4

Fabricating the European Union Safety Net

This chapter jumps ahead several decades from the previous chapter and straight into the dot-com bubble crash around 2000. Like in the previous chapter, this time period was also important as the roles of different actors in new communication territories were (re)constructed and (re)defined, crafting new media categories along the way. It was a time that, just like the development of information theory, redefined what it meant to be human, the nature of communication, and introduced new measuring devices and units. This period in the internet's history is crucial as it redefined the way people and territories were mediated and introduced new power relations that needed training. Similar to the early days of the telephone it was not clear whether the internet would survive. This chapter explores the way media practitioners wanted to make sure the internet—specifically its iteration as the World Wide Web—succeeded in yielding profit and what strategies they deployed to find a way to fund it.

In the previous chapter we heard how Bell constructed noise to be everything that interfered their business model. Bell wanted an efficient and smoothly functioning communication channel, and ordered people in particular times and spaces to accommodate that. This chapter examines digital communications, specifically in the European Union (EU) internet. Just as noise was defined to cater to Bell and the NAC's needs, here too spam is defined (and undefined) to cater

to the needs of the digital advertising industry. This chapter shows what strategies were conducted to make spam a separate, *flexible*, media category to cater to perceived threats to the advertising industry's business model.

The chapter continues the same project of examining at how media practitioners use the seven sonic epistemological strategies to (re)produce territories and people (here they turn into data subjects). Whereas the previous chapter examined the reconstruction of New York City, the first section of this chapter focuses on a different territory—the internet in the EU. It shows how new architectures of knowing people were created. These architectures were the building blocks to many of today's emergent problems with big technology companies—trackers, fingerprinting, micro-targeting, profiling, data brokers, real-time-bidding—which are part of the out-of-control digital advertising ecosystem. The second part of this chapter will continue the project that Bell started in shaping, training, and managing people's bodies to become automated machines who function as communication channels, to the exclusion of (what they define as) noise. Similarly, this second part shows how media practitioners measure people's behavior and categorize their deviant behavior, now called spam.

In this chapter, there is a development from material and embodied epistemological tools of sound, noise, listening, and rhythm to more immaterial tools on the internet. However, as Lakoff and Johnson argue, concepts "structure what we perceive, how we get around in the world, and how we relate to other people. Our conceptual system thus plays a central role in defining our everyday realities" (Lakoff and Johnson, 2008: 4). In other words, concepts and metaphors *do* things.[1] Such metaphors are powerful in their ability to do things, as can be seen with the now commonly used metaphor in technology—'the cloud'. More than that, these digital territories affect many aspect of people's everyday lives—from price discrimination, to micro-targeting citizens during elections and onto how they can organize and protest online—the consequences are very material. Ultimately, this chapter shows how the web's business model was standardized as the *only* way to experience it; a design for living that impacts our societies in ways which we are only starting to understand and act upon.

This chapter focuses on the struggle between EU legislators (mainly the European Commission), advertising associations, and internet standard organizations to define what is communication on the internet, who are the actors in this process, how they should operate, how their environments and possibilities of living should be designed and understood, and the (unwanted) categories of such events. These texts are usually considered to be the 'boring' bits, but underneath the many pages of legal documents and technical standards lies

the power to produce new media territories. As John Oliver once said when talking about Apple's iTunes user agreement: "If you want to do something evil, put it inside something boring". Susan Leigh Star recognized the powerful narratives hidden in boring things like information infrastructure back in 1999, as she says:

> Study an information system and neglect its standards, wires and settings, and you miss equally essential aspects of aesthetics, justice, and change. Perhaps if we stopped thinking of computers as information highways and began thinking of them more modestly as symbolic sewers, this realm would open up a bit. (Star, 1999: 379)

This chapter will open up the sewer and surface the foul odors and show that behind these seemingly boring things there is a struggle to define how we experience the web. To do that, this chapter focuses on legal and technical discourses. Since law and computing need specific definitions to operate (and execute) these fields are extremely productive for examining digital phenomena. Both of these fields also present their definitions as objective truths, hiding the politics, struggles, and power structures engineered into their discourses.

Such discourses, then, should not be taken at face value, but rather should be carefully peeled back in layers like the examination of any other data, to get to the heart of things. This chapter then provides a critical analysis synthesising EU legislation, advertising associations' standards, and internet standards, and I shows how they construct power relation. This is done by naturalizing specific behaviors, mainly those of the advertising industry, over others. In doing so the digital advertising industry create standards that seem like the only way things can function. But as the history of the telephone shows—there are many ways technologies can develop, operate, used, and be managed.

