer at Xerox's Palo Alto Research Center (Parc 1991)*[1]

The Internet of Things isn't just about locating objects and using them to sense the surrounding environment - or accomplish automated tasks. It's a way to monitor, measure, and understand the perpetual motion of the world and the things we do. The data generated by the IoT will provide deep insights into physical relationships, human behavior, and even the physics of our planet and universe.

Samuel Greengard,
The Internet of Things,
MIT Press (2015)[2]

1. *The Computer for the 21st Century* (Mark Weiser, Scientific American 1991)
courses.cs.washington.edu/courses/cse440/07au/readings_files/Weiser-Computer21stCentury-SciAm.pdf

2. The Internet of Things Samuel Greengard (MIT Press, 2015)

CONTENTS

INTRODUCTION

Over a few years, the application fields of '*Internet of Things*' (*IoT*) technologies have expanded steadily: from optimization of industrial processes to energy management, from autonomous transport to environmental control, from agriculture to health safety. These technologies contribute to the development of new industrial sectors and help implement public policies, particularly in the environmental field. Governments', administrations' and local authorities' projects already include many components based on the Internet of Things, whether these be transportation infrastructures, health care or smart cities[3]. Connecting all the objects that surround us to the Internet is a strategic objective for technology players but also a political and industrial challenge for the European Union.

For European Union member states, digital sovereignty is no longer a question of control over their own information infrastructures or independence from non-European technologies. It is also about ensuring that *IoT* technologies do not jeopardize our fundamental freedoms or the very foundations of our social welfare systems. Indeed, the *IoT* also raises new questions about the intrusion of these technologies into citizens' privacy and new threats they could pose to the functioning of democracies. For France as for Europe, the aim now is to create technologies and regulations that will allow an Internet of Things to develop in accordance with principles shared by Europeans. These technologies could soon condition the way citizens exercise their fundamental rights and freedoms and, more generally, how rule of law and democracy are defined.

3. *Internet of Things: The New Government To Business Platform a Review of Opportunities, Practices, and Challenges* (Banque Mondiale, 3 novembre 2017) http://documents1.worldbank.org/curated/en/610081509689089303/pdf/120876-REVISED-WP-PUBLIC-Internet-of-Things-Report.pdf

Digital sovereignty has become a strategic objective for the European Commission in terms of *IoT* technologies development. For Thierry Breton, European Commissioner for Internal Market, the Union must stop the naivety which characterized its past actions in the technological field:

> We will also strengthen the protection of our information space, which is still too largely dominated by non-European geo-economic players, and establish the legal framework for a single European data space. Europe missed the first wave of the personal data economy. It will not miss the enormous potential of industrial data that is whetting the appetite of the GAFAMs and other BATXs. We are also working to secure our 5G networks, because our critical infrastructures cannot be vulnerable. And we are finalising a new cyber security strategy – a "European Cyber Shield" – to take into account the arrival of billions of connected things, from cars to children's toys, healthcare devices and household appliances. Industrial data, 5G, cyber security and computing power will condition our sovereignty for decades to come.[4]

4. *Europe: The End of "Naïvety"*, Thierry Breton (European Commission Sept 10, 2020) https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/europe-end-naivety_en

1
TECHNOLOGIES AND EVOLUTIONS OF CONNECTED OBJECTS

First generations of connected objects available to the general public were complex electronic devices (smartphones, tablets, smart speakers, connected cars, etc.), while the other market of IoT technologies was based on sensors, *RFID* chips and connected devices for monitoring, tracking and optimizing production and logistics processes. These '*smart factory*' technologies currently represent one of the world's largest markets for the Internet of Things. The *Gartner* research firm predicts that by 2024, at least 50% of enterprise applications in production will be IoT-enabled.[5]

In the future, we could witness a convergence of industrial Internet technologies and connected objects technologies beyond traditional electronic devices. This new phase in the development of the *IoT* could bring about a rise in services related to connected products and beyond to the creation of *'connected environments'*. The Internet of Things has been described by many different names depending on the origin of the technologies involved or of industrial strategies. Some of these names are registered trademarks and, beyond connected devices or products, they usher in the evolution towards a '*connected world*' (cf. table 1).

5. *Gartner's IT Automation Predictions for 2020* (Advanced Systems Concepts - IT Automation Without Boundaries 2020) info.advsyscon.com/it-automation-blog/gartner-it-automation

INTERNET OF THINGS (IoT) SYNONYMS AND ORIGINS

- **Machine to Machine** (M2M, Theodore Paraskevakos, 1968[1])
- **Ubiquitous Computing** (Mark Weiser, 1993[2])
- **Internet of Things** (IoT, Kevin Ashton, 1999[3])
- **Ambient Intelligence** (*Philips* 1998[4]/*Commission européenne,* 2001[5])
- **Everyware** (Adam Greenfield, 2006[6])
- **Object Hyperlinking** ou **Phylinking** (*Microsoft* Tags, 2009[7])
- **Web of Things** (*Ericsson,* 2012[8])
- **Smarter Planet** (*IBM,* 2008[9])
- **Industrial Internet** (*General Electric,* 2012[10])
- **Programmable World** (*Wired Magazine,* 2013[11])
- **Internet of Everything** (*Cisco,* 2013[12])
- **Physical Web** (*Google,* 2014[13])
- **Systèmes cyber-physiques** (Programme *Industrie 4.0,* 2015[14])
- **OMO (Online-Merge-Offline), O2O (Online-to-Offline)** (Kai-Fu Lee, 2018[15])

1. *The machines are coming: how M2M spawned the internet of things* (John Kennedy, Silicon Republic, May 18, 2016) www.siliconrepublic.com/machines/m2m-cutting-edge-machines-internet-of-things-explained
2. *Some Computer Science Issues in Ubiquitous* Computing (Mark Weiser CACM, July 1993) graphics.stanford.edu/courses/cs428-03-spring/Papers/readings/General/Weiser_Ubi_CACM93.html
3. *Interview with Kevin Ashton – inventor of IoT: Is driven by the users* (Smart Industry Feb 11, 2018) www.smart-industry.net/interview-with-iot-inventor-kevin-ashton-iot-is-driven-by-the-users/
4. F*rom Devices to "Ambient Intelligence": The Transformation of Consumer Electronics presentation* by E. Zelkha, B. Epstein, S. Birrell, C. Dodsworth and R. Pieper (Philips Research 1998) epstein.org/wp-content/uploads/DLR-Final-Internal.ppt
5. *Scenarios for Ambient Intelligence in 2010* (European Commission, Feb 2001) cs.millersville.edu/~bliffick/cs425/docs/ISTAG-Final.pdf
6. *Everyware: The Dawning Age of Ubiquitous Computing* (Adam Greenfield ,Ed. New Riders 2006)
7. *Microsoft and Object Hyperlinking* (Dr Dobbs, Jan 6, 2009) www.drdobbs.com/architecture-and-design/microsoft-and-object-hyperlinking/228701102
8. *A Social Web of Things* (Ericsson, 2012) www.ericsson.com/en/blog/2012/4/a-social-web-of-things

9. *IBM Smarter Planet* 2008
www.ibm.com/ibm/history/ibm100/us/en/icons/smarterplanet/
10. *Industrial Internet* (General Electric, 2012)
www.ge.com/europe/industrial-internet
11. *In the Programmable World, All Our Objects Will Act as One* (Wired Magazine, May 14, 2013)
www.wired.com/2013/05/internet-of-things-2/
12. *The Internet of Everything Global Private Sector Economic Analysis* (Cisco 2013)
www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoE_Economy_FAQ.pdf
13. *The Physical Web* (Scott Jenson, Google 2014) github.com/google/physical-web
14. *Germany Industrie 4.0 Cyber Physical Systems – IoT Innovation* (RCR Wireless News, Oct 29, 2015)
www.rcrwireless.com/rcrtv/germany-industrie-4-0-cyber-physical-systems-iot-innovation-episode-22
15. *AI Superpowers: China, Silicon Valley, and the New World Order* (Kai-Fu Lee, HMH Books 2018)

1.1 Towards an 'Intrinsically Digital World'

Nobel Prize laureate in Physics, Dennis Gabor described the principle governing technological civilization in these terms: *"What can be made will be made. Progress tends to apply new techniques and to establish industries regardless of whether they are truly desirable or not..."*[6] This principle could be reformulated to apply to the Internet of Things: *"What can be connected will be connected, regardless of whether it is truly desirable or not...".*

> **"What can be connected will be connected, regardless of whether it is truly desirable or not...**

After the industrial Internet and the automation of production process, we could be ushering in the era of smart products. So, beyond the connection of electronic devices, the next phase of the *IoT* development could involve the connection of everyday objects: clothing, manufactured products, foodstuffs, medicines, etc. As Niall Murphy, CEO of *Evrythng* put it: "*3.5 trillion products are made and sold every year, and there is a wide range of technologies allowing digital tech to find its way in...*"[7]. For network equipment manufacturer *Cisco*, the economic potential of what it terms the *'Internet of Everything'* derives from the

6. *Can We Survive Our Future? A Conversation with Dennis Gabor* (Encounter Vol.38, No.1-6 (Jan-June) 1972)
archive.org/details/dli.bengal.10689.15707/page/n157/mode/2up

7. *By 2020, everything from clothes to food will be connected to the web* (Wired Magazine UK, Oct 11, 2017)
www.wired.co.uk/article/niall-murphy-evrythng-internet-of-things-shopping-products

fact that 99.4% of the physical objects that could one day be part of it are still "not connected"[8].

The rise of the Internet of Things is not linked to a 'natural' or 'deterministic' evolution of the Internet. It is rather the result of a convergence of economic, industrial and technological interests. In the last decade, the rapid drop in sensors costs allowed them to be used within connected devices in massively different ways. Moreover, increased storage capacities and lower computing costs allowed to process data from connected devices on a larger scale. This is in addition to the ubiquitous nature of smartphones, whose ergonomics and 'gestural grammar' are now familiar to more than 3 billion users around the world. Mobile devices have thus become the '*remote controls*' and the '*exo-brains*' of many other connected objects. Memory and processing capabilities previously located on connected devices have been transferred to smartphones and tablets. This division of tasks has allowed to design more cost-effective devices with the minimum amount of intelligence and energy required to function.

In the meantime, the development of artificial intelligence technologies allowed to automate the processing of collected data to facilitate decision-making, such as in assisting with medical diagnosis, or being able to perform complex tasks formerly reserved to humans, like controlling driverless vehicles. We are thus witnessing the convergence of traditional Internet and *IoT* technologies, which rely on artificial intelligence systems to analyze and process data from these new generations of connected devices. This '*enhanced perception with artificial intelligence*' could be a leverage tool for creating high value-added services. According to artificial intelligence expert Kai-Fu Lee:

> When your refrigerator at home tells your shopping cart at the store that you're out of milk, are you moving through a physical world or a digital one? I call these new blended environments

8. *The Internet of Everything Global Private Sector Economic Analysis* (Cisco 2013) www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoE_Economy_FAQ.pdf

> OMO: online-merge-offline. OMO is the next step in an evolution that already took us from pure e-commerce deliveries to O2O (online-to-offline) services. Each of those steps has built new bridges between the online world and our physical one, but OMO constitutes the full integration of the two.[9]

1.2 Telecommunications Dedicated to the Internet of Things

The development of connected objects has led to the creation of telecommunications services specifically designed for the Internet of Things. Such offerings enable short-range communication systems (*NFC, RFID, Bluetooth, Zigbee*) to be combined with medium and long-range communication technologies (*NB-IoT, LTE-M*), to which can now be added *5G* communications and very long-range systems via satellite communications. In addition to differences in range, the 'spectrum' of these technologies ranges from low-speed communications (*LoRa*, *Sigfox*) for simple sensors up to high-speed or high-capacity communications. These communication technologies particularly concern the management of large fleets of objects and the most demanding real-time applications in terms of bandwidth, such as augmented (or virtual) reality applications. A 2019 survey by Ericsson among executives from 100 global telecom operators found that 92% believe the most important 5G feature is the way in which it will pave the way for emerging *IoT* technologies[10].

9. *AI Superpowers: China, Silicon Valley, and the New World Order* (p. 118 Kai-Fu Lee, HMH Books 2018).

10. *5G and IoT: An in-depth review of how next gen mobile connectivity will unlock new opportunities* (UK Tech News, 22 septembre 2020) www.uktech.news/news/5g-and-iot-an-in-depth-review-of-how-next-gen-mobile-connectivity-will-unlock-new-opportunities-20200921

1.3 Space Technologies and the Internet of Things in Europe

Space has become the new battleground for industrial, political and military confrontation for the connection and tracking of the next

generations of connected devices. Space technologies (*space tech*) play a key role in tracking connected objects and vehicles. Thus, the European satellite geolocation system *Galileo*, the next-generation satellites of which has just been announced[11], should make it possible to further improve the precision of the tracking of moving objects. This programme is the European response to the three satellite geolocation systems: America's *GPS*, Russia's *GLONASS* and China's *Beidou*. The *Galileo* programme will contribute to the strategic autonomy the European Union for the management of fleets of connected objects in the field of transport, in the management of energy infrastructures and urban planning.

Beyond objects' geolocation, information exchange from these objects could also use satellite communications. Thus, alongside satellite constellations designed to ensure global Internet connectivity (*SpaceX's Starlink, Amazon's Kuiper Systems, OneWeb*), new constellations of low orbiting satellites have been specifically developed for the *IoT*[12]. Examples of such nanosatellites constellations will comprise *ELO's Eutelsat*, *Sateliot* for *5G* connection, or the constellation of French company *Kinéis*, whose 25 satellites will be launched in 2022[13]. These satellite constellations should potentially connect tens of millions of connected objects.

1.4 Gradually Overcoming Barriers...

A 2015 study by the *World Economic Forum* estimated that the main barriers to the development of the Internet of Things in industry were related to the lack of interoperability between the solutions, the lack of security of connected objects and the immaturity of available technological solutions. Besides technological aspects, there were also concerns about the social acceptability of these technologies, and particularly their impact on privacy. The persons interviewed in this

11. Galileo next-gen satellites to be more powerful, reconfigurable (GPS World, Aug 14, 2020) www.gpsworld.com/galileo-next-gen-satellites-to-be-more-powerful-reconfigurable/

12. *Internet of Things (IoT) via Satellite* (Fraunhofer Institute for Integrated Circuits IIS) www.iis.fraunhofer.de/en/ff/kom/satkom/satellite_iot.html

13. *Constellation de satellites: Kineis, le nouveau champion du New Space français* (Challenge, 3 février 2020) www.challenges.fr/entreprise/aeronautique/constellation-de-satellites-kineis-le-nouveau-champion-du-new-space-francais_697061

study also mentioned the societal consequences of these technologies on organizations and on the development of skills and therefore on employment in the upcoming years.

Over a 5-year period, some technological hurdles have been overcome and many industrial sectors have developed uses for connected sensors. Nevertheless, interoperability between different families of connected objects has not yet been achieved and security vulnerabilities remain a major weakness of *IoT* technologies. Aware of the impact of the security of connected objects on the development of this market, the authorities in both the United States and Europe are starting to create specific regulations aimed at enhancing connected objects security. However, issues related to the consequences of the Internet of Things on users' privacy are still in the early stages of their formalization by regulators.

1.5 ...and Significant Growth Prospects

For the experts of the *World Economic Forum*: *"It is estimated that industrial IoT alone can add $14 trillion of economic value to the global economy by 2030. The economic value increases even more once consumer and public sector IoT are included*[14]". The industrial players involved in the transformation of the Internet of Things are already forecasting considerable growth in IT needs for these technologies. For example: *"ARM, whose designs dominate the market for the sorts of low-power chips that are embedded in everything from smartphones to televisions, organises its business around the assumption that there will be a trillion computers in the world by 2035"*[15].

In the last 5 years, global spending related to the Internet of Things increased fourfold. This increase is especially related to industrial manufacturing, transport, energy and major infrastructure networks.

14. *Internet of Things Guidelines for Sustainability* (World Economic Forum, Jan 2018) www3.weforum.org/docs/IoTGuidelinesforSustainability.pdf

15. The Internet of Things - The Economist Technology Quarterly (sept 2019)

The '*Industrial Internet of Things*' sector alone represented a $40 billion market in 2020. According to a *Statista* study, global spending on the Internet of Things could reach $1.6 trillion in 2025[16].

1.6 *"Smart, Hackable and No Longer Something You Own..."*

Embedding sensors and communication systems in objects add functionalities to these objects and modify their uses. For industrial players, the analysis of connected object data provides key additional information and enables them to improve on the services provided by these objects. But the information gathered from these connected objects also enables to improve their knowledge on the behavior of their users. What will be the industrial, social and political consequences of the rise of the IoT in our societies?

Far from being an extension of the services that already exist on the Internet, the connection of everyday objects will produce new effects on the industrial and technological landscape and on the relationship that users have with their objects. In 2014, Alexis Madrigal and Robinson Meyer announced in *The Atlantic* that three things happen when an object connects to the Internet: "*When a thing connects to the Internet, three things happen: it becomes smart, it becomes hackable, and it's no longer something you own*"[17].

1.7 IoT: the Weakest Link in Cybersecurity

Like every Internet connected device, remotely accessible objects create opportunities for new kinds of vulnerability and computer attacks. The growth in various categories of connected devices increases the 'attack surface' and creates new opportunities for malicious hackers.

16. Global spending on IoT in 2015 and 2020, by industry sector in billion U.S. dollars (Statista, Sept 1, 2020) www.statista.com/statistics/1095375/global-spending-on-iot-by-industry-sector/

17. Alexis C. Madrigal & Robinson Meyer When Everything Works Like Your Cell Phone (The Atlantic, Sept 28, 2014) www.theatlantic.com/technology/archive/2014/09/when-everything-works-like-your-cell-phone/379820

Whether these attacks are aimed at using connected objects against traditional Internet infrastructures or specifically targeting the objects or their users. The *IoT* has become one of the weakest links in global computer security and could be even more so with the rise of new generations of connected objects. In 2016, one of the largest massive denial of service (*DDoS*) attacks ever observed was carried out against the *Dyn Managed DNS* service with the *Mirai* malware. This attack affected major companies such as *Amazon*, *Twitter*, *Netflix*, *Github*, *Spotify* and *OVH*. Unlike previous generations of attacks which used 'zombie' computers controlled without the knowledge of their users, this attack was carried out using connected objects other than traditional computers: *"One of the sources of the attack is internet-connected products like printers, DVRs, and appliances, often called the "Internet of things"..."* [18].

"Besides being a major concern for users, the security of the Internet of Things has also become a national security challenge for States..

This attack was the first large-scale use of connected objects as attack vectors against 'traditional' Internet infrastructures. Since then, other types of attacks have been observed by Internet of Things cybersecurity experts. These attacks were directed against connected objects, data they could collect, and even against users themselves.

Besides being a major concern for users, the security of the Internet of Things has also become a national security challenge for States. Already back in 2014, the *CIA* had expressed its fear that the Internet of Things would become the new theatre of international conflicts[19]. Consequently in 2014, Dan Geer, head of cybersecurity at the venture capital firm of the *CIA* (*In-Q-Tel)*, called on States and citizens to analyze their dependence on *IoT* technologies and security services:

18. *A massive cyberattack knocked out major websites across the internet* (Business Insider Oct 21, 2016) www.businessinsider.fr/us/amazon-spotify-twitter-github-and-etsy-down-in-apparent-dns-attack-2016-10/

19. *The CIA Fears the Internet of Things* (Defense One, Jul 24, 2014) www.defenseone.com/technology/2014/07/cia-fears-internet-things/89660/

> As society becomes more technologic, even the mundane comes to depend on distant digital perfection. Our food pipeline contains less than a week's supply, just to take one example, and that pipeline depends on digital services for everything from GPS driven tractors to drone-surveilled irrigators to robot vegetable sorting machinery to coast-to-coast logistics to RFID-tagged livestock. Is all the technologic dependency, and the data that fuels it, making us more resilient or more fragile? Does it matter that expansion of dependence is where legacy comes from? Is it essential to retain manual means for doing things so that we don't have to reinvent them under time pressure?[20]

These words resonate differently today following the *COVID-19* crisis. The pandemic has demonstrated the dependence of our societies on technologies and supplies, which for the most part were non-European. The citizens of the countries of the European Union have now become aware not only of their health system vulnerability, but also of their technological and industrial dependence. Dan Geer concluded his appeal with his personal definition of cybersecurity: *"My personal definition of a state of security is "The absence of unmitigatable surprise." My personal choice for the pinnacle goal of security engineering is "No silent failure."*[21] This definition from a cybersecurity expert also applies to users of Internet of Things technologies. This security and this 'absence of surprise' are essential prerequisites for maintaining the social acceptability of such technologies and to avoid a massive rejection of *IoT* technologies in the future.