As part of **restructuring territories**, this chapter introduces multi-layered communication channels that are concealed from people and at the same time rely on their behavior. This reorganization introduces new listening capacities, which enable people's behavior on the internet to be measured, categorized, recorded, and filtered. This is precisely why sound is more suitable when we examine these digitally mediated territories because it can move between multi-layered infrastructure boundaries like the internet. These channels communicate people's behaviors which become the message (turning into 'data') and are listened to through (first and third party) cookies allowing for further ways of knowing people through **measurement**. You can think of cookies as dozens and hundreds of tentacles sent from various sources and plugged to your body, and importantly—*without* your

knowledge or consent. Power is enacted here in two main ways: first, knowing about the existence of these channels, usually making cookies communication 'silent' for the average user; second, the scope of listening—the more people and spaces media practitioners can listen to, the more power they gain.

The second part of this chapter focuses on the way new data subjects are (re)produced on the EU internet in three ways. I use Evelyn Ruppert's definition of data subjects as "the practices through which one *becomes* data through interactions with numerous other actors and actants" (2011: 255). In this context, people are always in the process of becoming data subjects. First, the **new experts** have been involved in developing new *processed listening* capacities using standardized units to **measure** people's behavior on the internet, mostly through web-browsers. Such *processed listening* turns people's behaviors into objects—data—which can be quantified, compared, transferred, and monetized in the accelerated rhythm channels. To have more accurate measures of behaviors on the internet, the advertising industry has developed filtration mechanisms. They **filter** non-human traffic that can jeopardize the consistent and accurate listening procedure. **Measuring** in a standardized manner and turning the internet into a monetizable medium was a problem. Rendering the population as audiences according to advertising companies measuring units, instruments and rationales enabled this medium to survive after the dot-com bubble crash and thrive in the aftermath.

Second, part of the standardization process was providing 'control' mechanisms for people. But while these were presented as protecting the bodies of people, what they were actually doing was protecting media companies. In this way, people were trained to behave and understand very limited ways of using the web while other actions were **filtered** out because they were noise to the sound of e-commerce. Third, producing data subjects was also conducted by **training of the digital bodies** through the Safer Internet Programmes that spanned from 1999 to 2013. This biopolitical training program educated EU citizens in reporting and stabilizing the EU online market by encouraging citizens to report illegal content and navigate between pre-decided **filtering** mechanisms that were provided to parents. People's digital lives were a default setting.

Opening the 'Back-End'

To understand how it was possible to create all these multi-layered communication channels and turn people into multiple data subjects we have to go back in time, to the end of the 1980s. One of the first steps to produce the European

online territory can be traced to 1987, when the European Commission introduced the *Green Paper on the Development of the Common Market for Telecommunications Services and Equipment*. The Green Paper[2] emphasized the need to break national barriers for the development of vital economic activity. The European Community argued at the time that the "single most important factor in modern 'production': knowledge" (Commission of the European Communities, 1987: 44). This knowledge economy involved data trade and exchange, which ultimately meant the commodification and trade of EU citizens' behavior. The European Commission made clear that no barriers, and hence no regulation, should be applied:

> For one sector of the emerging communications market, the exchange of data, i.e., the linking of computers, the impact will come earlier. Present narrow-band networks, upgraded through digitisation and the introduction of ISDN, allow considerable expansion of data exchanges, especially if regulatory obstacles to such expansion are removed. (Commission of the European Communities, 1987: 54, emphasis in original)

Such free movement of data within the EU helped to establish new communication channels that transferred and traded data, or in other words—people. It created a new online market where people's behavior was (re)produced as the key product of trade. As the Green Paper indicates:

> One important economic, political and cultural advantage for Europe of advanced Europe-wide telecommunications derives from the possibilities created for the enhanced exchange and free flow of information. This advantage can only be fully materialised with the development of a common market for information. (Commission of the European Communities, 1987: 139)

The Paper insisted that this online market should be managed by commercial actors, which meant there needed to be a separation between regulatory and operational functions. But to achieve that, commercial actors needed to obtain more power from EU states; they needed to be granted authority, a **license** to be the **new experts**.

The 1987 Green Paper was part of a larger European-wide governance transition to 'soft law'.[3] Just like it sounds, soft law has no teeth, and purposefully so. According to Linda Senden (2005), from the mid-1980s, the European Community started to change its approach to legislation towards co-regulation, and self-regulation as the main instruments of governance. Senden outlines two

complementary approaches that represent this European legislation policy; first, 'do less [regulation] in order to be better'; and the second, use more non-binding recommendations, best practices, guidelines, and communications. Another tool Senden emphasises is flexibility, meaning there is no need for the agreement of all member states on issues. Ultimately, the soft law approach meant delegating power to commercial actors to decide and apply their own values and principles. From the European Commission standpoint, it was cheaper, more efficient, and made it much easier to avoid responsibility when things go wrong.

An important legal document laying the groundwork for the delegation of power to commercial actors in the EU telecommunications sector was the 1999 decision regarding safer internet and combating illegal and harmful content (276/1999/EC). This decision introduced the first phase in applying the soft law approach and aimed to highlight the importance of **licensing** commercial actors to regulate illegal and harmful behaviors on the internet. This rationale can be seen in Recital 5:

> [P]romotion of industry self-regulation and content-monitoring schemes, development of filtering tools and rating systems provided by the industry and increased awareness of industry services as well as fostering international cooperation between all parties concerned will play a crucial role in consolidating that safer environment and contribute to removing obstacles to the development and competitiveness of the industry concerned.

What such statements were meant to do is cement the central role of commercial actors, in making important decisions in the then new online European market on how the internet should function as an economically viable and thriving medium. Importantly, Recital 12 states that, "cooperation from the industry in setting up voluntary systems of self-regulation can efficiently help to limit the flow of illegal content on the Internet" (276/1999/EC). This was a key moment in institutionalizing the position of commercial actors by granting them a **license** to be the new producers and regulators of the internet through 'voluntary', self-regulation mechanisms. This **license** enabled them to conduct processed listening and rhythmedia, and, consequently, to produce data subjects. The EU tried to sell the idea that these steps were about safety, but these instruments introduced unaccountable procedures of monitoring, spying, and **measuring** citizens' movements online, while commodifying and trading them. In this way, citizens' behaviors were conceived as things, objects, and products to be traded in the new online market created under the soft law approach.

What emerges from the EU policy documents is a discourse that normalizes commercial actors' deep involvement in producing the internet territory as well as policy-making and enforcement. As Katharine Sarikakis argues about the naturalization of privatization in internet governance:

> The ideological and normative constructions of policy-making for the Internet express a form of *neo-liberalist determinism* that can be categorized in three major narratives: technological determinism, economic and structural inevitability and the ideology of private–public partnership, asserting the involvement of the private sector in public policy. (Sarikakis, 2004)

Such narratives appear in all the EU legislation documents examined in this chapter which, as Sarikakis argues, are designed to regulate people's behaviors rather than the economy, as they argue. This new online market produces bodies, data subjects that can be listened to, **measured**, categorized, segmented, and traded. This is done by rendering people's behavior into data that is then fed to re-order people's personalized experiences through their web browsers. This approach will be shown below in the case of distinguishing between spam and cookies through non-legislative agreements and documents produced by the Interactive Advertising Bureau (IAB)[4] using its standards and measuring metrics.

To provide **licenses** to themselves, advertising associations drafted various self-regulation standards, 'best practice', charters and models which authorized their positions as key players in the EU online market. In June 2004, the European Advertising Standards Alliance (EASA[5]) organized a self-regulation summit with over 130 participants from the advertising industry, including the European Commission, to sign the Self-Regulation Charter. This Charter relied on two earlier documents: the EASA Statement of Common Principles and Operating Standards of Best Practice (2002), and the EASA Best Practice Self-Regulatory Model (2004). According to the Charter, its main aim is to promote '*a high standard of consumer protection based on the premise that advertising should be legal, decent, honest and truthful*' (EASA, 2004b: 1, emphasis in original). This was a way for the digital advertising industry to show the EU that regulation would be a bad idea, and that their industry can control itself (an argument they keep on telling…).

Regulation, as the Charter says, cannot be achieved by legislation but with self-regulation, and legal measures should only be taken with 'rogue traders'. Here, the advertising industry **licenses** itself to act according to its own rules, but asks states' legal systems to make self-regulation 'effective'

by punishing problematic advertisers and traders who do not follow their standards. The digital advertising industry's 'self-regulation' is funded by the industry, adjudicated by the industry, to guidelines established by the industry, but enforced and punished by the state. In this way, digital advertisers position themselves as key players, whose rules are constructed without the state but are enforced by it.