Technologies and services related to the security of connected objects are an essential market for all technology players[22]. However, the security of these objects has remained rudimentary. From the absence of encryption mechanisms for data transmission[23], to the impossibility of integrating security updates, the security of connected objects is today one of the weakest links in the infrastructure of

20. *Dan Geer, Security of Things* (May 7, 2014) geer.tinho.net/geer.secot.7v14.txt

21. *Ibid*.

22. *How the 'insecurity of things' creates the next wave of security opportunities* (TechCrunch Jun 26, 2016) techcrunch.com/2016/06/26/how-the-insecurity-of-things-creates-the-next-wave-of-security-opportunities/

23. *Internet of Things Security Study: Smartwatches* (Hewlett Packard Entreprise Study, 2015) www.ftc.gov/system/files/documents/public_ments/2015/10/00050-98093.pdf

the Internet. These failings are even becoming critical in certain sectors related to personal security, such as health technologies. David Talbot had already sounded the alarm in the *MIT Technology Review* in 2012: *"Computer viruses are "rampant" on medical devices in hospitals"*[24]. Five years later, in 2017, these same vulnerabilities of connected medical devices were again singled out by *Wired* magazine as an impending nightmare for cybersecurity experts[25]. More recently, in his book on Cybersecurity and the Internet of Things, Bruce Schneier described unprecedented threats to people and no longer just to information infrastructures: "*We're already living in a world where computer attacks can crash cars and disable power plants—both actions that can easily result in catastrophic deaths if done at scale. Add to that hacks against airplanes, medical devices, and pretty much all of our global critical infrastructure, and we've got some pretty scary scenarios to consider"*[26].

> **"We're already living in a world where computer attacks can crash cars and disable power plants—both actions that can easily result in catastrophic deaths if done at scale. Add to that hacks against airplanes, medical devices, and pretty much all of our global critical infrastructure, and we've got some pretty scary scenarios to consider**
>
> **Bruce Schneier**

In his report on the Internet of Things prepared for *NATO* (*North Atlantic Treaty Organization*), Matej Tonin specified that security devices will have to be integrated by default into connected objects (*security by design*), rather than waiting for manufacturers to spontaneously decide to adopt them. This is even more important as the risks associated with security breaches in the Internet of Things can have 'systemic' consequences for States:

> A key debate in IoT security and privacy protection is whether strong protections should be "baked in" from the beginning or whether the market should take off first and then additional

24. *Computer Viruses Are "Rampant" on Medical Devices in Hospitals* (MIT Technology Review, October 17, 2012) www.technologyreview.com/s/429616/computer-viruses-are-rampant-on-medical-devices-in-hospitals/

25. *Medical Devices Are the Next Security Nightmare* (Wired, Mar 2, 2017) www.wired.com/2017/03/medical-devices-next-security-nightmare/

26. *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World* (p. 9) Bruce Schneier, (Ed. Norton & Company, 2018)

> security can be "bolted on" once the IoT market has taken off. For advocates of the former, regulators can avoid some of the faults with the Internet's development, which was originally designed for small-scale networks of trusted computers – not a mass market filled with its cyber criminals. The view that such "security by default" should be the aim of designing devices and services is the most widespread position. [...] One expert argues that not every IoT device needs the same high level of security and privacy. He proposes to apply three metrics: the value of data collected, the criticality of the data and the scalability of failure. In other words, protection should be highest if IoT devices and services collect and transmit highly valuable and/or critical data, and/or if failure in one part could cascade into widespread failures.[27]

It was also the finding of an 'endemic' vulnerability in connected objects that pushed the *NSA (National Security Agency)* to fund the development by the *University of Alabama* of security systems for connected objects and their cloud-based information storage[28]. This security concern met a double need: to 'defensively' ensure the resilience of the US Internet of Things in the event of an attack or intrusion, and most likely also to ensure that the security solutions developed by manufacturers can include backdoor devices to facilitate investigative or surveillance work. However, as Bruce Schneier[29] reminded us, one of the biggest mistakes developed countries could make would be to deliberately create security breaches in connected objects. Indeed, if these backdoors were to become legal obligations[33], they would inevitably end up being discovered by malicious hackers.

Regulations on the security of connected objects and more generally the processing of data from these objects are major challenges in terms of safeguarding liberties, but also in terms of confidence for all technology players. As new forms of cyberattacks based on connected objects are developed, the economic future of this sector could

27. *The Internet of Things: Promises and Perils of a Disruptive Technology,* Matej Tonin, Rapporteur Sub-Committee on Technology Trends and Security (NATO Parliamentary Assembly Oct 8, 2017) www.nato-pa.int/document/2017-internet-things-tonin-report-175-stctts-17-e-bis

28. *UAH developing architecture to build design-phase cybersecurity into systems* (The University of Alabama in Huntsville, *Aug 6, 2015)* www.uah.edu/news/research/uah-developing-architecture-to-build-design-phase-cybersecurity-into-systems

32. *Data and Goliath* (Bruce Schneier, Ed. Norton & Company 2015)

29. *'Five Eyes' governments call on tech giants to build encryption backdoors - or else* (TechCrunch, Sept 3, 2018) techcrunch.com/2018/09/03/five-eyes-governments-call-on-tech-giants-to-build-encryption-backdoors-or-else/

depend on the ability of European manufacturers to develop security solutions that will protect the data obtained from these objects as well as their users. Accordingly, the measures that will make it possible to strengthen the security of connected objects (from the extraction of information by the object itself to the remote processing of this information) could become a key element of European industrial policies for the *IoT*.

When *California IoT Security Law* was introduced, Bruce Schneier described the end of an industrial chapter marked by manufacturers' negligence in terms of security. He also heralded a new era where the manufacturers of such objects would be gradually compelled to adopt more responsible behaviors:

> Insecurity is profitable only if you can get away with it worldwide. Once you can't, you might as well make a virtue out of necessity. So everyone will benefit from the California regulation, as they would from similar security regulations enacted in any market around the world large enough to matter, just like everyone will benefit from the portion of GDPR compliance that involves data security. Most importantly, laws like these spur innovations in cybersecurity. Right now, we have a market failure. Because the courts have traditionally not held software manufacturers liable for vulnerabilities, and because consumers don't have the expertise to differentiate between a secure product and an insecure one, manufacturers have prioritized low prices, getting devices out on the market quickly and additional features over security.[30]

In Europe, *GDPR* measures encouraged to establish codes of conduct[31] and "*data protection certification mechanisms and of data protection seals and marks*"[32]. Like in *energy labels* that guide consumer choice on the energy performance of electrical appliances, compliance certification or a trust label based on the *GDPR* could inform citi-

30. *Bruce Schneier, New IoT Security Regulations* (Blog Post Nov 2018) www.schneier.com/blog/archives/2018/11/new_iot_securit.html

31. Art. 40 GDPR.

32. Art. 42 GDPR.

zens about the level of privacy and security of connected objects. The Commission services consider important to reflect upon possibilities for certification of networked devices that would provide a minimum level of secure authentication, from the hardware level to network integrity[33]. This would require manufacturers to analyze the functions of each device and provide secure data processing for the *IoT*. To this end, the *Cybersecurity Act*[34] was definitively adopted by the European Union in June 2019. The *European Union Agency for Cybersecurity* (*ENISA)*, has been tasked with developing a certification framework for the security of connected objects in Europe.

> **“They were aggrieved because they thought they had bought the books when in fact, it turned out, they were merely renting them...**
>
> **Bobbie Johnson**

1.8 The End of Ownership?

Another kind of change brought about by connected objects is due to the fact that their functionalities and value come from their connection to remote servers. If this connection to remote servers is suspended for economic reasons, such as company closure, or for technological reasons, due to lack of updating, the functioning of these connected objects (and even their usefulness) is called into question. The users of these objects can thus be ‘dispossessed’ of them without them being taken away.

Amazon gave a prime example of such changes in the very concept of ownership in the age of the IoT. In 2009, a legal dispute arose between *Amazon*’s *Kindle* division and the publisher of George Orwell’s novel *1984*. All copies of the novel, which describes the possible end of books in a totalitarian society, were removed from *Kindles* overnight. It suddenly dawned on users that works they had duly paid for could be taken from them. Users’ reactions to this ‘forced expropriation’ were

33. *Advancing the Internet of Things in Europe* (page 31) Commission Staff Working Document Apr 19, 2016 eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX-:52016SC0110&from-EN

34. *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)* eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX-:32019R0881&from=EN

so strong that Bobbie Johnson gave the following explanation in *The Guardian* newspaper: "*Why were people so offended? Customers weren't really angry about the gadget, or the legality of the books in question – they were furious with the sleight of hand Amazon performed by secretly removing them from their machines. They were aggrieved because they thought they had bought the books when in fact, it turned out, they were merely renting them*"[35].

Faced with the controversy generated by the removal, and mindful of the risks that this decision posed for the long-term existence of the *Kindle* platform, *Amazon* owner Jeff Bezos was forced to write a letter of apology in unusual terms to *Kindle* users: *"This is an apology for the way we previously handled illegally sold copies of 1984 [...] Our 'solution' to the problem was stupid, thoughtless, and painfully out of line with our principles. It is wholly self-inflicted, and we deserve the criticism we've received. We will use the scar tissue from this painful mistake to help make better decisions going forward, ones that match our mission"*[36].

Ten years later, it was *Microsoft*'s turn to highlight the short-lasting nature of ownership of connected objects and their associated services. When *Microsoft* closed its e-bookstore in June 2019, users were no longer able to access the downloaded books that they had legally acquired. This was not due to a legal conflict in this case, but the way that *Microsoft DRM (Digital Rights Management)* technologies are used to lock in users. Brian Barret, director of *Wired* magazine, noted that these technologies were becoming the strong arm of a strategy to lock users of connected objects and their content into a few large-scale platforms:

> More than anything, Microsoft's ebook rapture underscores the hidden dangers of the DRM system that underpins most digital purchases. Originally intended as an antipiracy measure, DRM now functions mostly as a way to lock customers into a given ecosystem, rather than reading or viewing or listening to their

35. *Why did Big Brother remove paid-for content from Amazon's Kindles?* (The Guardian, Jul 22, 2009) www.theguardian.com/technology/2009/jul/22/kindle-amazon-digital-rights

36. *Amazon's Jeff Bezos apologises for Kindle deletions* (The Telegraph, Jul 24, 2009) www.telegraph.co.uk/technology/news/5901667/Amazons-Jeff-Bezos-apologises-for-Kindle-deletions.html

purchases wherever they want. It's a cycle that has persisted for decades and shows no signs of abating[37].

Another way users can be 'dispossessed' of connected objects is by a lack of software updates. Besides increasing the risks of hacking, some objects may even become unusable if they are not updated. A number of IoT manufacturers have been accused by their users of practicing new forms of planned obsolescence. This was the case for smart speaker manufacturer *Sonos*, which was forced to continue providing technical support for its speakers after criticism from its purchasers[38].

> **"We have fewer rights as digital tenants than we do as tenants of real estate, where eviction is subject to due process. If we purchase something, it is ours. We shouldn't let ownership go down the memory hole…**
>
> **Zeynep Tüfekçi**

Two decades ago, in his book *'The Age of Access',* Jeremy Rifkin described the possible end of individual ownership and invited us to *"imagine a world where virtually every activity […] is a paid-for experience, a world in which traditional reciprocal obligations and expectations […] are replaced by contractual relations in the form of paid memberships, subscriptions, admission charges, retainers, and fees"*[39]. More recently, Turkish-American sociologist Zeynep Tüfekçi warned IoT users of the risks of questioning social norms in terms of ownership: *"We have fewer rights as digital tenants than we do as tenants of real estate, where eviction is subject to due process. If we purchase something, it is ours. We shouldn't let ownership go down the memory hole"*[40].

Safeguarding European digital sovereignty will be closely connected with preserving the principles and cultural values on which were founded the countries of the Union. Foremost among these principles are rights of ownership for these connected objects and their data. These rights are crucial when these platforms acquire considerable

37. *Microsoft's Ebook Apocalypse Shows the Dark Side of DRM. Microsoft has closed its ebook store - and will soon make its customers' libraries disappear along with it.* (Wired, Jun 30 2019) www.wired.com/story/microsoft-ebook-apocalypse-drm/

38. *UK government introduces security rules for 'internet of things'* (Financial Times, Jan 27, 2020) www.ft.com/content/bfc6f2f4-412d-11ea-bdb5-169ba7be433d

39. *The Age of Access: The New Culture of Hypercapitalism, Where all of Life is a Paid-For Experience* Jeremy Rifkin (p. 9 Penguin Publishing 2000)

40. *Zeynep Tufekci: We Are Tenants On Our Own Devices* (Wired, June 2019) www.wired.com/story/right-to-repair-tenants-on-our-own-devices/

power over the conception, dissemination and use of ideas and cultural creations. Establishing a bond of trust with IoT users will require the overhaul of ownership rights for connected objects and services. Measures to ensure their longevity will have to be put in place at the design stage, whether in terms of durability of connected objects or by enabling the transfer of data or related services. Provided that these measures do not jeopardize the security of connected objects and their users, the 'proprietary' nature of technologies should not hinder the ability to use these objects on a long-term basis. To this end, interoperability and design standards need to be imposed to ensure data portability and longevity of IoT content and services. This transparency of operation and durability will be particularly important when objects concern cultural activities, health or education.

2

PREREQUISITES FOR THE RISE OF THE INTERNET OF THINGS

To extend Internet of Things technologies to all products and manufactured goods, designers of these technologies must be able to respond to several types of constraints. First and foremost, these technologies will require great robustness to operate in highly diverse technological environments and under significant time constraints. They must also have a strong scalability capacity and a high level of security to avoid information leaks, particularly of sensitive information, but also to prevent these objects from turning against their users if hacked.

In addition to the functionalities offered by these new generations of connected objects, security and trust could thus become key elements in users' choices with regard to *IoT* technologies[41]. Other specific industrial features could condition the 'durability' of connected objects. As noted by *World Bank* experts, these connected objects work differently from most electronic devices, especially when deployed outdoors or in public spaces. Specific contractual terms must therefore be used to limit the risk of malfunctions during their life cycle:

> The typical consumer electronics life cycle of 2-4 years is not feasible for large-scale IoT. The costs and logistics of updating/

41. See on this point the conclusions of the IoT Security Working Group set up by the *ISOC* (ISOC March 7, 2020) www.isoc.fr/iot-22-recommandations/

redeploying any pieces of an IoT system every 2-4 years can potentially outweigh the value for all stakeholders. Any IoT solution should have a clear annual maintenance contract (AMC) in place to support the devices and services over the lifetime of the system. An AMC will incentivize the system provider to provide devices that will be able to withstand external conditions, their sensors remaining calibrated to ensure proper measurements[42].

2.1 Unique Identifiers and Software Interoperability

One of the cornerstones of the interoperability of IoT technologies will also concern the adoption of unique identifier systems and interoperable communication protocols across all connected objects. Many identification systems are currently 'proprietary' systems, as is the case for connected objects on *iOS*, *Android* or *Amazon AWS* platforms. Identifiers and application programming interfaces (*API*s) will need to be interoperable so as to link objects from different information 'silos' (for example, environmental control and health devices or foodstuffs). For these unique object identifiers to be integrated into the various logistics chains and different technological environments, they will have to be coordinated by all the industrial players involved in their development and use, as is currently the case for *GTIN (Global Trade Item Number)* product codes. Unlike current product codes, however, which are essentially useful for logistics, the aim of these new generations of unique identifiers will be to monitor and interact individually with each object from its design and assembly (or production) and then throughout the object's lifetime until it is recycled.

The large-scale technologies used to access information resources on the Internet could thus constitute one of the bases for the interoperability of unique object identifiers. This is the case with the *DNS*

42. *Internet of Things The New Government To Business Platform a Review of Opportunities, Practices, and Challenges* (World Bank Group Nov 3, 2017) documents1.worldbank.org/curated/en/610081509689089303/pdf/120876-REVISED-WP-PUBLIC-Internet-of-Things-Report.pdf

(Domain Name System), which is used to convert Internet domain names into IP addresses. This distributed system has proved its robustness since its creation in 1983. By way of example, the content delivery network *Akamai* 'resolves' over 2,200 billion *DNS* queries every day[43]. And, as part of evolutions towards the Internet of Things, technologies derived from *DNS* such as *ONS (Object Naming Service)*[44] were envisioned to access unique object identifiers[45]. *ONS* has been the subject of standards work[46] carried out jointly by *Afnic* (the organization designated by the French State to manage .fr domain names) and *GS1* (the international standardization organization for *GTIN (Global Trade Item Number)* product codes). As an extension of its work on *ONS*, *Afnic* has also been involved in the activities of the *AIOTI (Alliance for Internet of Things Innovation*) in the standardization of unique identifiers for connected objects[47].

Interoperability of connected objects also concerns the ways they connect to the network. Just as the Internet allows computers to be linked together, the IoT must allow different identification technologies to be linked. This will involve meeting the needs of industrial market players who use technologies designed to respond to specific needs or trades. *Roaming* technologies will need to be implemented for connected device tracking so as to allow continuous communication with these objects regardless of their environment. Again, *DNS* technologies could be one of the solutions to the ramp-up of object tracking[48].

2.2 RFID Tags on All Products?

One of the key object identification technologies is provided by *RFID (Radio-Frequency Identification)* chips. These chips are among the oldest IoT technologies. Scientist and inventor Harry Stockman came up with the principle behind these chips in 1948[49].In the early days, these chips were used for military logistics applications. *RFID* chips can be

43. *Learn How Trillions of Dns Requests Help Improve Security* (Akamai Technologies, 2018) blogs.akamai.com/2018/05/learn-how-trillions-of-dns-requests-help-improve-security.html

44. *The Internet of Things - GS1 France & Afnic major contributors to the ONS 2.0* (Feb 18, 2013) www.afnic.fr/en/about-afnic/news/general-news/6703/show/the-internet-of-things-gs1-france-afnic-major-contributors-to-the-ons-2-0.html

45. *Why DNS should be the naming service for Internet of Things?* (Sandoche Balakrichenan – Afnic 2016) ant.isi.edu/events/dinr2016/P/p72.pdf

46. *GS1 ONS Version 2.0.1 Ratified Standard* (Issue 2 Jan 31, 2013) www.gs1.org/gsmp/kc/epcglobal/ons/ons_2_0_1-standard-20130131.pdf

47. *Identifiers in Internet of Things (IoT) Version 1.0*, Feb 2018 AIOTI WG03 – IoT Standardisation aioti.eu/wp-content/uploads/2018/03/AIOTI-Identifiers_in_IoT-1_0.pdf.pdf

48. See on this point the work of the *Wireless Broadband Alliance* on *OpenRoaming* wballiance.com/openroaming

49. *"Communication by Means of Reflected Power"* Harry Stockman (Proceedings of the IRE, vol. 36, no. 10, pp. 1196-1204, Oct 1948) simson.net/ref/1948/stockman.pdf

used to assign an identifier to an object, and the simplest are equipped with a rudimentary processor and antenna. The antenna enables the processor to be triggered via a short electromagnetic pulse. The chip's function is to respond to this pulse by decoding the series of numbers encoded on its processor. The unit price of the simplest *RFID* chips is just a few cents and they are long-lasting since they do not contain any internal power source that could run out of charge, or moving parts that could wear out.

RFID chips could thus be used to replace optical identification systems for manufactured products (bar codes, QR codes, Data matrix, etc.). For example, the identifier on barcodes is useful to logistics players and, to a lesser extent, the purchaser (for price comparisons or to collect information on the product's composition).

RFID chips could be used for services beyond the point of sale. *RFID*-tagged products could, for example, transmit information to a household appliance: a food product to a refrigerator, or a piece of clothing to a washing machine, etc. These chips could also be used to inform users about events occurring during an object's lifetime. Tire manufacturer *Michelin* has experimented with integrating *RFID* chips for tire identification (unique identification number for each tire) and to obtain information on parameters such as its date of assembly, its wear, pressure, temperature, etc.[50].

Most *RFID* chips do not contain any deactivation or encryption mechanisms, or security devices. Integrating such mechanisms to protect chips from queries from unauthorized users (*skimming*) or encrypting their communications still involves significant additional costs. Such security devices could, for example, prevent sensitive data from a medical device being fraudulently captured. But this additional security cost can only be covered by producers or distributors of these objects (and ultimately by consumers) if it is for a service that can be

50. Track Connect: connected tire solution (Michelin, Mar 26, 2018) https://www.youtube.com/watch?v=Cili2VJ7OXs

used throughout the object's lifetime (from its design until it is recycled). In this case, *RFID* chips could become an essential link in IoT services.

It is already proving cost-effective to add connected functions to 'smart' electronic devices. But the price of *RFID* sensors or identification devices is still a barrier to the rise of the Internet of things which up to now have been considered 'stupid' (foodstuffs, clothing, manufactured products, etc.). If the integration of deactivation/reactivation devices or cryptographic security systems were to become a legal obligation, manufacturers of connected objects could be faced with a 'margin squeeze' associated with the additional cost of connected sensors and *RFID* chips.

In 2018, *Decathlon*, the world's leading sporting goods retailer, decided to extend the installation of *RFID* chips to almost all of its items[51]. For *Decathlon*, the economic equation of *RFID* chips was different from traditional players in the retail and distribution industry. Indeed, 80% of the products sold by the sports chain are from its own brands[52] and therefore allow the installation of *RFID* chips to be vertically integrated into the production and distribution process. Moreover, the unit cost of chips was negligible compared to the average price of sporting goods. The unit price for encoded *RFID* tags was between €0.05 and €0.1. By way of comparison, an anti-theft *EAS* tag costs between €0.02 and €0.03[53]. For food products with much lower unit prices, this additional cost is still too high for distributors. Initially chosen to improve the visibility of logistics flows, *RFID* chips can also be used to improve the user experience in the brand's stores (information on stock levels, for example)[54].

The shift towards individual tagging of food products will go hand in hand with the development of new generations of services linked to other connected objects or products. Other avenues are now being considered in order to meet environmental goals, such as using *RFID*

51. *Case Study: Decathlon: getting smart with RFID tags* (Internet Retailing, Aug 1 2019) https://internetretailing.net/magazine-articles/magazine-articles/case-study-decathlon-getting-smart-with-rfid-tags

52. *Decathlon : Le bilan financier 2018 et les perspectives pour 2019* (SportBuzzBusiness, February 25, 2019) www.sportbuzzbusiness.fr/decathlon-le-bilan-financier-2018-et-les-perspectives-pour-2019.html

53. *La RFID révolutionne les magasins Decathlon* (LSA-Conso, Jan 13, 2016) www.lsa-conso.fr/la-rfid-revolutionne-les-magasins-decathlon,228999

54. *The rise, fall and return of RFID* (Supply Chain Dive, Aug 21, 2018) www.supplychaindive.com/news/RFID-rise-fall-and-return-retail/530608/

chips to identify reusable food product packaging. These unique packaging identifiers could then be associated with a product during the checkout process. New high value-added services could thus be created to find out the availability of products in the user's home or whether they are suitable for consumption[55]. R&D work also aims to create biodegradable micro-sensors which can be used to ensure that there have been no breaks in the cold chain for food products[56].

> **"A convenience store you just walk out of is a friendly mask on the face of a highly controversial application of technology: ubiquitous personal surveillance…**
>
> **Devin Coldewey**

'Amazon Go' supermarkets: the choice of artificial intelligence

Other technologies can also be used to identify products in stores. Rather than placing *RFID* chips on products, *Amazon* went for other technological options to develop its 'cashierless' stores. To analyze customer movements and find out which products they were buying, *Amazon* developed a combination of technologies based on artificial intelligence (*Deep Learning/Object Detection/Sensor Fusion/Computer Vision*) for the real-time analysis of images from multiple cameras and sensors associated with object detection systems[57]. The aim of the technologies used by *Amazon* was to simplify the user experience within the stores themselves, but not to create a continuum to develop services related to the items beyond the point of sale. Besides equipping its own stores with these devices, *Amazon* intends to distribute this technology to all of the major 'physical' distribution chains. However, Devin Coldewey, one of the first journalists to try out the *Amazon Go* supermarket in Seattle, questioned the social and political acceptability of these technologies: *"On the philosophical side, I'm troubled, of course - a convenience store you just walk out of is a friendly mask on the face of a highly controversial application of technology: ubiquitous personal surveillance…"*[58].

55. *IoT is about to tell you when your food is spoiled* (Network World, Aug 22, 2017) www.networkworld.com/article/3218120/internet-of-things/iot-is-about-to-tell-you-when-your-food-is-spoiled.html

56. *Biodegradable microsensors: the link between food products and the Internet of Things?* (ETH Zürich, Sept 2017) www.youtube.com/watch?v=S9ZiXGnadno

57. *How the Amazon Go Store's AI Works* (Medium, Towards Data Science Jun 7, 2019) towardsdatascience.com/how-the-amazon-go-store-works-a-deep-dive-3fde9d9939e9

58. *Inside Amazon's surveillance-powered no-checkout convenience store* (TechCrunch, Jan, 22 2018) techcrunch.com/2018/01/21/inside-amazons-surveillance-powered-no-checkout-convenience-store

2.3 Towards a Right to the *'Silence of the Chips'*

When such objects are designed, new functionalities will have to be provided for 'citizen-users' to control the flow of data exchanged by their connected objects. It must therefore be possible to temporarily or permanently deactivate connected objects, especially since information can be exchanged without users being informed. Thus, in its report on the links between administrations and the Internet of Things, the *World Bank* recommends that future legislation should take into account these new technological dimensions related to personal data protection:

> It is important to establish forward-looking regulatory standards to guard the security and privacy of data. Most of the current solutions to these issues rely on higher-level computational and memory-intensive processes that tend to be limited in IoT devices. Significant hardware support, such as encryption, authentication, and attestation, and software support, such as run-time self-healing architecture, are required for future IoT devices. It is critical to ensure that only authorized users are allowed to access the data and that the systems are developed with processes and standards and monitored to ensure bad actors cannot exploit the system to access the data or damage the systems, particularly when the IoT systems feed back into the physical world[59].

However, while sophisticated electronic devices, such as a smartphones, are relatively easy to deactivate, it is a different matter when it comes to an *RFID* chip used to 'tag' an industrial object or foods. The principle of the right to the '*Silence of the Chips*' was developed in 2006[60] with the aim of allowing users to control information from *RFID* chips. It entails including deactivation/reactivation devices associated with encryption systems as from the design stage for objects carrying

59. *Internet of Things The New Government To Business Platform a Review of Opportunities, Practices, and Challenges* (World Bank Group Nov 3, 2017) http://documents1.worldbank.org/curated/en/610081509689089303/pdf/120876-REVISED-WP-PUBLIC-Internet-of-Things-Report.pdf

60. In the text *Organizing Internet Architecture* (Bernard Benhamou, Revue Esprit, May 2006). www.netgouvernance.org/esprit-eng.pdf see also « *Les Mutations Économiques, Sociales et Politique de l'Internet des Objets* » (Bernard Benhamou, Cahiers de la Documentation Française, January 2013). http://www.netgouvernance.org/IOT%20Cahiers%20DOC%20FRANCAISE.PDF

sensitive data, especially for medical data or data relating to personal security and safety.

The right to the silence of the chips was officially mentioned in May 2008 during the first European ministerial meeting on the Internet of Things[61], and was then taken up by the European Commission[62] [63] and the European Parliament[64]. This right was also mentioned by the Council of State of France in its 2014 report '*Digital technology and fundamental rights*'[65] as one of the avenues for reflection for the future of the Internet of Things. However, it has not yet been the subject of legislative implementation in Europe. Reservations expressed by manufacturers include concerns about the change to the economic balance that could be generated by such devices. Nevertheless, disputes over the uncontrolled dissemination of personal data now make the prospect of such legislation more likely[66]. It would inevitably result in additional costs if *RFID* chip makers were legally compelled to incorporate new security features as well as deactivation/reactivation mechanisms. The key issue is a trade-off between the development of new industrial sectors and the necessary protection of personal data of EU citizens. However, increased risks relating to the security of connected objects and users concerns about new risks on their personal data could alter the conditions of such a trade-off. This trend could be even more pronounced given that eventually *RFID*-tagged objects could outnumber all other types of connected objects.

3.3 Self-Powered Sensors and Devices

Another major challenge for the deployment of the IoT will be related to the energy autonomy of sensors. This autonomy is a strategic issue for connected object manufacturers from both an environmental and an industrial point of view. While the simplest *RFID* chips do not have an internal energy source, all active sensors require batteries,

61. *"Internet of Things-Internet of the Future"* European ministerial conference organized within the framework of the French Presidency of the European Union (Nice 2008).

62. The right to the "Silence of the Chips". The Commission will launch a debate about whether individuals should be able to disconnect from their networked environment at any moment. Citizens should be able to read basic RFID (Radio Frequency Identification Devices) tags – and destroy them too – to preserve their privacy. Such rights are likely to become more important as RFID and other wireless technologies become small enough to be invisible. *Europe prepares for the internet revolution* (European Action Plan, June, 18 2009) europa.eu/rapid/press-release_IP-09-952_en.htm

63. *Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification* (May 12, 2009) https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=6496

64. *Motion For A European Parliament Resolution On The Internet Of Things* (Committee on Industry, Research and Energy, Rapporteur: Maria Badia i Cutchet, May 10, 2010) www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2010-0154+0+DOC+PDF+V0//EN

65. *Le numérique et les droits fondamentaux* (Annual report of the French Council of State, September 2014) www.vie-publique.fr/sites/default/files/rapport/pdf/144000541.pdf

66. *The "silence of the chips" concept: towards an ethics (-by-design) for IoT,* Caroline Rizza & Laura Draetta. International Review of Information Ethics. vol. 22. 10.29173/irie125 (2015) www.researchgate.net/publication/282029896_The_silence_of_the_chips_concept_towards_an_ethics_-by-design_for_IoT/citation/download

which imposes significant limits on their lifespan but also in terms of replacement costs. A number of European tech companies are already setting up research programs based on the principle of *energy harvesting*. This allows sensors to be recharged through physical variations in their environment. Energy 'harvesting' can use the vibrations of the object, heat and light variations or the energy resulting from other electromagnetic waves:

> To drive down prices even further, *Sigfox*'s R&D laboratory is trying to solve one of the main issues in the sector: battery change, which is still an expense, even though it is only required once every ten years on average. The company's researchers are working on *energy harvesting* technologies. Devices with this type of equipment can are capable of extracting energy from the surrounding environment and (if the research is successful), become 100% autonomous. *Sigfox* has also announced radio connectivity modules marketed at $0.2 for 2020, and subsequently at $0.02[67].

In a related field, in Paris, car manufacturer *Peugeot* has experimented using billboards with piezoelectric sensors to transform vibrations from urban traffic noise into electricity to charge electric vehicles[68]. Another example of energy harvesting in everyday objects is provided by the microturbines in *Hydrao* shower heads[69]. The sensors are powered by the water flow and provide information on the volume of water used.

67. *Sigfox prototypes self-powered IoT devices* (Mobile World Live, Nov 21, 2019) https://www.mobileworldlive.com/latest-stories/sigfox-prototypes-self-powered-iot-devices

68. *New Peugeot 208 - Recycle the Noise, Silence the City* (Peugeot, Nov 12, 2019) www.youtube.com/watch?v=6_lVGiokmNM

69. *This smart shower flashes when you've used too much water* (Wired Jan 5, 2016) https://www.wired.co.uk/article/hydrao-smart-shower-ces-2016

3

IOT AND RECONFIGURATION OF THE INDUSTRIAL LANDSCAPE

Internet technologies have enabled major tech companies such as *GAFAM (Google, Amazon, Facebook, Apple, Microsoft), NATU (Netflix, Airbnb, Tesla, Uber)* and their Chinese counterparts *BATX (Baidu, Alibaba, Tencent, Xiaomi)* to gain a foothold in areas initially outside of their sectors. These companies are already becoming major players in finance, transport, health, media and tourism. Today, IoT technologies and the ability to extract data on industrial processes, and on individuals and their environment, creates new opportunities for domino effects in other areas of business. IoT may ultimately speed up the reconfiguration of entire segments of the economy of developed countries.

An example of this use of connected objects in the industrial field is related to connected objects for energy management. In just a few years, user optimization of energy consumption has become one of the key sectors for the IoT. According to the *Allied Market Research* report, the global smart thermostat industry was pegged at $1.36 billion in 2018 and is estimated to reach $8.78 billion by 2026[70]. *Nest* (a *Google* subsidiary) has already sold over 11 million smart thermostats worldwide[71]. They automatically adjust house temperature by means of a set of sensors and software that analyzes user behavior to save energy. These smart thermostats can also improve

70. *Smart Thermostat Market to Reach $8.78 Billion, Globally, by 2026 at 26.0% CAGR, Says Allied Market Research* (Bloomberg, Dec 11, 2019) www.bloomberg.com/press-releases/2019-12-11/smart-thermostat-market-to-reach-8-78-billion-globally-by-2026-at-26-0-cagr-says-allied-market-research

71. *Nest says it has sold over 11 million devices since 2011* (CNET Feb 7, 2018) www.cnet.com/news/nest-says-it-has-sold-over-11-million-devices-since-2011/

consumption management at district or even city level. They can be used to smooth consumption and thus reduce the consumption 'peak' between 6 and 8 pm, which represents the most significant infrastructure expense for energy suppliers and distributors. A number of energy providers in the United States (such as Texan company *Reliant*) have decided to give these connected thermostats to their subscribers[72]. Because they allow companies to acquire more detailed knowledge of user behavior and control their consumption, these connected thermostats, initially perceived as *B2C* (*Business to Consumer*) products, have become a leverage tool for optimizing energy production and distribution.

3.1 Cars and Connected Health

Cars are already among the connected objects most heavily equipped with sensors (radar, sonar, cameras, accelerometers, thermometers, humidity detectors, etc.). These sensors are now coordinated by increasingly powerful on-board computer systems, the functions of which are often managed by companies other than car manufacturers themselves. Hence Dieter Zetsche's, CEO of Mercedes-Benz, description of the car of the future as "*a smartphone on wheels*"[73]. By way of example, the volume of information generated by sensors on board the connected *Ford Fusion* was already 25 gigabytes of data per hour in 2012[74]. Now, with the development of driverless cars, terabytes of data will be processed by vehicle sensors[75]. While most of these sensors are used to analyze the vehicle's operating parameters, others are specifically intended to analyze the driver's physiological parameters or driving style. Beyond assessing the driver's level of vigilance, these sensors could become a valuable source of information, particularly with regard to the driver's state of health. Analysis of driving behavior by connected devices has also given rise

72. *In the world of Texas electricity, free is not always free (*Dallas Morning News, Oct 12, 2013) www.dallasnews.com/news/watchdog/2013/10/13/in-the-world-of-texas-electricity-free-is-not-always-free/

73. *Detroit Motor Show: Car firms take on the tech giants* (BBC News, Jan 13, 2015) www.bbc.com/news/business-30786709

74. *Ford Issues Predictions for Next Wave of Automotive Electronics Innovation* (Washington Times, Dec 27, 2012) www.washingtontimes.com/news/2012/dec/27/ford-predicts-next-auto-electronics-innovation/

75. *Les nouveaux défis de la cartographie routière pour les voitures autonomes* (Le Monde, March 10, 2017) www.lemonde.fr/pixels/article/2017/03/12/les-nouveaux-defis-de-la-cartographie-routiere-pour-les-voitures-autonomes_5093246_4408996.html

to experiments by insurance groups in order to adjust premiums (the '*Pay How You Drive*' principle). It should be noted that to date, these experiments have often been deemed too intrusive by potential policyholders[76].

For a number of years now, auto manufacturers have been experimenting with integrating connected sensors to collect the physiological parameters of a vehicle's driver. Carmaker *Ford*, for example, has been considering integrating sensors to monitor cardio-respiratory conditions or even problems of alertness[77]. Another risk of disease prevention and monitoring with *IoT* technologies concerns non-medical uses of this data. By getting to know their users' intimate reactions, connected objects may also give rise to entirely new forms of manipulation based on biological and behavioral analysis. Historian Yuval Harari summed it up as follows:

> It is crucial to remember that anger, joy, boredom and love are biological phenomena just like fever and a cough. The same technology that identifies coughs could also identify laughs. If corporations and governments start harvesting our biometric data en masse, they can get to know us far better than we know ourselves, and they can then not just predict our feelings but also manipulate our feelings and sell us anything they want — be it a product or a politician. Biometric monitoring would make Cambridge Analytica's data hacking tactics look like something from the Stone Age[78].

3.2 From Individual Cars... to Shared 'Robotaxis'?

IoT technologies combined with artificial intelligence technologies could lead to other radical changes in existing economic models. These new forms of economic 'rationalization' are the common thread in

76. *Assurances auto : êtes-vous prêt à tout dévoiler pour payer moins cher ?* (L'Express, February 2, 2016) votreargent.lexpress.fr/high-tech/assurances-auto-etes-vous-pret-a-tout-devoiler-pour-payer-moins-cher_1759408.html

77. *3 Ways Ford Cars Could Monitor Your Health. Ford is experimenting with car features that could help drivers with diabetes, heart problems, and more* (IEEE Spectrum, May 19, 2017) spectrum.ieee.org/the-human-os/biomedical/diagnostics/3-ways-ford-cars-could-monitor-your-health

78. *Yuval Noah Harari: the world after coronavirus* (Financial Times Mar 20, 2020) www.ft.com/content/ 19d90308-6858-11ea-a3c9-1fe6fedc-ca75?segmentid=acee4131-99c2-09d3-a635-873e61754ec6

industrial transformations in the automotive sector. The development of driverless cars could eventually lead to a decline in the number of cars sold and, according to some experts, could even signal the end of individual vehicle ownership[79]. Commercial transport would be provided by autonomous and shared cars and individual vehicle ownership could be reserved for 'leisure driving' segments. According to Andreas Tschiesner, automotive lead for Europe at *McKinsey*, the fleets of self-driving cars he calls "robotaxis" could upend manufacturers' business models (cf. Change in carmakers' income structure (source: *McKinsey*, *Financial Times*[80])).

Manufacturers would thus reinvent themselves as providers of transport services: "*Car brands typically earn $2,000 from a vehicle sale. That is just $0.01 per kilometre over the lifetime of a vehicle, whereas for robotaxis the potential is 20 to 25 cents per kilometre, so there is huge potential to capture more*"[81]. Carmakers' interest would consequently turn to boosting the number of trips made during the vehicle's lifetime and no longer to promoting the rapid replacement of their vehicles.

Beyond mere transport functions, a new source of value-added services for vehicle (and autonomous vehicle) manufacturers will be provided by leisure and information services on board vehicles (*in-car infotainment*). For example, communications groups and film production companies[82] are already investing to develop new formats for films, games and news content specifically designed for autonomous vehicles. According to *Allied Market Research*, the in-car infotainment market could reach $21 billion in 2026[83].