The self-regulation sanctions appear limited to publishing decisions, though without any mention of the scale or to which audiences. These standards also encourage consultation and involvement without stating how binding such engagement might be, and advocate awareness of the self-regulation system without stipulating what mechanisms are to be deployed and how awareness is to be assessed or by whom. In addition, this Charter only applies to advertisers and not its accompanying industries such as data brokers and other companies who trade and exchange data on the silent communication channels, specifically Demand Side Platform (DSP) and Supply Side Platform (SSP) (which will be discussed below). In this way, the regulation on the digital advertising industry is soft, but the power they gain is not.

In these documents, moreover, when it comes to 'consumer awareness', the EASA discusses awareness of people's ability to complain about the industry's misconduct but not about the existence of the multiple actors involved in the online market. When the EU did decide that people should be educated about the internet, it was not about how digital advertising, and specifically first- and third-party cookies, ad networks, ad exchange, DSP and SSP and other ad-tech technologies work to fund their 'free' access. Rather, as the last section of this chapter shows, people were educated about the illegal and harmful behaviors they should avoid while reporting deviant citizens who conduct them. In this way, the digital advertising industry can produce data subjects that have limited understanding of the internet territory, and create a specially designed territory that will make sure they will also have limited options of behaving.

Therefore, standards documents such as the EASA Best Practice mentioned above, and others such as IAB UK's Good Practice Principles (2009), FEDMA's European Code of Practice for the Use of Personal Data in Direct Marketing Electronic Communications Annex (2010), the IAB Europe EU Framework for Online Behavioral Advertising (2011), the EASA Best Practice Recommendation on Online Behavioral Advertising (2011), are operating as **licenses** that are provided by these organizations *to themselves* in order to legitimize their practices. Importantly, these **licenses** provide the authority and credentials to create new power relations constructed by the new online market.

Governing Softly

The topic of internet governance and specifically the multiple actors involved in EU internet governance, or any internet governance for that matter, is complex. It comprises international bodies, governments, private companies and, NGOs that (try to) coordinate in a way that produces the operation of the internet (its structure and user experience). According to Marianne Franklin, internet governance "designates the technoeconomic and legal issues arising from any decisions, de facto or by law, that affect the design, access, and use of the Internet as a specific sort of communication network architecture" (2013: 138). This means that internet governance is conducted on a global, regional, and national level of territories, all at the same time.

With such complexity, it has been very difficult to agree on how the internet should function between countries and regions who think very differently about governing and media. Therefore, it was more convenient and desired by many western states to promote the soft law approach rather than specific laws. This saves governments and regional bodies the headache of having to handle with the operation, regulation, and enforcement of the internet. These companies can also help governments when they ask them to hand over sensitive information, as we were made aware in the Edward Snowden revelations in 2016. The self-regulation codes of conduct of advertising associations and contracts with commercial companies such as Internet Service Providers (ISPs), software, and protocol patent holders have become the new standard.

In the case of the EU, the power conflict between the multiple network actors becomes even more complicated as actors that are involved in establishing internet governance negotiate between member states, zooming out to the EC, and onto global actors such as the International Telecommunication Union (ITU[6]), the Internet Society (ISoc[7]), the Internet Corporation for Assigned Names and Numbers (ICANN[8]), the Word Wide Web Consortium (W3C[9]), the Internet Engineering Task Force (IETF[10]), and the Electronic Foundation Frontier (EFF[11]). Most of these organizations were founded and are based in the United States and receive criticism on the centrality of their values, language, and standards that are influencing internet governance.

Self-regulation of advertising associations and contracts with commercial companies such as ISPs, platforms and applications have become the new governing standard in the EU internet.[12] Such interest groups "have adapted to the multi-layer character of the European system by establishing organizations at all levels, building direct channels of contact to supranational as well as to national

political actors" (Kierkegaard, 2005: 312). These **new experts** have been influential players in designing the internet architecture in which people operate, as well as deciding, defining, managing and controlling their behaviors. In particular, these groups aimed to establish legitimate and illegitimate behaviors and architectures according to their business model. This is illustrated in their strategies to distinguish between spam and cookies and restructuring the spaces where these can be performed.