79. *Could Self-Driving Cars Spell the End of Ownership?* (Wall Street Journal, Dec 1, 2015) www.wsj.com/articles/could-self-driving-cars-spell-the-end-of-ownership-1448986572

80. *Race to build a million-mile car becomes a reality* (Financial Times, Jan 13, 2018) www.ft.com/content/1255be4c-f680-11e7-88f7-5465a6ce1a00

81. *Robotaxis: can automakers catch up with Google in driverless cars?* (Financial Times Jan 31, 2019) www.ft.com/content/dc111194-2313-11e9-b329-c7e6ceb5ffdf

82. *Why Hollywood Could Make Billions From Self-Driving Cars* (Hollywood Reporter Aug 28, 2017) www.hollywoodreporter.com/behind-screen/why-driving-cars-could-be-hollywoods-next-big-thing-1031554

83. *In-Car Infotainment Market by Installation Type and Component Global Opportunity Analysis and Industry Forecast, 2019–2026* (Allied Market Research, Jan 2020) www.alliedmarketresearch.com/in-car-infotainment-market

3.3 IoT and Urban Planning: New Political Challenges

The introduction of fleets of autonomous vehicles (AVs) could also have an impact on the organization of urban and suburban zones. If city parking (for vehicle recharging and maintenance) can be pushed out to the outskirts, these technologies could alter the proportion of building areas within urban spaces. But the design of the algorithms required to operate such fleets could generate new forms of geographic discrimination for users and create new challenges for the regulators of these technologies. Thus, in its survey on self-driving cars, *The Economist* draws a parallel between these new forms of algorithmic discrimination and older ones based on city architecture:

> For a start, AVs will record everything that happens in and around them. When a crime is committed, the police will ask nearby cars if they saw anything. [...] If, as seems likely, human-driven cars are gradually banned on safety grounds, passengers could lose the freedom to go anywhere they choose. The risk that not all robotaxis will serve all destinations could open the door to segregation and discrimination. [...] If all this sounds implausible, recall that Robert Moses notoriously designed the Southern State Parkway, linking New York City to Long Island's beaches, with low bridges to favour access by rich whites in cars, while discriminating against poor blacks in buses. And China's "social credit" system, which awards points based on people's behaviour, already restricts train travel for those who step out of line[84].

Unlike changing urban infrastructures of our cities, discriminations created by modifying *IoT* technologies or services could initially be invisible to citizens.

This will raise new questions over the use made of the data collected by connected objects and vehicles. As such, the *Washing-*

84. *Self-driving cars offer huge benefits - but have a dark side* (The Economist, Mar 1, 2018) www.economist.com/leaders/2018/03/01/self-driving-cars-offer-huge-benefits-but-have-a-dark-side w

ton Post reported on the "*sentry*" mode of *Tesla* connected cars, which enables the US police force to collect camera images in the event of accidents or offences occurring near the vehicle[85]. A connected car would thus serve as the eye of the authorities in police investigations.

"Another strategic objective for public officials will be to make the risks of misuses of technologies deployed in urban spaces visible to citizens…

Another strategic objective for public officials will be to make the risks of misuses of technologies deployed in urban spaces visible to citizens. This could take the form of education and awareness measures and the regulation of these technologies. Opportunities for democratic debate and consultation will also have to be provided to involve citizens upstream in the development of urban IoT technologies.

3.4 Risks of "Social Downgrading 4.0"?

The social risks generated by the combination of artificial intelligence and IoT technologies are becoming significant decision-making factors for all industrial stakeholders. For employees in the sectors targeted by transformations, the synergy between the IoT and artificial intelligence could lead to shifts in their core business or even their elimination. This is the case for transport, for example, with the arrival of autonomous vehicles. According to John Samuelsen, International President of TWU (Transport Workers Union of America), which represents nearly 150,000 workers, most of whom are involved in passenger transport, these technologies come with significant social risks:

> *Autonomous vehicles are "a terrible idea for transit".* In September 2018, Samuelsen traveled to Columbus to personally lead

85. *My car was in a hit-and-run. Then I learned it recorded the whole thing* (Washington Post, Feb 27, 2020) www.washingtonpost.com/technology/2020/02/27/tesla-sentry-mode/

> a protest over the city's AV shuttle pilots. Top of mind for Samuelsen is the impact of AV technology on his members' jobs. AV backers say driverless transit vehicles will need workers to collect fares, answer questions, and address safety issues, such as passenger harassment. But Samuelsen says that claim misses the point: "*Even if bus operator jobs were replaced with attendants, they would never earn an equal wage*." He says AV transit tech "*will be taking wealth right out of the working neighborhoods of America and delivering it to Wall Street and Silicon Valley*"[86].

For Kai-Fu Lee, the ethical and social consequences of introducing these technologies are already beginning to have an impact on decision-makers and especially on policy makers: "*They may well lead American politicians, ever fearful of interest groups and attack ads, to pump the brakes on widespread self-driving vehicle deployment. We've already seen early signs of this happening, with unions representing truck drivers successfully lobbying Congress in 2017 to exclude trucks from legislation aimed at speeding up autonomous-vehicle deployment*"[87].

3.5 Smart City: the Counterexample of Google in Toronto

Smart city technologies and services are among the most important market opportunities for IoT stakeholders. IoT technologies are involved in the implementation of all public policies at local level; from transportation infrastructures to control of large infrastructure networks, health care, energy management and environmental control. The governance of smart city projects has also become a strategic and political challenge for public sector players and citizens alike.

However, these projects can also give rise to abuse when public players are not able to control the strategic decisions of companies

86. *A Move for Driverless Mass Transit Hits Speed Bumps* (Wired, Aug 18, 2020) www.wired.com/story/driverless-mass-transit-hits-speed-bumps/

87. *AI Superpowers: China, Silicon Valley, and the New World Order* (Kai-Fu Lee, HMH Books 2018)

granted smart city contracts. This was the case with the city of Toronto when it tasked a Google subsidiary (*Sidewalk Labs*) with organizing smart city functions and services for its *Waterfront* district. Observers started noticing strange and disturbing similarities between *Google*'s smart city project and China's *Social Credit* strategies: rating certain behavior as 'good' and penalizing other behavior. Especially for citizens who refuse 'transparency' and do not provide their personal information. The Canadian newspaper *Globe & Mail* obtained the preparatory documents for this project, which described how the Google subsidiary had the "*power to levy its own property taxes, track and predict people's movements and control some public services. [...] an experience based, in part, on how much data they're willing to share, and which could ultimately be used to reward people for "good behavior""*[88]. It should be noted that it was the citizens of Toronto, buoyed by an ardent press campaign[89], who called into question the very existence of this initiative. In May 2020, the *Google* subsidiary announced that it was pulling out of its *Quayside* project for Toronto[90].

"Observers started noticing strange and disturbing similarities between *Google*'s smart city project and China's *Social Credit* strategies...

88. *Sidewalk Labs document reveals company's early vision for data collection, tax powers, criminal justice* (Globe & Mail Oct 30, 2019) www.theglobeandmail.com/business/article-sidewalk-labs-document-reveals-companys-early-plans-for-data/

89. *Google wants to run cities without being elected. Don't let it* (The Guardian Oct 24, 2017) www.theguardian.com/commentisfree/2017/oct/24/google-alphabet-sidewalk-labs-toronto

90. *Why we're no longer pursuing the Quayside project — and what's next for Sidewalk Labs* (Daniel L. Doctoroff, Medium May 7, 2020) medium.com/sidewalk-talk/why-were-no-longer-pursuing-the-quayside-project-and-what-s-next-for-sidewalk-labs-9a61de3fee3a

3.6 Social Acceptability Challenges of the IoT

Social acceptability of IoT technological innovations has become a crucial factor for all industrial stakeholders. Citizens seem to be increasingly dissatisfied with 'remuneration' for trading their personal data in return for a 'free' service. The more they learn of the risks of abuses from hacking of their data or the risks of generalized surveillance, the more reluctant they become. Requests from Internet platforms to obtain users' personal data receive a wide range of responses. As a

Morgan Stanley survey found, the degree of acceptance varies according to the country and cultural origins of interviewees:

> The limits of public tolerance for such nudging and nannying are not yet clear. "*There's definitely a crossover point where this goes from helpful to creepy*," says Mr Hocking. Morgan Stanley has done surveys asking people what level of price reduction they would require to share their data. He says respondents in Asia were most willing to trade data for a price cut. Westerners were less keen, and Germans the most wary of all[91].

While public opinion is becoming critical of the social and political risks of the IoT, this need for clarity could lead designers of the next generations of technologies to integrate these concerns upstream rather than risk repeating the kind of scandals witnessed in recent years with the Edward Snowden leaks, and more recently with the *Cambridge Analytica* scandal. According to *The Economist*, by helping to 'demine' the main risks associated with the IoT upstream, such heightened vigilance could paradoxically ensure greater durability for IoT technologies:

> These days, things are different. Blamed for everything from addicted children to nurturing terrorism, Big Tech has lost its Utopian shine. That disillusionment has fed back into gloomy predictions about the iot. In many ways, that is valuable, for if problems can be foreseen they can be more easily prevented. But if the techno-optimism that infused the 1990s and 2000s now looks naive, the techno-pessimism that is fashionable today can be similarly overdone. Like the original internet, the iot promises huge benefits. Unlike the original internet, the iot will mature in an age that has become sceptical about where a connected, computerised future might lead. If it has to earn the trust of its users, it will be the better for it in the long run[92].

91. *The Internet of Things* (The Economist Technology Quarterly, Sept 2019)

92. Ibid.

4

NEW REGULATORY CHALLENGES OF THE IoT

4.1 States and the IoT: Synergy or 'Uberization'?

Internet technologies have increasingly adopted the shapes and contours of States when their essential functions require the use of the network. Accordingly, the fundamental instruments of sovereignty are already indistinguishable from the tools of technological power. The IoT, whose technologies will be used in an increasing number of public sector activities, could further speed up this phenomenon. Public players' lack of control of IoT technologies could see them become ever-more dependent on digital players.

> **"The fundamental instruments of sovereignty are already indistinguishable from the tools of technological power…**

Back in 2011, during his hearing before the antitrust commission of the US Senate, Eric Schmidt, then CEO of *Google*, quoted Andy Grove, former CEO of Intel: "*This is easy to understand. High tech runs three-times faster than normal businesses. And the government runs three-times slower than normal businesses. So we have a nine-times gap"*[93]. Later, in 2013, Eric Schmidt confirmed in his book *The New Digital Age*[94] that for him, States had become too slow and inefficient to keep up with the speed of technological developments.

93. *Google's Eric Schmidt Expounds on His Senate Testimony* (Washington Post, Sep 30, 2011) www.washingtonpost.com/national/on-leadership/googles-eric-schmidt-expounds-on-his-senate-testimony/2011/09/30/gIQAPyVgCL_story.html

94. *The New Digital Age: Transforming Nations, Businesses, and Our Lives* by Eric Schmidt and Jared Cohen (Ed. John Murray 2014)

Above and beyond the uberization of entire economic sectors, the sovereign functions of States can now be 'privatized' through the introduction of artificial intelligence and Big Data technologies. This Big Data analysis logic has enabled *Palantir*, the company founded by Peter Thiel and originally financed by *In-Q-Tel*, the CIA's venture fund, to equip almost all US intelligence services for the fight against terrorism. In France, the recent renewal of the agreement signed by the French intelligence agency *DGSI* (*General Directorate for Internal Security)* with *Palantir*[95] underlined the risks of political dependency linked to technological dependency. Especially as *Palantir* has been associated with the *Cambridge Analytica*[96] scandal and its founder, a close ally of Donald Trump, was a member of his presidential transition team.

It must be emphasized that whenever States have perceived threats to their 'traditional' sovereign prerogatives, they have demonstrated a reactivity unlike that which they deploy in the field of competition regulation and antitrust laws in particular. For example: when *Facebook* announced its "*Libra*" cryptocurrency project, the European and US authorities immediately expressed their readiness to regulate or even prohibit such an initiative[97]. Besides being a new channel for the collection of personal data, this currency could eventually have competed with sovereign currencies, facilitated money laundering or made the financing of terrorism untraceable. Thus, in a matter of weeks, the main project partners (*Visa, MasterCard, eBay* and *PayPal*) stopped working with *Facebook* for fear of alienating their government contacts. *Facebook*, which saw *Libra* as a way to diversify its activities in a strategic sector after the *Cambridge Analytica* scandal, was thus forced to scale down its ambitions. Conversely, when in March 2019 the European Union fined *Google* €1.49 billion for abuse of a dominant position, this sanction came after many years of investigation (some of the allegations against *Google* dated back to 2006). Moreover, such economic sanctions have so far shown only a limited impact on the company's activity.

95. *La société américaine Palantir, proche de la CIA, est toujours indispensable aux espions français* (Le Monde, November 29, 2019) www.lemonde.fr/economie/article/2019/11/29/l-americain-palantir-est-toujours-indispensable-aux-espions-francais_6021016_3234.html

96. *Palantir, l'embarrassant poisson-pilote du big data* (Le Monde, October 9, 2018) www.lemonde.fr/pixels/article/2018/10/09/palantir-l-embarrassant-poisson-pilote-du-big-data_5366568_4408996.html

97. *Facebook Unveils Cryptocurrency Libra in Bid to Reshape Finance* (Wall Street Journal, June 18, 2019) www.wsj.com/articles/facebook-unveils-crypto-wallet-based-on-currency-libra-11560850141

Care should be taken to ensure that the technologies used by France (and more widely by EU States) are controlled and that they clearly contribute to the general interest. To this end, it would be advisable to create the role of coordinator of State technologies, like the "*Chief Technology Officer*" (*CTO*) of the US federal administration. This kind of national coordinator would be tasked with ensuring that all technologies put in place by governments are controlled by State officials, that they are sustainable and that they cannot lead to uses that are not in citizens' interests. For this State technologies coordinator to fully exercise their interministerial mission, this role should be directly attached to the Prime Minister's office and the coordinator should have their own team of experts to analyze the matters to be dealt with from technological, economic, industrial and social angles.

4.2 IoT and Health: Towards Social Control Technologies?

Even before the *COVID-19* pandemic, a number of scientists had suggested integrating sensor networks and artificial intelligence systems for the early detection of epidemics. The urgency of the pandemic now makes even more likely the deployment of IoT technologies to contain biological threats, whether these be *wearable* connected objects (headsets, rings, glasses or wristbands fitted with sensors), drones for thermal imaging or urban sensor networks[98]. IoT technologies that can be used in this field are becoming increasingly diversified as new artificial intelligence-based analytical methods are developed. These algorithms can indeed reveal (or infer) information on a person's state of health from seemingly trivial information. As such the possibility of cardiac or circulatory disorders can be predicted by analyzing a person's movements over time. *Facebook* has even developed patents on the constant analysis of its users' movements[99]. A number of companies are also

98. *Internet of Things for Current COVID-19 and Future Pandemics: An Exploratory Study* by M. Nasajpour, S. Pouriyeh, M. Parizi, M. Dorodchi, M. Valero, H. Arabnia Dept of Information Technology and Dept of Software Engineering and Game Development, Kennesaw State University, Department of Computer Science, University of North Carolina and University of Georgia (article submitted on Jul 22, 2020) arxiv.org/pdf/2007.11147.pdf

99. *What 7 Creepy Patents Reveal about Facebook* (New York Times, June 21, 2018) nytimes.com/interactive/2018/06/21/opinion/sunday/facebook-patents-privacy.html

working on detecting the early signs of *COVID-19* infection by analyzing the heart rate and activity of smart watch wearers[100]. Research teams from *MIT*[101] and the École Polytechnique Fédérale de Lausanne *(EPFL)*[102] have recently announced that they are developing artificial intelligence algorithms that can detect people carrying the coronavirus from an analysis of the sound of a forced cough via smartphone microphones. These *COVID-19* early detection systems, designed after analyzing tens of thousands of recordings, would make it possible to discover sound variations inaudible to the human ear in people affected by the virus, including those who are asymptomatic.

On a different note, several companies in China are experimenting headsets with built-in brain sensors that analyze the brain waves of their employees in order to detect stress or anger, or when they are falling asleep[103]. *Amazon* recently launched a new generation of *Halo* wristbands with sensors to analyze their wearers' emotional state and physiological parameters[104]. Another recent release, the new version of the *Apple Watch* is touted as being able to detect stress levels and prevent panic attacks. This function will use the combined analysis of blood oxygen levels and heart and respiratory rates, alongside other parameters such as the user's movements or location[105].

Here again, it will be the measures taken to ensure the security of the data collected by these sensors that will determine whether these devices are used for prevention, control or manipulation of individuals. Indeed, as several authors have noted, there is a fine line between the prevention of risky behavior and the conditioning of users via connected objects. This trend towards controlling populations could in effect mark the transition from social engineering to social control assisted by the IoT.

100. *Could You Have Covid-19? Soon Your Smartwatch or Smart Ring Might Tell You* (Wall Street Journal, Jul 28, 2020) www.wsj.com/articles/could-you-have-covid-19-soon-your-smartwatch-or-smart-ring-might-tell-you-11595949072

101. *Artificial intelligence model detects asymptomatic Covid-19 infections through cellphone-recorded coughs Results might provide a convenient screening tool for people who may not suspect they are infected.* (MIT News Office October 29, 2020) news.mit.edu/2020/covid-19-cough-cellphone-detection-1029

102. *A new app can help detect the coronavirus - Ecole Polytechnique Fédérale de Lausanne* (Medical Xpress, Apr 10, 2020)https://medicalxpress.com/news/2020-04-app-coronavirus.html

103. *'Forget the Facebook leak': China is mining data directly from workers' brains on an industrial scale* (South China Morning Post, Apr 29, 2018) https://www.scmp.com/news/china/society/article/2143899/forget-facebook-leak-china-mining-data-directly-workers-brains

104. *Amazon Announces Halo, a Fitness Band and App that Scans Your Body and Voice* (The Verge, Aug 27, 2020) www.theverge.com/ 2020/8/27/21402493/amazon-halo-band-health-fitness-body-scan-tone-emotion-activity-sleep

105. *Apple Watch may soon be able to detect panic attacks before they happen* (SlashGear, May 10, 2020) www.slashgear.com/apple-watch-may-soon-be-able-to-detect-panic-attacks-before-they-happen-10619926

In the extreme, according to the *Frost & Sullivan* research firm, the most 'efficient' response for fighting pandemics would be to create a global network of biosensors. This sensor network would enable worldwide early detection of biological threats. However, as the authors note, such a proposal, which would be among the most important technological market opportunities ever designed for the IoT, would inevitably run into opposition from public opinion due to the restrictions on freedoms it entails:

> The simple answer might for enterprises, cities, and national governments to collectively create a massive global network of sensors to detect viruses. However, this would require planning and implementation on a global scale that would tax the very foundations of democracy and obligate governments to place the needs of the planet ahead of the needs of their citizens. The most logical solution is often the most difficult to implement. The amount of planning required to make this solution a reality would, arguably, make it one of the most significant achievements in the history of mankind. [...] I find this to be the "holy grail" of IoT opportunity in the long term[106].

The fascination with 'techno-efficiency' expressed by some IoT tech players brings to mind the "*technological solutionism*" described by Evgeny Morozov in his book '*To Save Everything, Click Here*'[107]. This fascination is even more pronounced when it comes to developing IoT technologies in healthcare. This trend is not exclusive to authoritarian regimes, but is also seen in economic actors or governments which assess the benefit/risk ratio of these technologies and consider democracy and protection of freedoms as mere adjustment variables...

106. *The Next Generation of IoT – Addressing the Coronavirus and Preventing Future Outbreaks* (Frost & Sullivan, Jan 31, 2020) ww2.frost.com/frost-perspectives/the-next-generation-of-iot-addressing-the-coronavirus-and-preventing-future-outbreaks/

107. *To Save Everything, Click Here: Technology, Solutionism, and the Urge to Fix Problems that Don't Exist* (Evgeny Morozov, Ed. Penguin 2013)

4.3 Health Insurance and the IoT: Shifting from Treatment to Prevention

Collecting and processing health data have become strategic challenges for tech companies. Connected health devices, and more specifically technologies for monitoring and preventing disease, are becoming the new focus of expansion for technology manufacturers. More cost-effective personalized prevention and monitoring systems can now be set up thanks to the new generations of connected medical devices that can continuously monitor users' activities and physiological parameters. These connected objects, with users on a daily basis, should enable the early diagnosis of chronic diseases (cancer, diabetes, asthma, cardiovascular disease, etc.). They should also make it possible to modify user behavior so as to control risk factors, such as a sedentary lifestyle or obesity.

Other key sectors of European economies could thus be transformed through the introduction of new generations of IoT services; namely, health and insurance. Indeed, tech companies could gain a foothold in the prudential sector (banking and insurance) and shift the health economy's center of gravity towards prevention. On this point, see the *Goldman Sachs*[108] 2015 report on connected health, which estimates savings of $305 billion dollars could be made in the United States by introducing IoT technologies in the health sector. Of these savings, $200 billion would be derived from improved chronic disease prevention and management, especially cardiovascular disease, asthma and diabetes. These savings would represent nearly 10% of total health spending in the United States ($3.6 trillion in 2018)[109].

This same risk prevention dynamic was already included in the *HR1313* bill introduced in the US Congress in 2017. This bill's stated objective was to develop measures for the prevention and early detection of

108. *The Digital Revolution comes to US Healthcare* (Goldman Sachs Equity Research 2015) www.anderson.ucla.edu/Documents/areas/adm/acis/library/DigitalRevolutionGS.pdf

109. *National Health Expenditures 2018* (U.S. Centers for Medicare & Medicaid Services 2019) www.cms.gov/files/document/highlights.pdf

disease by means of large-scale genetic tests carried out in companies. The law envisaged deploying genetic tests in American companies, imposing penalties of $4,000 to $5,000 a year against employees who refused to undergo this 'genetic screening'[110].

One of the challenges for public authorities in France and Europe will be to ensure that *IoT* evolutions do not undermine our social model in favor of systematic control of individuals. All the more so as data from genomics will soon be integrated into these platforms. From now on, safeguarding our social welfare model will fall under digital sovereignty. The implementation of a logic of hyper-individualization of health coverage would go against our social model, which is based on solidarity and the pooling of risks across the whole of society. However, connected health devices already allow major platforms to supplement their information on users in order to refine their profiles. This would enable an accurate health risk assessment for every single person, an unprecedented advance. As Mr Demurger, Managing Director of *MAIF*, stated: *"This has upended the world of insurance. Insurers have traditionally had very little data on their clients but a large number of clients. Thanks to big data, we can now collect a large amount of behavioral data on a single person"* [111].

The health insurance sector is therefore becoming one of the priority targets for major tech companies. Rather than becoming directly involved in healthcare, a sector which requires significant and hazardous long-term investments, big Internet platforms can now use the data accumulated on their users to provide disease prevention services. By means of connected sensors associated with artificial intelligence systems, such data will allow them to accurately model the risks related to each individual's health and thus optimize the profits of their insurance services. *Google* (via *Alphabet*) has just announced that it is moving into the health insurance sector with its new divi-

110. *Employees who decline genetic testing could face penalties under proposed bill* (Washington Post, March 11, 2017) www.washingtonpost.com/news/to-your-health/wp/2017/03/11/employees-who-decline-genetic-testing-could-face-penalities-under-proposed-bill/

111. *Santé: faut-il faire payer les assurés en fonction de leur mode de vie ?* (Le Monde, September 6, 2016) www.lemonde.fr/economie/article/2016/09/06/assurance-votre-vie-privee-vaut-bien-une-ristourne_4993378_3234.html

sion, *Coefficient*: "*Verily, Alphabet's healthcare business, is overseeing a new subsidiary that will offer stop-loss insurance to employers. Coefficient Insurance Company is backed by insurance megacorp Swiss Re, and relies on data analytics to predict and reduce risk. [...] Verily is responsible for a suite of health gadgets, medical research and COVID-19 testing solutions, and it's the company behind Project Baseline, a comprehensive four-year study into human health around the globe. To that end, Verily created a smart watch with electrocardiogram technology built-in".*[112].

In this field, the fact that the French Ministry of Health has set up a *Health Data Hub*, designed to become a one-stop shop for access to all health data, promises developments in connected health. This platform aims to develop new artificial intelligence services applied to health. However, as health professionals and medical IT experts have pointed out, having this hub hosted by *Microsoft*[113] was both a risk in terms of sovereignty over sensitive data and a missed opportunity to develop essential know-how in the French connected health ecosystem[114]. Faced with controversies over choosing *Microsoft*, the government recently announced that it now intends to "repatriate" hosting to French or European companies[115]. Meanwhile, the French data protection authority *CNIL* took note of the decision of the Court of Justice of the European Union to terminate the *Privacy Shield* which had allowed US companies to transfer Europeans' personal data to the United States. With regard to the hosting of the *Health Data Hub* and similar platforms, "*according to the CNIL, the changes should take place as soon as possible*"[116]. The *CNIL*'s opinion is a *de facto* recognition of the principles of *data localization/data residency*, particularly for sensitive data. If it were to be codified in an EU directive, this would entail a departure from the principles on which the activities and business models of large tech companies are based.

112. *Alphabet's Verily begins offering stop-loss health insurance* (yahoo!finance, August 25, 2020) https://au.finance.yahoo.com/news/alphabet-verily-health-inscurance-coefficient-212604107.html

113. *« L'exploitation de données de santé sur une plate-forme de Microsoft expose à des risques multiples »* (article published in *Le Monde* on December 10, 2019) www.lemonde.fr/idees/article/2019/12/10/l-exploitation-de-donnees-de-sante-sur-une-plate-forme-de-microsoft-expose-a-des-risques-multiples_6022274_3232.html

114. *Health Data Hub : « Le choix de Microsoft, un contresens industriel ! » (interview Bernard Benhamou* Le Point, June 18, 2020) www.lepoint.fr/technologie/health-data-hub-le-choix-de-microsoft-et-un-contresens-industriel-10-06-2020-2379394_58.php

115. *Microsoft doit se retirer du Health Data Hub, d'après la Cnil* (L'Usine Digitale October 9, 2020) www.usine-digitale.fr/article/microsoft-doit-se-retirer-du-health-data-hub-d-apres-la-cnil.N1014634

116. *La Cnil réclame l'arrêt de l'hébergement des données de santé des Français par Microsoft* (L'Obs, 9 octobre 2020) www.nouvelobs.com/high-tech/20201009.OBS34527/la-cnil-reclame-l-arret-de-l-hebergement-des-donnees-de-sante-des-francais-par-microsoft.html

4.4 Data Brokers: a 'Toxic' Business Model?

The mass collection of personal data is now a political issue for all EU regulators. Regulators have thus started looking into the little-known activity of data brokers in both the United States and Europe, where their activities could be considered as being contrary to the GDPR, given that data brokers aggregate personal data from many different sources and consolidate user profiles, the largest of which number in the hundreds of millions. These profiles can in some cases reach several *tens of thousands of parameters per person*. These profiles are then sold on to banks, insurers, distribution chains, governments and even other data brokers to consolidate their profile databases. It should be noted that it was in the aftermath of the *Cambridge Analytica* scandal that *Facebook* announced the end of its partnership with data brokers for targeted ads[117].

> **"The European Commission forecasts the data market in Europe could be worth as much as €106.8bn by 2020…**

While their activities are practically unknown to the general public, data brokers occupy a strategic place in the economy of major Internet platforms. The European Commission forecasts the data market in Europe could be worth as much as €106.8bn by 2020[118]. IoT is now among the major data collection sources for data brokers. People's medical, religious, sporting and political profiles can all be drawn up simply by analyzing their geolocation data.

The recent termination of the transatlantic *Privacy Shield* agreement, further to the termination of its predecessor *Safe Harbor* in 2015, makes the durability of data brokers' business model even more uncertain. Indeed, the very nature of their economic model labels such companies a risk factor for the uncontrolled dissemination of information held on Internet users.

117. *Facebook ends data broker partnerships in blow to targeted ads* (VentureBeat, Mar 28, 2018) venturebeat.com/2018/03/28/facebook-ends-data-broker-partnerships-in-blow-to-targeted-ads/

118. *Data brokers: regulators try to rein in the 'privacy deathstars'* (Financial Times, Jan 9, 2019) www.ft.com/content/f1590694-fe68-11e8-aebf-99e208d3e521

4.4.1 Is it Impossible to Regulate Data Brokers?

The *GDPR* has started to force data brokers to introduce an ethical dimension into their activities. John Mitchison, Director of Policy and Compliance at the *Data & Marketing Association* (the trade organization for data companies and marketers) described the impact of the *GDPR* on the organization of data broker activities in Europe:

> When GDPR came in, people were forced to look at the legislation and realised the tech they were using was right at the boundary and limit of the existing [law]. One of the most drastic things I've seen happen is all of these companies have radically reduced the number of third-party companies they will accept data from. You now need evidence that data were collected properly so they've weeded out a lot of suppliers that don't meet those standards[119].

In its report on data brokers, written before the *Cambridge Analytica* scandal, the American *FTC* (*Federal Trade Commission*) was already concerned about the extent of personal information held by these companies, as well as their considerable ability to 'infer' people's behavior:

> Data brokers combine and analyze data about consumers to make potentially sensitive inferences. Data brokers infer consumer interests from the data that they collect. They use those interests, along with other information, to place consumers in categories. Some categories may seem innocuous such as "Dog Owner," "Winter Activity Enthusiast," or "Mail Order Responder." Potentially sensitive categories include those that primarily focus on ethnicity and income levels, such as "Urban Scramble" and "Mobile Mixers," both of which include a high concentration of Latinos and African Americans with low incomes[120].

119. *Data brokers: regulators try to rein in the 'privacy deathstars'* (Financial Times, Jan 9, 2019) www.ft.com/content/f1590694-fe68-11e8-aebf-99e208d3e521

120. *Data Brokers: A Call for Transparency and Accountability* (Federal Trade Commission report, May 2014) www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

4.4.2 Greater Transparency and Visibility for Data Brokers

Data brokers have so far benefited from the invisibility in which they carry out their user profile aggregation. In addition to obtaining user consent for transmission of their personal data, it would be advisable to display all structures receiving collected information. The *FTC* suggested setting up a centralized mechanism so that users could choose whether or not to transmit their personal data:

> Given the current invisibility of data brokers, the question remains: If these access and opt-out tools were to exist and be available to consumers through a centralized mechanism, how would a consumer learn about them? One way legislation could increase the visibility of the data broker industry and the access and opt-out tools they offer is to require that consumer-facing sources provide a prominent notice to consumers that they share consumer data with data brokers and give consumers choices, such as the ability to opt out of sharing their information with data brokers[121].

Provisions of this type have since been implemented in Europe within the framework of the *GDPR;* however, as Antoine Dubus, researcher at the *Institut Mines-Télécom*, points out, this transparency is not enough to reduce risks for users:

> Contrary to first impressions, our initial results show a risk of intensification of personal data collection and sale by data brokers, linked to the application of the new obligations defined by the *GDPR*. In reality, complying with legal obligations raises the cost of collecting personal data. Data brokers will therefore seek to optimize their profit either by shifting their collection activity to more profitable data, or to other consumers not initially targeted. Our results also suggest that companies purchasing ser-

121. *Ibid.*

vices from data brokers face a prisoner's dilemma. In the case of data brokers, this principle is characterized as follows: companies' profits would be increased if none of them used the services of a data broker. Nevertheless, it is not in any company's interest to be the only one not to deal with data brokers, because its competitors would then gain a dominant position. Our economic analysis therefore suggests that protection authorities could help companies out of this prisoner's dilemma by offering trust marks, for example, to certify that an organization does not use services based on the use of customers' personal data without their knowledge. This would help cut down on the amount of personal data collected by data brokers[122].

4.4.3 European Data Regulation: the Prospects of the *Data Governance Act*

Beyond the *General Data Protection Regulation (GDPR),* new European data market activities required the implementation of new forms of regulation of this sector. By launching the *Data Governance Act*[123], the European Commission sought to put an end to the legal and technological uncertainties prevailing in the data market. This involved establishing control over the activity of data brokers, especially for data from the industrial IoT, personal data and also public sector information.

Due to the lack of specific regulations, data brokers contributed to the dissemination of personal data and to the development of undesired uses of this data. Owing to their business model, these companies also participated in data concentration in the hands of major tech platforms. So, as Commission Executive Vice-President Margrethe Vestager noted at the launch of the Data Governance Act: *"It is intended as an alternative model to the data-handling practices of big tech platforms*.[124]"

122. *Les effets du RGPD sur la collecte et la monétisation des données personnelles* (Chaire Valeurs et Politiques des Informations Personnelles - Institut Mines-Télécom, May 10, 2019) cvpip.wp.imt.fr/2019/05/10/les-effets-du-rgpd-sur-la-collecte-et-la-monetisation-des-donnees-personnelles/

123. *Regulation of the European Parliament and of the Council on European Data Governance* (Data Governance Act) (Nov 25, 2020) ec.europa.eu/newsroom/dae/document.cfm?doc_id=71222

124. *Speech by Executive Vice-President Vestager at the Press Conference on the Data Governance Act and the Action Plan on Intellectual Property* (Nov 25, 2020) ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_2210

European data sharing companies or *data intermediaries* will have to function strictly as neutral intermediaries whose activity will consist of linking data holders and data users, due to new limits imposed on those involved in this data sharing. Thus, to avoid resale and data consolidation between data brokers, the *Data Governance Act* provides that data cannot be resold to other *data intermediaries*:

> A key element to bring trust and more control for data holder and data users in data sharing services is the neutrality of data sharing service providers as regards the data exchanged between data holders and data users. It is therefore necessary that data sharing service providers act only as intermediaries in the transactions, and do not use the data exchanged for any other purpose. This will also require structural separation between the data sharing service and any other services provided, so as to avoid issues of conflict of interest. This means that the data sharing service should be provided through a legal entity that is separate from the other activities of that data sharing provider[125].

In order to mitigate the risks associated with the use of public sector information, the conditions for re-using this data will be set by contract and may no longer exceed a period of three years. The *Data Governance Act* thus provides for the creation of new *European data spaces* which will cover areas such as health, mobility, manufacturing, financial services, energy, agriculture and thematic areas, such as the *European Green Deal* or *European data spaces* for public administration and skills.

4.4.4 The IoT Will Give Data Brokers Even More 'Intrusive' Capacities

Through the proliferation of information sources and the possibility of collecting information on users' most trivial actions, the Internet

125. *Regulation of the European Parliament and of the Council on European Data Governance* (Data Governance Act) (Nov 25, 2020) https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=71222

of Things gives data brokers new tools to consolidate user profiles.

Techniques like data minimization or aggregation of users' data may not therefore be sufficient to safeguard users' privacy. In fact, behavior patterns associated with sensitive data can already be inferred by artificial intelligence systems through analysis of seemingly insignificant data[126]. This is the case, for example, with the *Nest Protect* smoke detector, which has a presence sensor that switches on a night light when someone walks by the detector at night. The information from this 'additional' function could have significant consequences on the user's profile, since the time and the number of times someone passes by this sensor could be indicative of behavioral disorders or conditions. Once submitted to risk analysis algorithms, such data could then be used to modify the user's insurance profile.

Other forms of inference regarding sensitive data can come from analyzing information from smart electricity meters. Ethnic or religious user profiling can subsequently be carried out by analyzing energy consumption patterns. For example, reduced or very low power consumption at specific times makes it possible to infer whether users change their consumption patterns during Ramadan, or on Friday evenings and Saturdays for those observing the Shabbat.

4.4.5 Security Risks Inherent to Data Broker Activities

More recently, in the United States, it was the *NSA (National Security Agency)* that expressed concern about the uncontrolled dissemination of geolocation data on US government agents. This meant that it was possible via data brokers to track people's movements and know what they were doing. This created a vulnerability for government agents, and military and intelligence agents especially:

126. Sensitive data (definition of the European Commission): personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs; trade-union membership; genetic data, biometric data processed solely to identify a human being; health-related data; data concerning a person's sex life or sexual orientation. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en

> The National Security Agency issued new guidance on Tuesday for military and intelligence-community personnel, warning about the risks of cellphone location tracking through apps, wireless networks and Bluetooth technology. The detailed warning from one of the nation's top intelligence agencies is an acknowledgement that Silicon Valley's practice of collecting and selling cellphone location information for advertising and marketing purposes poses a serious national-security risk to many inside the government[127].

Following the *Cambridge Analytica* scandal, some researchers even draw a parallel between the security risks from weapons dissemination, and the social and political risks arising from the dissemination of sensitive data on individuals which, in turn, can become weapons[128]. Initially, regulations were designed 'downstream' of data capture, regulators believing that this would suffice to limit the risks of abuses from the Internet and subsequently from the Internet of Things. For *Harvard* professor Shoshana Zuboff, data broker activities contribute to shifting our societies towards what she calls "*surveillance capitalism*":

> In this new phase of capitalism's development, it's the raw material of human nature that drives a new market dynamic, in which predictions of our behavior are told and then sold. The economic imperatives of this new capitalism produce extreme asymmetries of knowledge and the power that accrues from that knowledge. This is unprecedented territory with profound consequences for 21st century society[129].

For these technologies to be able to develop without compromising European principles and values, mechanisms will be required to limit the collection, storage and circulation of data from connected objects.

127. *NSA Warns Cellphone Location Data Could Pose National-Security Threat* (The Wall Street Journal, Aug 4, 2020) www.wsj.com/articles/nsa-warns-cellphone-location-data-could-pose-national-security-threat-11596563156

128. *Weaponizing the Digital Influence Machine: The Political Perils of Online Ad Tech* (Data & Society Report, Oct 17, 2018) datasociety.net/library/weaponizing-the-digital-

129. *Twenty years of surveillance marketing - Shoshana Zuboff* (Wired Magazine Nov 21, 2018) www.wired.com/beyond-the-beyond/2018/11/twenty-years-surveillance-marketing/

4.5 IoT and "*Behavioral Surplus*"

The major Internet platforms discovered that they could obtain valuable information on their users' personalities, convictions, habits and personal histories by analyzing their activities. Once collected and analyzed, this information turned out to be a potent way of influencing the consumption behavior of users of these platforms and even of shaping certain convictions. This principle was invented by *Google* in the early years of its search engine development and has been described by Shoshana Zuboff as corresponding to an analysis of what she calls "*behavioral surplus*"[130]. It began when *Google* decided to analyze all user requests very early on, and not just data to improve search engine results. With this additional information, *Google* has been able to extensively analyze the behaviors and interests of billions of users. Such information not only allowed it to improve the effectiveness of its advertising but also to act over time on user behavior. Indeed, by analyzing users' reactions, they could be sent targeted messages according to their mood, location, family or professional situation or their religious and political convictions.

> **"Privacy regulations could become so restrictive that companies will be forced to move to a more decentralized model. They might realize that storing and collecting all this personal information is just not worth their while anymore..."**
>
> **Lalana Kagal**

IoT technologies will trigger a second phase of this *behavioral surplus* which, beyond online information interactions, will allow data to be collected on users' everyday behavior. Indeed, the Internet user profiles already constructed by micro-targeting platforms significantly increase the effectiveness of advertisers' approaches. By connecting previously 'inanimate' objects and allowing them to 'speak' about their users, these technologies reveal behaviors and reactions that were not previously visible to data brokers. As Shoshana Zuboff points out: *"The research director*

130. *The Age of Surveillance Capitalism. Shoshana Zuboff* (The Discovery of Behavioral Surplus, page 63) (Public Affairs 2019) https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook

of Gartner, the well-respected business advisory and research firm, makes the point unambiguously when he observes that mastery of the "internet of things" will serve as "a key enabler in the transformation of business models from 'guaranteed levels of performance' to "guaranteed outcomes""[131].

4.6 New Architectures to Protect Privacy?

In view of these data aggregator giants, it will be a major legal and technological challenge to ensure that Internet users have better control over their data. New technological and legal architectures will have to be implemented to guarantee interoperability and portability between the various platforms that process IoT data. Lalana Kagal from *MIT*'s *Computer Science and Artificial Intelligence Laboratory* expects changes in personal data regulations to encourage these companies to review the architecture of their applications: "*Privacy regulations could become so restrictive that companies will be forced to move to a more decentralized model. They might realize that storing and collecting all this personal information is just not worth their while anymore*"[132].

Many longstanding Internet actors have offered new technological architectures to help users better control their personal data online, including the inventor of the World Wide Web, Tim Berners-Lee, with his project *Solid*[133]. This project, developed after the *Cambridge Analytica* scandal, is based on the principle of 'structural separation' between the data entered by users and the applications that process them. According to Tim Berners-Lee: *"There's a very strong need today to separate the apps from data storage. These programs can access and process your photos, your information, your contacts, and so on, that's not a problem. You should have complete control of your data. You should be the one to authorize any given service to access it."*[134]

131. *The Age of Surveillance Capitalism. Shoshana Zuboff* (Public Affairs 2019)

132. *A plan to redesign the internet could make apps that no one controls* Will Douglas Heaven (MIT Technology Review, Jul 1, 2020) www.technologyreview.com/2020/07/01/1004725/redesign-internet-apps-no-one-controls-data-privacy-innovation-cloud/

133. *Ibid.*

134. *Les solutions de Tim Berners-Lee pour sauver le web* (Le Temps, March 12, 2019) www.letemps.ch/economie/solutions-tim-bernerslee-sauver-web

Similarly, in his op-ed for the *Electronic Frontier Foundation*, author Cory Doctorow described the need to create new information intermediaries who could act in the place and on behalf of users during collection and use of their personal data. The idea behind his proposal was to open up big tech information silos and ensure their interoperability. Another aim would be to ensure that data was no longer being used and disseminated without any control. According to Cory Doctorow, those acting on behalf of users should be governed by new rules: *"The data shared should be minimized to what is actually necessary to achieve interoperability. And companies that collect data through these new interoperable interfaces should not be allowed to monetize that data in any way, including using it to profile users for ads"*[135].

4.7 What Regulation for IoT Technologies?

Another platform regulation tool concerns the analysis of the algorithms that process personal data. Transparency with regard to the '*Code*' of these algorithms could soon become mandatory for democratic societies. Regulation could apply in particular to the design of algorithms for connected devices that will impact people's safety. An example of this would be the algorithms ensuring the operation of autonomous vehicles. The *MIT Media Lab* set up its *Moral Machine* project to analyze users' ethical and moral choices in the event of accidents involving driverless cars. An international survey was conducted on people from 233 different countries and territories. Analysis of this survey reveals the consensus points but also the differences in users' ethical choices according to their country of origin (see diagram *MIT Moral Machine*[136]).

For preeminent expert on Internet law, Lawrence Lessig[137], the '*Code*' of the algorithms that are crucial to citizens' lives must be controlled by them and no longer covertly designed by companies without any

135. *A Legislative Path to an Interoperable Internet* (Bennett Cyphers and Cory Doctorow, Electronic Frontier Foundation, Jul 28, 2020) www.eff.org/deeplinks/2020/07/legislative-path-interoperable-internet

136. *The Moral Machine Experiment* (E. Awad, S. Dsouza, R. Kim, J. Schulz, J. Henrich, A. Shariff, J-F. Bonnefon & I. Rahwan - Nature, Nature, Oct 24, 2018) www.americaninno.com/wp-content/uploads/2017/05/The-MM-Experiment.pdf

137. *Code and other Laws of Cyberespace,* Lawrence Lessig (Basic Books, 1999)

democratic control. Likewise, in his book *The Black Box Society*, academic Frank Pasquale calls for transparency for these algorithms which have a major impact on our societies: "*Demanding transparency is only the first step. An intelligible society would assure that key decisions of its most important firms are fair, nondiscriminatory, and open to criticism. Silicon Valley and Wall Street need to accept as much accountability as they impose on others*"[138]. This need for regulation will be all the more important for the Internet of Things as new generations of connected devices will be present in users' environments without their necessarily being aware. So, whether these concern environmental control, autonomous transport or smart city sensors, the technologies that will collect and process this information must be under citizens' control. But regulations to impose greater transparency on these platforms, and interoperability with their competitors, are still hampered by the speed with which technological actors evolve. Rather than making public the code of these algorithms, which are crucial for economic actors and for the democratic operation of our companies, Frank Pasquale suggests creating mechanisms for experts to audit the code (known as "*qualified transparency*"). In Europe, the principle of the transparency of crucial algorithms already appears to be a necessity for regulators. Margrethe Vestager announced that she wished to include provisions in the *Digital Services Act*[139] to ensure transparency of the algorithms of big tech companies. According to the Vice-President of the European Commission: *"So we can't just leave decisions which affect the future of our democracy to be made in the secrecy of a few corporate boardrooms"*[140].

> **"So we can't just leave decisions which affect the future of our democracy to be made in the secrecy of a few corporate boardrooms...**
>
> **Margrethe Vestager**

138. *The Black Box Society* by Frank Pasquale (Harvard University Press 2015)

139. Regulation of the European Parliament and of The Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (Dec 15, 2020) https://ec.europa.eu/info/sites/info/files/proposal_for_a_regulation_on_a_single_market_for_digital_services.pdf

140. *Algorithms and democracy* (Margrethe Vestager at AlgorithmWatch Online Policy Dialogue, 30 octobre 2020) https://ec.europa.eu/commission/commissioners/2019-2024/vestager/announcements/algorithms-and-democracy-algorithmwatch-online-policy-dialogue-30-october-2020_en

As well as regulating existing platforms, European industrial actors must also be able to develop technologies that respect citizens' principles and values. They could pioneer alternatives to existing platforms that would not be based on extracting user data for advertising purposes. Surprisingly, in the wake of the Snowden affair and the more recent *Cambridge Analytica* scandal, Europe has a window of opportunity for an industrial rebound based on technologies that will ensure a better protection of freedoms and individuals. The risks of a systemic trust crisis are so great that business models focusing on personal data and micro-targeting now appear risky to investors, due to the uncertainties regarding changes in the legal framework of big tech companies, and on their economic models.

4.8 Algorithmic Radicalization… and Electoral Manipulation

The algorithms of the big tech companies may already have a decisive influence on the formation of public opinion. These platforms play a major political role by promoting their users' exposure to more 'divisive' or 'polarizing' content. Sociologist Zeynep Tüfekçi describes a "toxic convergence of interests" between *YouTube* and the most radical political movements in the following terms: "*It seems as if you are never "hard core" enough for YouTube's recommendation algorithm. It promotes, recommends and disseminates videos in a manner that appears to constantly up the stakes.*" And concludes that: *"Given its billion or so users, YouTube may be one of the most powerful radicalizing instruments of the 21st century"*[141].

> **"Given its billion or so users, YouTube may be one of the most powerful radicalizing instruments of the 21st century…**
>
> **Zeynep Tüfekçi**

141. *YouTube, the Great Radicalizer* Zeynep Tufekci (Op-Ed New York Times, Mar 10, 2018) www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html

Social networks allow intimate knowledge of individuals which may already have consequences on the very functioning of democracies. As the *Cambridge Analytica* scandal demonstrated, electoral manipulation of a small number of people can have major political consequences for crucial elections. The hyper-targeted messages that were sent based on voters' political and emotional profiles may have tipped the 2016 US presidential election, which was decided by 107,000 votes in 3 states (Pennsylvania, Wisconsin and Michigan), even though they represented just 0.09% of the votes cast in the election[142]. As noted by the researchers of the *Data* & *Society* think tank, campaigns based on voter micro-targeting cannot bring about a change in entire sections of the electorate but are effective enough to influence the fringe of undecided voters who can tip an election in the event of a close ballot:

> Weaponized political ad targeting will rarely, if ever, be effective in changing individuals' deeply-held beliefs. Instead, the goals of weaponized DIM campaigns will be to amplify existing resentments and anxieties, raise the emotional stakes of particular issues or bringing to the foreground some concerns at the expense of others, stir distrust among potential coalition partners, and subtly influence decisions about ordinary behaviors (like whether to go vote or attend a rally). In close elections, if these tactics offer even marginal advantages, groups willing to engage in such machinations may reap significant benefits[143].

Other mechanisms that combine data from social networks and the processing power of artificial intelligence systems are now being used to subvert the electoral process itself. According to US Supreme Court judge Elena Kagan, partisan redistricting (*gerrymandering*) assisted by artificial intelligence could undermine the very foundations of democracy. Manipulating elections in this way could in fact make certain constituencies 'unwinnable' or, conversely, 'unlosable'. According to Elena

142. *How Trump won the presidency with razor-thin margins in swing states* (Washington Post Nov 11, 2016) www.washingtonpost.com/graphics/politics/2016-election/swing-state-margins/

143. *Weaponizing the Digital Influence Machine: The Political Perils of Online Ad Tech* (Data & Society Report, Oct 17, 2018) datasociety.net/library/weaponizing-the-digital-influence-machine/

Kagan: *"Gerrymanders will only get worse (or depending on your perspective, better) as time goes on. What was possible with paper and pen — or even with Windows 95 — doesn't hold a candle (or an LED bulb?) to what will become possible with developments like machine learning. And someplace along this road, 'we the people' become sovereign no longer"*[144].

144. *Supreme Court Justice Elena Kagan warns AI-powered gerrymandering could undermine US democracy* (Business Insider, Jun 28, 2019) www.businessinsider.com/justice-elena-kagan-warns-ai-powered-gerrymandering-may-hurt-democracy-2019-6

5
GEOPOLITICS OF THE INTERNET OF THINGS

5.1 US-China Conflict over *5G*

Due to their strategic nature for States, *IoT* technologies may be the root of international tension. The conflict between the US authorities and *Huawei* over *5G* technologies has been a wake-up call in this respect for all European governments. Above and beyond the challenges related to Sino-American industrial competition, the security of IoT infrastructure has become a national security issue for all EU member states. In France, the *ANSSI* (France's National Cybersecurity Agency) has set an 8-year deadline on use of *Huawei* equipment for telecom operators already equipped with it[144].

This crisis has also highlighted changes in the transatlantic dynamic in terms of technology. Former U.S. Attorney General William Barr contended that the "*United States and allied companies*" should consider taking a controlling stake in European equipment manufacturers *Nokia* and *Ericsson* to counter the Chinese company's dominance[145]. Because these two companies have some of the largest patent portfolios in the *5G* field (see *Iplytics* table[146]). The US authorities thus perceived European industries as 'prey' with which they could enhance the power of US companies in their conflict with Chinese company *Huawei*.

144. *5G : L'Anssi affirme qu'il n'y aura pas de «bannissement total» de Huawei* (L'Usine Digitale, July 6, 2020) www.usine-digitale.fr/article/5g-l-anssi-affirme-qu-il-n-y-aura-pas-de-bannissement-total-de-huawei.N982976

145. *Barr urges US stakes in Nokia and Ericsson to stall Huawei* (Financial Times, Feb 6, 2020) www.ft.com/content/1aa61918-48fc-11ea-aeb3-955839e06441

146. *Who is leading the 5G patent race? A patent landscape analysis on declared 5G patents and 5G standards contributions* (IPlytics – Nov 2019) www.iplytics.com/wp-content/uploads/2019/01/Who-Leads-the-5G-Patent-Race_2019.pdf

The US-China conflict over technologies could have other major geo-political consequences. Indeed, the trade embargo imposed by the US authorities affects several American companies, but also the Taiwanese chip maker *TSMC*, manufacturer of 90% of the chips used in *Huawei* smartphones. Some observers believe that the dependency of one of China's largest companies on the 'renegade province' could be the pretext the Chinese authorities are looking for to invade Taiwan. The Hong Kong daily *South China Morning Post*, a subsidiary of the *Alibaba* group, recently hinted that the Chinese military could take action against Taiwan, claiming China's need to secure its supply of strategic technologies.[147]

5.2 *'Internet By and For China'?*

The Chinese government has on a number of occasions sought to wrest control of the architecture of fundamental Internet protocols (*TCP/IP*) and thus obtain a greater level of control over the Web and its users. Already in 2004, the Chinese authorities backed a proposal for an "*IPv9*" protocol to allow centralization of Internet control and censorship processes[148]. This proposal was quickly scrapped in the face of hostility from all industrial and technology players who perceived a risk of Internet '*balkanization*'. This fragmentation of the Internet that some now call '*splinternet*' could occur if the Internet were to break up for political or technological reasons[149]. In his book on Internet fragmentation, academic Milton Mueller describes the risks of technological and economic stagnation that fragmentation could entail. He picks up on the definition of sovereignty formulated by political scientist Robert Jackson, which by extension could apply to digital sovereignty:

> Sovereignty is a foundational idea of politics and law that can only be properly understood as, at one and the same time, both

147. *As US targets China's Huawei, a perfect storm is brewing over Taiwan* (South China Morning Post, Aug 8, 2020) www.scmp.com/comment/letters/article/3096204/us-targets-chinas-huawei-perfect-storm-brewing-over-taiwan

148. *The Strange Case of China's IPv9* (Telecom Asia, Feb 4, 2008) www.telecomasia.net/content/strange-case-chinas-ipv9-0
Organizing Internet Architecture (Bernard Benhamou, Esprit May 2006) www.netgouvernance.org/esprit-eng.pdf

149. *Tech leaders have long predicted a 'splinternet' future where the web is divided between the US and China. Trump might make it a reality* (Business Insider Aug 6, 2020) www.businessinsider.fr/us/splinternet-us-china-internet-trump-pompeo-firewall-2020-8

> an idea of supreme authority in the state, and an idea of the political and legal independence of geographically separate states. Independence, supremacy, and territoriality are interrelated: a world based on state sovereignty is a world of mutually exclusive territorial jurisdictions; a world without overlapping jurisdictions. The implication is that to be supreme, authority must also be bounded geographically. It is the combination of supreme power, legitimacy, and exclusivity in a given territory that makes for a sovereign[150].

5.3 Control Architecture for the Chinese Internet of Things

Initially, the Chinese authorities risked a technological splintering of the Internet. However, creating an Internet standard that was incompatible with the rest of the world turned out to be too great a risk for the development of companies, and therefore the Chinese economy. Instead, China's strategy to redefine Internet architecture is to convince the rest of the world to adopt its technological standards. For this, the Chinese authorities are relying on research carried out by *Huawei,* which has developed a "*new IP protocol*". This protocol is intended to meet the requirements of a top/down control of the IoT. Despite the Chinese authorities setting up the *Great Firewall of China*, the fundamental Internet protocols still allow users to circumvent some of the control and censorship measures put in place by the Chinese government[151]. As so many times before, when governments or companies wanted to promote alternative technologies to the Internet, the arguments used were based on the need to improve its quality of service. For the Chinese authorities, the current *TCP/IP* architecture is 'unsuited' to foreseeable Internet evolutions. The examples put forward by Chinese authorities cite futuristic bandwidth-de-

150. Robert Jackson quoted by Milton Mueller in *Will the Internet Fragment?* (Digital Futures Ed. Wiley 2017)

151. *China is now blocking all encrypted HTTPS traffic that uses TLS 1.3 and ESNI* (ZDnet, Aug 8, 2020) www.zdnet.com/article/china-is-now-blocking-all-encrypted-https-traffic-using-tls-1-3-and-esni/

manding applications (such as holograms) or critical, ultra-low latency real-time applications such as telesurgery[152].

This *New IP* protocol aims to 'recentralize' control of the Web, taking as its starting point the observation that the decentralized architecture of the Internet is at the root of its alleged shortcomings[153]. If adopted as an international standard, this proposal would give its designers a double benefit: it would set Chinese tech players up as arbiters of *IoT* norms and standards and would allow them to natively integrate control and censorship functions[154]. The Chinese authorities' ultimate goal is to export this control technology beyond their borders. As reported by the *Financial Times*: *"The Chinese government in particular has viewed designing internet infrastructure and standards as core to its digital foreign policy, and its censorship tools as proof-of-concept for a more efficient internet, to be exported elsewhere"* [155].

A recent example of China's willingness to combine diplomatic actions with the export of surveillance technology came in response to the ban on *Huawei* and *TikTok* in the United States. China's diplomatic counter-offensive aims to forge an international alliance to thwart the extension of the *Clean Network*[156] set up by the Department of State to block Chinese technologies in the US. So, according to the *Wall Street Journal:*

> The Chinese initiative would urge countries to oppose "mass surveillance against other states," and call on tech companies not to install "backdoors in their products and services to illegally obtain users' data, control or manipulate users' systems and devices. It also would urge governments to respect other countries' sovereignty in how they handle data—in line with Beijing's vision of "cyber sovereignty," whereby countries exercise full control over their own corners of the internet[157].

152. *China's controversial mission to reinvent the internet* (Financial Times Mar 27, 2020) www.ft.com/content/ba94c-2bc-6e27-11ea-9bca-bf-503995cd6f

153. *Organizing Internet Architecture* (Bernard Benhamou Revue Esprit, May 2006) www.netgouvernance.org/esprit-eng.pdf

154. *China's "New IP" proposal to replace TCP/IP has a built in "shut up command" for censor ship* (Privacy News Online, Apr 3, 2020) www.privateinternetaccess.com/blog/chinas-new-ip-proposal-to-replace-tcp-ip-has-a-built-in-shut-up-command-for-censorship

155. *Inside China's controversial mission to reinvent the internet* (Financial Times, Mar 27, 2020) www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f

156. *The Clean Network* (U.S. Department of State, Aug 2020) www.state.gov/the-clean-network

157. *China to Launch Initiative to Set Global Data-Security Rules* (Wall Street Journal, Chun Han Wong (Sep 7, 2020) www.wsj.com/articles/china-to-launch-initiative-to-set-global-data-security-rules-11599502974

5.4 *Social Credit* a New Chinese Export?

Social Credit is another 'product' that China has developed from the combination of IoT technologies, facial recognition and artificial intelligence algorithms. This Orwellian device, developed by some of China's most powerful companies such as *Alibaba*, assigns a score to all Chinese citizens. The social, financial and political 'behavior' of every Chinese citizen can be assessed by means of this score (see the *Bertelsmann Foundation* infographic[158]). A low *Social Credit* score will block access to freedoms as fundamental as traveling by train or plane, accessing certain public services or getting a loan. According to the state-run news outlet *Global Times*, the Chinese government has already blocked 17.5 million people from flights and 5.5 million people from taking high-speed trains[159]. The aim, according to Hou Yunchun, former deputy director of the development research center of the State Council, is to make "*discredited people become bankrupt...*"[160]

And now, besides surveillance of its own people, China could export the *Social Credit* principle beyond its borders. For the Chinese authorities, this would mean imposing this rating principle on all their foreign economic partners. Tara Francis Chan of British newspaper *The Independent* describes the Chinese government's initiative to rate the political behavior of foreign companies, especially in the field of transport:

> According to a new report from the Australian Strategic Policy Institute, the system - which threatens restricted privileges for certain behaviour - was used to successfully threaten dozens of foreign airlines into adopting the political stance of the Chinese Communist Party on Taiwan. The carriers were told if they did not comply the violation would be listed on their credit records. Earlier this year foreign companies were required to get an 18-digit 'unified social credit code' which will reportedly help in recording credit violations and trigger sanctions[161].

158. *China's Social Credit System* (Bertelsmann Foundation 2019) https://www.bertelsmann-stiftung.de/fileadmin/files/aam/Asia-Book_A_03_China_Social_Credit_System.pdf

159. *China bars millions from travel for 'social credit' offenses* (Associated Press, Feb 23, 2019) apnews.com/article/9d-43f4b74260411797043ddd391c13d8

160. *China blacklists millions of people from booking flights as 'social credit' system introduced* (The Independent, Nov 22, 2018) www.independent.co.uk/news/world/asia/china-social-credit-system-flight-booking-blacklisted-beijing-points-a8646316.html

161. *It looks like China is extending its Black Mirror-like 'social credit system' to overseas companies* (Business Insider, July 3, 2018) www.businessinsider.fr/us/china-social-credit-system-controlling-foreign-companies-2018-6

More recently, during the *COVID-19* pandemic, the Chinese government set up a tracking app with *Alibaba* allowing for the real-time geolocation of all Chinese citizens in areas affected by the pandemic. This app could also block people's access to public places based on their suspected exposure to the virus[162].

Mass surveillance tools available to authoritarian regimes have never been more intrusive or more accurate than those they have now through the combined contribution of mobile devices, social networks and artificial intelligence. And now information from genomics technologies is set to be added to the information on people's behavior. Alongside *Social Credit*, the Chinese authorities are planning to use the "*Social Genome*" as a new mass surveillance tool[163]. Using the *DNA* sequencing kits from US company *Thermo Fisher Scientific*[164], China's mass surveillance system is intensifying, particularly among ethnic minorities (Tibetans, the Huis in Mongolia or the Uyghurs in Xinjiang). The Chinese police are collecting blood samples from men and boys across the country to gradually build up a genetic map of its 700 million men.

162. *In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flag* (New York Times, Mar 1, 2020) www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html

163. *China Is Collecting DNA From Tens of Millions of Men and Boys, Using U.S. Equipment* (New York Times, Jun 17, 2020) www.nytimes.com/2020/06/17/world/asia/China-DNA-surveillance.html

164. *U.S. DNA firm Thermo Fisher reportedly still helping China tamp unrest, crime* (Biometric Update, Jun 19, 2020) www.biometricupdate.com/202006/u-s-dna-firm-thermo-fisher-reportedly-still-helping-china-tamp-unrest-crime

6
INDUSTRIAL POLICY AND THE INTERNET OF THINGS

In the *IoT* era, digital sovereignty cannot be conceived in a purely defensive form but rather as the synergy between regulatory measures and the development of industrial policy mechanisms. The success of the German program *Industrie 4.0* has shown that a lasting solution to the technological and political challenges posed by non-European technologies in terms of digital sovereignty can only be found by developing alternative European technologies.

The US government's industrial policy has from the outset been supported by technologies (and industries) according to their strategic nature. Many Internet technologies (and the Internet itself) were initially developed in a military environment or with the support of military funds. The American State is so important to the development of Internet technologies that economist Mariana Mazzucato referred to the key technologies of the iPhone as follows: *"There is not a single key technology behind the iPhone that has not been state funded. This includes the wireless networks, the Internet, GPS, a touch-screen display, and ... the voice-activated personal assistant Siri"*[165]. The State's plan was articulated as follows: after public funding of fundamental research on strategic technologies, then public procurement (via the *Small Business Act*) allowed to uphold the initial stages in developing civil applications and to highlight the most promising which could in turn be financed by private funds.

165. *Tech's Enduring Great-Man Myth* (MIT Technology Review, Aug 4, 2015) www.technologyreview.com/s/539861/techs-enduring-great-man-myth/

6.1 Towards a French and European *'Small Business Act'*

Public procurement will also need to be geared towards innovative *SME*s for the technologies required to ensure the digital sovereignty of EU Member States to be developed. Public procurement is one of the most powerful instruments to help companies drive their business according to effective demand and thus develop their services and enable them to expand their activities. This growth of innovative *SME*s will also require a *Small Business Act* to be introduced in France and Europe to ensure that a significant portion of all public contracts will go to innovative *SME*s. It will also (and simultaneously) be able to block potentially hostile external buyouts of strategic technologies.

A defensive strategy based solely on the law will not be enough to safeguard our sovereignty and will not curb the current dynamic of dependence on non-European tech companies, nor the political, social and economic subservience that this could lead to over the coming years. The only way to avoid the abuses that we are witnessing on the part of these companies will be to support European companies that are capable of developing an independent industrial ecosystem.

In France, and more widely in Europe, companies that develop technologies related to critical *IoT* infrastructures will have to be considered in the future as '*operators of essential services*'. The takeover of these European companies, or the acquisition of a controlling stake, by non-European entities should first be appraised to determine whether the risks to the national security of EU countries may call any such acquisition into question.

6.2 Developing IoT Norms and Standards in France and Europe

EU Member States must be able to contribute to the development of the norms and standards which will govern the Internet of Things. *IoT* evolutions in the key sectors of health, energy, the environment and transport could thus provide Europe with the opportunity to assert its principles in the area of personal data protection and more generally the protection of freedoms. This was the view held by the German Vice-Chancellor Sigmar Gabriel, referring to the crucial importance of these norms and standards in Germany's *Industrie 4.0* program and more widely in terms of digital sovereignty[166]. In his book *Pax Technica*, Philip N. Howard, director of the *Oxford Internet Institute*, describes the importance of developing IoT norms and standards in the coming years, from both industrial and political perspectives:

> Internationally, we must actively engage in the process of setting global technology standards, encourage as much openness and interoperability as possible, and relax overrestrictive copyright regulations. And now we need to concern ourselves with the ownership structure of mobile phone companies, especially in countries where the government directly owns those companies. Media pundits used to rail against cross-ownership of newspapers, radio stations, or television stations. When infrastructure companies also produce content, net neutrality—the idea that all data on the internet should be treated equally - is at risk[167].

For France and Europe to be able to contribute to the development of IoT norms and standards, a high level of coordination is required between all companies and organizations responsible for developing these norms and standards in France and in Europe. At the same

166. Sigmar Gabriel: Minister Gabriel: We need to think further ahead about digitisation (Federal Ministry for Economic Affairs and Energy, BMWi 2016) www.bmwi.de/Redaktion/FR/Pressemitteilungen/2016/20160525-gabriel-bei-digitalisierung-jetzt-schon-weiter-in-die-zukunft-denken.html

167. *Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up,* Philip N. Howard (Yale University Press, 2015)

time, greater investment in IoT technologies is required, along with more involvement by France and European countries in international IoT standardization bodies.

6.3 Germany's *Industrie 4.0* Program

Industrial production has become one of the sectors with the fastest growing use of IoT technologies. According to the *AIOTI* (*International Alliance for Internet of Things Innovation*), these technologies are expected to play a crucial role in the optimization of all industrial processes:

> The convergence of cloud and IoT technologies will facilitate the development of factories of the future and the realisation of digital manufacturing. These future manufacturing plants will comprise numerous devices, physical and virtual smart objects, internally and externally interconnected, to dynamically enable configuration and monitoring of the operational capabilities of the plant, or networks of plants, quality control and efficiency improvement. Additionally, the traditional, fragmented processes of design, production and customer fulfilment will be replaced by a close-loop management of the end-to-end design-to-customer fulfil, where cycles are shorter and products are designed based on customer requirements (customer-focused manufacturing)[168].

Many countries have aspired to develop the use of IoT technologies in their companies. A case in point is the German government, which was concerned that its production base would gradually be made obsolete by the arrival of players using IoT technologies to obtain significant productivity gains and a preferential channel for customer relationships. The hallmark of the *Industrie 4.0* program is that it is an *ad hoc* example of industrial policy. For the German authorities, it was a matter of developing the IoT technologies and know-how that were

168. *Report on Smart manufacturing - The Alliance for the Internet of Things Innovation* (AIOTI WG11 2015) aioti.eu/wp-content/uploads/2017/03/AIOTIWG11Report2015-Smart-manufacturing.pdf

specifically required to strengthen Germany's industrial potential. For its promoters, the aim of this program was to enable manufacturers to save on existing industrial processes and create new services with high added value for their companies. The idea was to go from the *Internet of Things* to the *Internet of Services*. According to Dorothée Kohler and Jean-Daniel Weisz in their book on Germany's *Industrie 4.0* program:

> The primary objective of *Industrie 4.0* is not more automation, but more intelligent networking of machines between them and between machines and people. It responds to the growing need for product personalization and the fear of seeing Internet giants such as Google capture the exclusivity of the customer relationship, monopolize access to its usage data and hog a growing share of the margin within the value chain[169].

One of the essential tasks of the *Industrie 4.0* program set up by the German government was to enable changes in the very structure of the economic fabric of German companies by allowing industrialists to develop "*The ability to accept the vulnerability of business models that have demonstrated their robustness for over a hundred years...*"[170].For the designers of this program, all German industrial actors had to be made aware of these technologies in order to develop their practices and promote the use of industrial data as a vector for new economic models: "*This may even lead to the development of business models where a machine's value in use is sold rather than the machine itself*"[171].

Another original feature of this approach is that it was met with broad political, social and industrial consensus. In an interview with the heads of the *Fraunhofer Institute* responsible for this program, Drs Olaf Sauer and Thomas Usländer asserted that:

> The novelty of *Industrie 4.0* is that, for the first time in a long while, the subject of the production and creation of value is

169. *Industrie 4.0* by Dorothée Kohler and Jean-Daniel Weisz (La Documentation française, 2017)

170. *Ibid.*

171. *Ibid.*

> being included in the political agenda (see the coalition agreement). *Industrie 4.0* means that ministries, researchers, trade associations and companies are all singing from the same hymn sheet. It has sparked discussion within society on the benefits and consequences of *Industrie 4.0.* [...] *Industrie 4.0* is presented as the construction of a new industrial legend intended to drive out fear in the face of threats to German industrial leadership, to accept uncertainties, to count on strategic alliances to foil the intrusive power of the Internet giants, to seize growth opportunities, to count on collective leadership. Ultimately, it seeks to make not just a population of engineers and computer scientists dream of a technological revolution, but an entire society[172].

Research firm *Staufen AG* devised the *German Industry 4.0 Index*[173] to study the impact of these measures; the index has tracked the adoption of IoT technologies by German companies since the launch of the *Industrie 4.0* program. The companies interviewed were from the industrial engineering, automotive and electrical engineering sectors. Of all the German companies studied, the proportion of those that did not plan to use *Industrie 4.0* technologies halved over 5 years. Conversely, the proportion of companies that developed operational projects based on these technologies rose from 31 to 48% during the same period.

While other EU countries may have different industrial landscapes (and therefore different industrial policy needs), they could draw inspiration from the lessons in political will as applied to German industrial renewal under the *Industrie 4.0* program. Other industrial policy programs could be designed to fit the specific contours of French and European industrial landscapes. It is a case of building on the strengths and industrial specificities of each country in order to implement their general policy guidelines (health, political and environmental security, transport, energy transition, etc.) with these technologies.

172. *Ibid.*

173. *German Industry 4.0 Index 2019* (Staufen AG and Staufen Digital Neonex GmbH Studies 2019) www.staufen.ag/fileadmin/HQ/02-Company/05-Media/2-Studies/STAUFEN.-Study-Industry-4-0-index-2019-en_.pdf

6.4 Towards an 'Antitrust Moment' for the IoT?

European and American lawmakers are now talking about antitrust measures that could be taken to break up or regulate big tech companies. The economic sanctions imposed so far have not shown any real effectiveness either in tax behavior or in terms of compliance with competition laws. For companies which have hit unprecedented values, the sanctions recently imposed by the European Commission on *Google* or *Apple* in Ireland have so far done little to challenge their economic models. It should be noted that *Apple's* market capitalization almost doubled during the pandemic, to reach a value of $2 trillion. For the first time on record, the cumulative market caps of US tech companies amount to more than those of the 600 largest European listed companies (*Stoxx 600 Index*)[174].

In a major change of tack, European Commissioner Thierry Breton recently told the *Financial Times*[175] that he was contemplating unprecedented sanctions against US players that abuse their dominant position or refuse to apply EU directives or regulations. These measures could even go as far as excluding them from the EU single market or forcing these companies to dismantle. Thierry Breton clarified his comments in his speech to the European Parliament's Committee on Internal Market and Consumer Protection:

> In the same way that the 2008 financial crisis highlighted the role and systemic character of a few large banks, this crisis has shown the role and systemic character of certain platforms that often behave as if they were too big to care about legitimate concerns about their roles: "*too big to care*". And just as we did with banks, we will have to acquire the necessary regulatory tools to control those players that are no longer just online hosts, but diversified and vertically integrated service providers[176].

174. *A combination of the market capitalizations of the S&P 500 Information Technology Index, Amazon, Facebook and Google parent Alphabet -- which are classified in other sectors -- has surpassed that of Europe's benchmark Stoxx 600 Index for the first time on record* (Christophe Barraud, Bloomberg Aug 31, 2020) www.christophe-barraud.com/top-5-charts-of-the-day-31-aout-2020

175. *EU seeks new powers to penalise tech giants* (Financial Times September 20, 2020) www.ft.com/content/7738fdd8-e0c3-4090-8cc9-7d4b53ff3afb

176. *Discours du Commissaire Breton lors de l'échange de vues avec le Comité IMCO au Parlement européen* (September 28, 2020) ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/discours-du-commissaire-breton-lors-de-lechange-de-vues-avec-le-comite-imco-au-parlement-europeen_en

More recently, in the United States, the Democratic majority in the House of Representatives justified the need to implement antitrust measures against major tech companies such as *Apple, Google, Amazon* or *Facebook* in explicit terms:

> Although these four corporations differ in important ways, studying their business practices has revealed common problems. First, each platform now serves as a gatekeeper over a key channel of distribution. By controlling access to markets, these giants can pick winners and losers throughout our economy. They not only wield tremendous power, but they also abuse it by charging exorbitant fees, imposing oppressive contract terms, and extracting valuable data from the people and businesses that rely on them. Second, each platform uses its gatekeeper position to maintain its market power. By controlling the infrastructure of the digital age, they have surveilled other businesses to identify potential rivals, and have ultimately bought out, copied, or cut off their competitive threats. And, finally, these firms have abused their role as intermediaries to further entrench and expand their dominance. Whether through self-preferencing, predatory pricing, or exclusionary conduct, the dominant platforms have exploited their power in order to become even more dominant[177].

As the Internet of Things becomes a major political and economic issue, there is an even greater need to regulate the companies that deploy these technological solutions. All EU regulators recognize the need to promote new forms of competition and to avoid any kind of concentration that may be detrimental to economic actors and citizens alike. The European Commission has recently launched an inquiry into competition in the IoT sector. Executive Vice-President Margrethe Vestager, in charge of competition policy, said on the launch:

177. *Investigation of Competition in Digital Markets* (House Judiciary Committee's Antitrust Subcommittee, Oct 6, 2020) judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf

> The consumer Internet of Things is expected to grow significantly in the coming years and become commonplace in the daily lives of European consumers. [...] The possibilities seem endless. But access to large amounts of user data appears to be the key for success in this sector, so we have to make sure that market players are not using their control over such data to distort competition, or otherwise close off these markets for competitors. This sector inquiry will help us better understand the nature and likely effects of the possible competition problems in this sector[178].

Once again, control over connected objects' data will constitute the backbone of antitrust actions in Europe. As is the case for the major Internet platforms, the lack of interoperability between the various categories of connected devices translates into the temptation to create proprietary and 'closed off' environments for the devices designed for each platform. It is this closing off of markets that has proven to be conducive to abuse of a dominant position. However, as Shoshana Zuboff pointed out, while it would seem necessary to develop antitrust legislation in the technology field, it is data collection and processing legislation that will have to evolve in order to establish/restore trust in IoT technologies[179].

178. *Antitrust: Commission launches sector inquiry into the consumer Internet of Things (IoT)* (Press release Jul 16, 2020) ec.europa.eu/commission/presscorner/detail/en/IP_20_1326

179. *« La régulation des Gafa sous le prisme de l'antitrust doit être un début pas une fin »* (Le Figaro, October 15, 2020) www.lefigaro.fr/secteur/high-tech/shoshana-zuboff-la-regulation-des-gafa-sous-le-prisme-de-l-antitrust-doit-etre-un-debut-pas-une-fin-20201014

6.5 An Unprecedented Climate of Regulatory Uncertainty

In addition to the threat of antitrust actions, American and Chinese tech players are now at the heart of international tensions which could have unforeseeable consequences on the development of their companies. In the wake of the US-China conflict over *5G* technology, two Chinese Internet giants, social video sharing network *TikTok (Byte Dance)* and messaging and mobile payment aggregator *WeChat (Tencent)* were set to be banned in the United States as from November 12, 2020[180]. According to

180. *TikTok: Trump questions Oracle deal if ByteDance keeps stake* (The Guardian, Sept 17, 2020) www.theguardian.com/technology/2020/sep/17/tiktok-trump-questions-oracle-deal-if-bytedance-keeps-stake

Matt Perault, professor at *Duke* University's *Center on Science and Technology Policy*, we are witnessing for the first time a reversal of the risks encountered by US and Chinese companies: "*Chinese companies operating in the United States are now being forced to adopt strategies similar to those that American companies had long taken in China to reduce regulatory risk. The moves include divesting assets, limiting themselves to minority stakes in new investments and adjusting where they store customer data*[181]*".*

The tensions arising from the US-China technology conflict have created a climate of unprecedented industrial uncertainty. Such tensions are also connected to the expected changes in regulations on personal data collection and localization. All technological players are already anticipating major changes in EU and US legislative frameworks in these areas. In the documents for its initial public offering (IPO), *Palantir* warned investors that it could be forced to fundamentally alter its business on account of the changing data protection legal framework:

> The shifting nature of such laws, Palantir said, "could manifest in costs, damages, or liability" for the company if it fails to implement and follow proper programmatic controls, or experiences malicious or inadvertent breaches of privacy and data protection requirements. In addition to the fines, lawsuits, and other claims that could arise based on non-compliance, the company stated that new and overhauled laws could require Palantir to "fundamentally change" or modify its business[182].

These warnings came after the invalidation of *Privacy Shield*, the transatlantic agreement governing the processing of EU citizens' data in the United States. Ultimately, it now appears likely that regulations will be designed to better control the flow and processing of personal data. In Europe, new regulations could require Europeans' personal data (especially sensitive data such as health data) to be processed exclusively within the European Union.

181. *Trump's Attacks on TikTok and WeChat Could Further Fracture the Internet* (New York Times, Aug 17, 2020) www.nytimes.com/2020/08/17/technology/trump-tiktok-wechat-ban.html

182. *Palantir warns investors of complex, inconsistent global privacy law risk* (Yahoo Finance Aug 26, 2020) finance.yahoo.com/news/palantir-s1-warns-of-complex-inconsistent-global-privacy-law-risk-125635667.html

6.6 Invalidation of Privacy Shield: What Consequences for the IoT?

The European Commission's stance on 'non-personal' data has until now been based on "*Free Data Flow*"[183]. This principle may now be sidelined so as to promote the processing of European data by European industrial players. Recently, Thierry Breton alluded for the first time to the need to implement the principles of *Data Localization/Data Residency* for Europeans' data:

> "What makes the Internet so successful is its global character. As far as we Europeans are concerned, our data is the most precious thing we have in industrial matters", said the EU's Internal Market Commissioner. "I have always said that I wanted Europeans' data to be processed, stored and processed in Europe. I have the impression that Donald Trump is saying the same thing. The Chinese and the Russians are doing it, we will too"[184].

This declaration came following the decision of the *CJEU* (*Court of Justice of the European Union*) of July 16, 2020 which ruled that the transfer of Europeans' personal data to the United States did not provide sufficient protection in view of the risks of such data being accessed by US authorities[185].Faced with this new invalidation of a transatlantic agreement, the European Union may attempt to renegotiate an agreement, at the risk of seeing it invalidated in turn for the very same reasons. The other option would be to lay down the foundations for a new data circulation model, reaffirming that Europeans must be able to have access to their data, in both the tools and uses, through recourse to entities located in and governed from Europe. Since the invalidation of *Safe Harbor* in 2015, the *GAFAM* were already anticipating the fall of the *Privacy Shield* by setting up data centers in Europe in view of the potential tightening of regulations on data localization[186]. However, these precautions could prove insufficient due to laws such as the *Patriot Act* of 2001 and

183. *Free flow of non-personal data* (European Commission - Shaping Europe's digital future, Feb 24, 2020) ec.europa.eu/digital-single-market/en/free-flow-non-personal-data

184. *hierry Breton: « Je souhaite que les données des Européens soient traitées et stockées en Europe »* (BFMTV, August 25, 2020) www.bfmtv.com/economie/thierry-breton-je-souhaite-que-les-donnees-des-europeens-soient-traitees-et-stockees-en-europe_AD-202008250281.html

185. July 16: The Court of Justice of the European Union (EU) concluded that the US do not offer sufficient guarantees about the surveillance and the security of personal data, and therefore invalidated the EU-US Data Protection Shield, the agreement that regulates the transfer of the data of European users to processors in the US for commercial purposes. *The Fight for Digital Sovereignty : What It Is, and Why It Matters, Especially for the EU* (Luciano Floridi, Springer Nature, Aug 12, 2020) link.springer.com/article/10.1007/s13347-020-00423-6#Fn5 and curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf

186. *U.S. Tech Giants Are Investing Billions to Keep Data in Europe* (New York Times, Oct 3, 2016) www.nytimes.com/2016/10/04/technology/us-europe-cloud-computing-amazon-microsoft-google.html

especially the 2018 *Cloud Act* which adds an extraterritorial reach and allows US authorities to obtain data stored by American companies outside the United States. Even more recently, the *Court of Justice of the European Union* also declared that "*general and indiscriminate*" mass surveillance via data collected by telecom operators (geolocation data or connection metadata) was incompatible with EU law.[187].

One of the options now being considered by EU States is not only that Europeans' data must be processed within the EU, but that the headquarters of the companies responsible for processing the data must also be located in Europe. If this '*Data Residency*' option were to be retained by the European Union, sovereign European cloud projects would therefore take on particular importance. This was noted by the officials of the *European Council for International Relations* with regard to the *Gaia-X* project:

> The GaiaX project is motivated by the notion of "data sovereignty" or, more precisely, "data governance", and aims to bring data flows and storage under greater European control. It reflects the fact that not only will more and more core business processes run on cloud-based services, but that all major cloud providers are American-based companies and therefore subject to US jurisdiction. This makes Europe vulnerable because it cannot shape the way data is managed and governed[188].

The *Gaia-X* project embodies a new European strategy based on interoperability between different cloud providers and cloud technologies in Europe. Its success will also hinge on two determining factors in terms of digital sovereignty: vigilance vis-à-vis the technological choices made within the framework of this initiative and the implementation of a coherent policy regarding the use of sovereign and non-sovereign clouds in the European public space.

187. Judgments in Case C-623/17, Privacy International, and in Joined Cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Ordre des barreaux francophones et germanophone and Others Court of Justice of the European Union, Press release No 123/20, October 6, 2020 curia.europa.eu/jcms/upload/docs/application/pdf/2020-10/cp200123en.pdf

188. *Europe's Digital Sovereignty: From Rulemaker to Superpower in the Age of Us-China Rivalry* Carla Hobbs (ed.) Alicia Richart, Broadband: Europe's silent digital ally (European Council on Foreign Relations, Jul 2020) www.ecfr.eu/page/-/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry.pdf

7

EUROPE'S "THIRD WAY" FOR THE INTERNET OF THINGS

Legal framework measures and antitrust actions alone will not succeed in limiting the risks of abuses resulting from IoT technologies. The European Union must also build its own industrial strategy to ensure that the Internet of Things does not permanently threaten the principles and values on which Europe is founded. Charles Michel, the President of the European Council, summed it up as follows: "*Technological progress is pointless, if it doesn't make people's lives better. Between US "business above all" & China authoritarian state models, there's room for an attractive and human-centred model. This may well be our distinctive way, "Europe's way", into the digital revolution*[189]*".*

> **"Between US "business above all" & China authoritarian state models, there's room for an attractive and human-centred model. This may well be our distinctive way, "Europe's way", into the digital revolution…**
>
> **Charles Michel**

The *General Data Protection Regulation (GDPR)* has already become an international benchmark even beyond the borders of the European Union. Since its implementation, certain US states such as California have drawn inspiration from this European work to regulate personal data collection and processing. This is also true of Argentina, Peru and Brazil in South America, and of several countries in Africa and Asia[190]. Surprisingly, even China has acknowledged that it drew on the

189. twitter.com/eucopresident/status/1310978940173987840
cf. *"Europe's way" to set global standards in the digital revolution.* Charles Michel (Tech & Politics Forum Financial Times - ETNO Sept 26, 2020) www.consilium.europa.eu/en/press/press-releases/2020/09/29/the-digital-in-a-fractious-world-europe-s-way-speech-by-president-charles-michel-at-the-ft-etno-forum/

190. The impact of the GDPR outside the EU (Lexology, Sept 2019) www.lexology.com/library/detail.aspx?g=872b3db5-45d3-4ba3-bda4-3166a075d02f

GDPR when implementing its first law on cybersecurity and personal data protection[191].

Just as the *GDPR* has helped develop trust in the Internet, a European Internet of Things sector backed by data protection and user safety regulations could become a benchmark beyond the borders of the European Union. This alternative to technologies that are currently designed in the United States or in China has been dubbed the "*third way*" for a European Internet of Things. In order to become the architects of an IoT which will combine European values and principles, it will be necessary to rely on European industrial actors who will be able to develop the norms and standards of the next generations of the IoT.

7.1 Trust and Security, the 'Hallmarks' of the European IoT

After the *Cambridge Analytica* scandal, Tom Wheeler, former head of the influential *FCC* (*Federal Communications Commission*), declared: *"The New World must learn from the Old World. The internet economy has made our personal data a corporate commodity. The United States government must return control of that information to its owners*[192]*".* This homage to the European vision of data protection shows the extent to which trust has become a crucial factor for the development of these technologies. While companies may in the past have perceived personal data protection as a constraint, it could become a significant differentiating factor for the Internet of Things and a major competitive advantage for companies that develop an ethical approach in these areas. In their book '*Age of Context: Mobile, Sensors, Data and the Future of Privacy*', back in 2013 Robert Scoble and Shel Israel had already pointed to the crucial nature of data protection policies for companies on the Internet: *"We believe the most trustworthy companies will thrive in the Age of Context, and those found to be short on candor will end up*

191. *China unveils first law on personal data protection* (Global Times, Oct 13, 2020) www.globaltimes.cn/content/1203363.shtml

192. *Can Europe Lead on Privacy?* (New York Times, Apr 1, 2018) www.nytimes.com/2018/04/01/opinion/europe-privacy-protections.html

short on customers. Transparency and trustworthiness will be the differentiating factors by which customers will make an increasing number of choices"[193].

> **"Transparency and trustworthiness will be the differentiating factors by which customers will make an increasing number of choices…**
>
> **Robert Scoble and Shel Israel**

More recently, the protection of privacy has become a commercial argument for manufacturers of connected devices. *Apple*, for example, considers that the development of its business as a manufacturer of connected devices depends on it not being interested in its users' personal data, unlike its rival *Google*, whose business model is essentially linked to advertising. And yet, besides the applications hosted on the *App Store*, the services developed by *Apple* (*Apple Pay, Apple Music, Apple TV*) play an increasingly important part in the company's revenue[194]. These services allow *Apple* to aggregate information on its customers' tastes and activities even beyond the information that comes from the usual operation of connected devices. A survey conducted by the *Washington Post* in 2019 showed that in just one week, an average of 5,400 app 'trackers' transmitted personal data without the knowledge of *iPhone* users[195]. Which somewhat contradicts their advertising slogan: *"What happens on your iPhone, stays on your iPhone…"*.

7.2 What Regulations for the Security and Durability of the IoT?

For regulators, it is no longer just a matter of ensuring connected devices' security, but also of considering potential new malicious uses of the information collected by such devices. Regulators have several different 'layers' of concerns when it comes to IoT security.

The first level of protection regards the malicious takeover of connected devices. This is the most consensual point, since it concerns

193. *'Age of Context: Mobile, Sensors, Data and the Future of Privacy'*, R. Scoble and S. Israel (Brewster Press 2013)

194. *Apple's Services Revenue Reaches All-Time High* (Statista, May 2020) www.statista.com/chart/14629/apple-services-revenue/

195. *It's the middle of the night. Do you know who your iPhone is talking to*? (Washington Post, May 28, 2019) www.washingtonpost.com/technology/2019/05/28/its-middle-night-do-you-know-who-your-iphone-is-talking

preventing objects from turning against their users if they are hacked (whether through data leaks or by taking control of a connected device). California law and British law both take this aspect of IoT security into account as a matter of priority. This is also the case for the mandate awarded to *ENISA,* the European Union Agency for Cybersecurity, to develop a certification framework for connected objects in Europe under the *Cybersecurity Act*[196].

7.3 Responding to New Forms of IoT-Based Attacks

Nevertheless, the rise of connected devices in our societies has also led to an onslaught of new forms of attacks against people who rely on these devices. In her survey for the *New York Times*, Nellie Bowles described new forms of domestic violence often committed by people close to the victims:

> One woman had turned on her air-conditioner, but said it then switched off without her touching it. Another said the code numbers of the digital lock at her front door changed every day and she could not figure out why. Still another told an abuse help line that she kept hearing the doorbell ring, but no one was there. Their stories are part of a new pattern of behavior in domestic abuse cases tied to the rise of smart home technology. Internet-connected locks, speakers, thermostats, lights and cameras that have been marketed as the newest conveniences are now also being used as a means for harassment, monitoring, revenge and control[197].

Legal measures will aim to integrate these new forms of intrusion and aggression into the framework of offenses recognized by the courts. The societal dimensions of IoT security are only now being studied by industrial players and regulators. As is often the case when it comes

196. *Cybersecurity Act: Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013* eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881&from=EN

197. *Thermostats, Locks and Lights: Digital Tools of Domestic Abuse* (Nellie Bowles, New York Times, June 23, 2018) www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html

to Internet security, the measures to be taken are based on 3 principles: risk awareness, technological measures and legal framework for technologies.

User awareness and education will be key components for public action on IoT security. Unlike traditional devices, connected objects are '*gateways*' into people's homes, or more generally to their users, and must be recognized as such by their users. This awareness of the risks inherent in the IoT can have consequences for users, who will have to avoid risky behavior such as not using (or not renewing) security codes.

Technological measures must also provide these connected devices with better security, such as by introducing encryption security for connected devices. Builders and designers of IoT services will also have to design ergonomic devices that will take into account how difficult it is for most users to secure their home environment as if it were a workplace.

New regulation will also have to take into consideration other ways of using IoT data. An example of this is protecting against the uncontrolled dissemination of IoT data for microtargeting purposes, but also for political purposes. Some applications, and especially some smartphone games have been designed exclusively to collect information about their users. This is what happened with the personality quiz used by *Cambridge Analytica* which allowed it to harvest the data of tens of millions of *Facebook* users[198].

Such risks have also been observed for connected devices that transmit information unrelated to their function, and without the knowledge of their users, for monetization purposes. Shoshana Zuboff referred to the controversy around the autonomous vacuum cleaner *Roomba*:

> For example, in July 2017 iRobot's autonomous vacuum cleaner, Roomba, made headlines when the company's CEO, Colin Angle,

198. *Cambridge Analytica : 87 millions de comptes Facebook concernés* (Le Monde, April 4, 2018) www.lemonde.fr/pixels/article/2018/04/04/cambridge-analytica-87-millions-de-comptes-facebook-concernes_5280752_4408996.html

told Reuters about its data-based business strategy for the smart home, starting with a new revenue stream derived from selling floor plans of customers' homes scraped from the machine's new mapping capabilities. Angle indicated that iRobot could reach a deal to sell its maps to Google, Amazon, or Apple within the next two years. In preparation for this entry into surveillance competition, a camera, new sensors, and software had already been added to Roomba's premier line, enabling new functions, including the ability to build a map while tracking its own location. The market had rewarded iRobot's growth vision, sending the company's stock price to $102 in June 2017 from just $35 a year earlier, translating into a market capitalization of $2.5 billion[199].

> **"Although it may be possible to imagine something like the "Internet of things" without surveillance capitalism, it is impossible to imagine surveillance capitalism without something like the "Internet of things"**
>
> **Shoshana Zuboff**

Other connected device manufacturers have already been accused of collecting or monetizing users' data without their consent. Smart speaker manufacturers have on a number of occasions been accused of retaining recordings taken from their users[200]. The oddest case of unwanted recordings from a connected device involved *Lovense* sex toys, with company officials later describing these unauthorized recordings as a "*minor bug*" *(sic)*[201]...

7.4 Towards 'Ethics By Design' for the European Internet of Things

The forms that the Internet of Things will take in Europe could have major political consequences for citizens and all organizations. According to Shoshana Zuboff: *"Although it may be possible to imagine something like the "Internet of things" without surveillance capitalism, it is*

199. *Shoshana Zuboff. "The Age of Surveillance Capitalism"* (Public Affairs 2019)

200. *Smart talking: are our devices threatening our privacy?* (The Guardian, Mar 26, 2019) www.theguardian.com/technology/2019/mar/26/smart-talking-are-our-devices-threatening-our-privacy

201. *Sex toy company admits to recording users' remote sex sessions, calls it a 'minor bug'* (The Verge Nov 10, 2017) www.theverge.com/2017/11/10/16634442/lovense-sex-toy-spy-surveillance

impossible to imagine surveillance capitalism without something like the "Internet of things""[202].

Introducing an ethical dimension, from design to roll-out of these technologies, could become another hallmark of the European Internet of Things. Academic Scott J. Shackelford, who teaches corporate ethics at *Indiana University*, predicts that cybersecurity and data protection will become as important for corporate strategies as the approach taken with respect to sustainability:

> Another option that some companies like Eli Lilly are exploring is not just treating cybersecurity as a cost of doing business, but as a competitive advantage and a corporate social responsibility. The argument goes that it is in the corporate world's own long-term self-interest (as well as that of national security) to take such a wide view of private-sector risk management practices so as to encompass less traditional factors akin to what companies have done with respect to sustainability[203].

These comments echo those of Paul Nemitz, director at the Directorate-General for Justice at the European Commission, for whom data protection issues could develop into an industrial sector in its own right, in the same way as sustainable development, a sector in which the European Union could occupy a central place in the future: *"It is probably true that in the future digital world people will ask for more privacy protection and more protection of personal data rather than less. As it was with the Green movement, which started in Europe and which led European industry to enormous competitiveness but had resistance in the beginning in the '70s and '80s, it is very well possible also with data we will see the same trend"*[204].

202. "*The Age of Surveillance Capitalism*" Shoshana Zuboff (Public Affairs 2019)

203. *The Internet of Things: What Everyone Needs to Know* (Scott J. Shackelford, Oxford University Press 2020)

204. *Europe pivots between safety and privacy online* (Christian Science Monitor Jan 18, 2015) www.csmonitor.com/World/Europe/2015/0118/Europe-pivots-between-safety-and-privacy-online

CONCLUSION

The Internet of Things is a major political, industrial and technological challenge for European actors. IoT technologies are capable of transforming all of our economies but also our lifestyles and the organization of our democracies. The Internet of Things could also enable Europe to synergize environmental policies and policies related to data protection. It is true that energy management and environmental technologies (also known as *climate tech*[205]) are largely based on the analysis of information from sensors and connected devices. As these technologies spread in businesses but also into the public space, protecting data from connected devices will become a key element for their acceptability and will be a differentiating and trust factor for European technologies even beyond EU borders.

The major Internet companies are starting to face up to the social, political and industrial limitations of their 'data-centric' economic models. Their ever-growing appetite for accumulating personal data has led them to create increasingly intrusive technologies. All this is compounded by the risks of polarizing public opinion and of authoritarian excesses through the control of data from connected devices. Moreover, concentration of the main tech players and their abuse of a dominant position has led the governments of developed countries (and all other economic actors) to object to the *status quo* imposed by the major tech platforms.

205. *The State of Climate Tech 2020* (Price Waterhouse Cooper - Sept 2020) www.pwc.com/gx/en/services/sustainability/assets/pwc-the-state-of-climate-tech-2020.pdf

Developing an Internet of Things that respects data and citizens is essential for the digital sovereignty of EU Member States. It also provides Europe with the opportunity to create an industrial, political and social alternative to US or Chinese technologies. Regaining control of its technological destiny will therefore be one of Europe's most important political and industrial challenges in the coming decade.

ABOUT ISN AND AFNIC

INSTITUTE OF DIGITAL SOVEREIGNTY
INSTITUT DE LA SOUVERAINETÉ NUMÉRIQUE (ISN)

www.souverainetenumerique.fr

The *Institute of Digital Sovereignty* (or *ISN)* is a non-profit association whose mission is to bring together digital and economic actors in order to create synergy in the challenges posed by European digital sovereignty. Since its foundation in 2015, the *ISN* has been committed to educating and mobilizing citizens and their representatives on digital sovereignty challenges. The *ISN* considers that our cyberspace should be protected in the same way as our land, sea and air spaces. The *ISN* recommends technological, legal and political actions and measures enabling digital sovereignty to be asserted over all of our digital resources and in particular over our data. Lastly, the *ISN* seeks to contribute to the digital transformation of the French government to ensure protection of our sovereignty and to preserve our individual and collective freedoms at the same time.

L'ASSOCIATION FRANÇAISE POUR LE NOMMAGE INTERNET EN COOPÉRATION (AFNIC)

www.afnic.fr

Afnic is a non-profit organization and the State-appointed Registry for the management of domain names under the .fr. *Afnic* is a multi-registry operator of the top-level domains corresponding to the national territory of France (.fr and those of the overseas territories) and of several French projects for new Internet TLDs. *Afnic* contributes to the development of a secure and stable Internet, open to innovation. *Afnic* carries out its assignments in the public interest by involving all the relevant stakeholders in its decisions (scientists, the public authorities, and representatives of the private sector involved in the Internet in France). As the primary operator in France of registry services on the Internet, the goals set by *Afnic* are to develop a preference for the .fr TLD in France, to help strengthen the resilience of the Internet, and to promote its skills among the Internet community at large.

ACKNOWLEDGEMENTS

This report was produced by the *Institut de la Souveraineté Numérique* in partnership with *Afnic*. It was coordinated by **Bernard Benhamou**, Secretary-General of the ISN, who previously served as the interministerial delegate on Internet usage at the French Ministry of Research and Ministry of the Digital Economy. Bernard Benhamou also coordinated the first European Union Ministerial Conference on the Internet of Things during France's Presidency of the European Union in 2008. He previously served as Advisor to the French Delegation at the United Nations World Summit on the Information Society (WSIS).

Pierre Bonis, CEO of *Afnic*, and his teams, and especially **Benoît Ampeau**, Partnerships and Innovation Director and **Lucien Castex,** Representative for Public Policy and Partnership Development, also contributed to this report.

The *ISN* and *Afnic* would like to thank the following for their participation in the preparation of this report:

Vincent Audebert
IoT & Telecom Expert
EDF Lab

Olivier Beaujard
Member of the Board of Directors & Regulatory Work Group Chairman
LoRa Alliance
Senior Director
Semtech

Paul-Emmanuel Brun
Innovation & IoT Program Leader
Airbus CyberSecurity

Francis Jutand
Deputy Executive Director
Institut Mines Télécom

Rob van Kranenburg
Founder
Internet of Things Council

Sophie Le Pallec
Head of Public and Regulatory Affairs
GS1 France

Désirée Miloshevic
Founder of *Descon (IoT* Ecology Hackathon)
Former special advisor to the Chair Advisory Group
United Nations - Internet Governance Forum (IGF)

Michael Nelson
Director of Technology and International Affairs
Carnegie Endowment for International Peace
Former advisor on technology of Al Gore, vice-president of the United States

Javier Pallero
Policy Director
Access Now

Dr Françoise Roure
Chair Working Party Biotech, Nanotech and Converging Technologies
OECD

Gérald Santucci
Former Head of Unit Future Internet Enterprise Systems and Internet of Things
European Commission (*DG CONNECT*)

Pierre-Jean Verrando
Director
Eurosmart

INSTITUT DE LA
SOUVERAINETÉ
NUMÉRIQUE

afnic

Printed in January 2021

Graphic design: batphil@batphil.com

Printed by: Imprimerie Compedit Beauregard