So how do spam and cookies relate to online behaviors? Are they behaviors at all? And how does that relate to how we experience and understand the web today? We can start by checking the definitions. While spam's exact definition cannot be found in EU law, non-governmental organizations such as the IETF have described it as "mass unsolicited electronic mail" (Lindberg, 1999), or, similarly, as the anti-spam organization Spamhaus explains, "Unsolicited Bulk E-mail … Spam is an issue about consent, not content" (Spamhaus, n.d.). Emphasising these characteristics shows two important aspects when classifying forms of behavior on the internet: whether this behavior creates a burden on the system's infrastructure (bandwidth), and whether this behavior was conducted without being requested. These two topics have different interpretations and meanings for different actors at different times.

When it comes to the second aspect—'consent' (more on the politics behind consent in the sections below) provides insight into the politics of categorizing spam, because a division has been created between spaces where people have the right to reject communication, and spaces where they do not.[13] This division is about what constitutes public and private space on the internet. Just as people do not have a right to reject seeing advertisements when they walk down the streets—because these are communicated in public spaces—they also do not have a right to refuse advertisements in spaces on the internet that are conceived as public. To do that there was a need for a different kind of architecture online, to produce an economically friendly territory that will fund the web.

Baking Cookies into the Ecosystem

Designing an architecture that re-draws the boundaries between private and public spaces on the internet began with cookies. In the original HTTP protocol[14] (Berners-Lee, Fielding, and Frystyk, 1996), which is the main protocol used for communicating through the web, each request made by a client (a user's computer) from user agents (web browser) would be treated as 'new'. This meant that origin servers (websites/publishers) would not 'remember' that the user had

requested an object(s) in the past, or any other activity the user did on this space. Cookies were meant to change this by creating what computer scientists call a 'stateful' session.

Originally designed to make shopping online easier, cookies were invented in 1994 by the programmer Lou Montulli and refined by John Giannandrea, both employees at Netscape Communications. "Montulli decided to store the information on the user's computer instead of within the URL. This solution was termed Persistent Client State HTTP Cookies" (Shah and Kesan, 2009: 321–2). Cookies revolutionized the web because instead of treating each time you use the web as a 'new' *anonymous*—session, it began to remember what you previously did in a particular time and space. Cookies gave the web a memory; it gave your actions on the web a 'past' which you have no idea about or access to.

With the introduction of cookies, two other important things happened to the web—cookies penetrated people's *private* bodies, enabling access to their personal computers, and importantly, they introduced additional layers of communication channels to people's internet. Cookies opened a new architecture with a separate economic ecosystem that was hidden, automated and accelerated. According to Schwartz (2001), in 1995, the IETF established a working group led by David Kristol, and later joined by Montulli, to propose standards for cookies and their purposes. The way that cookies work, as the IETF standard document outlines, is that (human) users request various software objects (images, texts) from an origin server via their browsers, but instead of sending back only a response to these specific requests, and thanks to browsers' standards, the origin server also "returns an extra response header to the client, Set-Cookie … An origin server may include multiple Set-Cookie headers in a response" (Kristol and Montulli, 1997: 2–3). The Set-Cookie contains all the details of that cookie, for example, its name, expiration date, domain (the website/server you requested), 'value', which is a unique ID number, and 'Path', which means a URL in a domain that it is valid. In this way, the origin server sends the tentacles and attach them to the user's unique body. The ID number, assigned to people's individual computers as an identification marker (and therefore cookies are commonly called 'identifiers'), is one of the main arguments that advertising companies use to justify this surveillance ecosystem, as it is creating the notion that the communication is anonymous. This unique body may be identified with a numerical sequence, but, as I will show below, that does not mean that it is anonymous.

So how many cookies could be sent before people (browsers) got sick? Montulli and Kristol outline the minimum design requirements that browsers must apply to support cookies, mainly that "user agents' cookie support should

have no fixed limits. They should strive to store as many frequently-used cookies as possible" (Montulli and Kristol, 1997: 14). These browsers' design capabilities should allow "at least 300 cookies … at least 4096 bytes per cookie … at least 20 cookies per unique host or domain name" (Ibid). In this way, cookies were authorized and legitimized by design. This standard enabled hundreds of cookies to be plugged into people's bodies (through their browsers) and communicate the behaviors they conduct in multiple websites to various media companies that traded them.

With this special **restructuring of the online territory** people's experience on the web was conducted in a specific space called the 'front end', while the advertising industry's activities were conducted in the 'back end'. This created a knowledge boundary between 'average' users and the online market which was operating in accelerated rhythm at the back-end. So, although cookies rely on people's browsing behavior, they are not signalled through visual or audio cues about this activity. Instead of automatically adopting computer scientists' definition of cookies as a form of memory ('state'), cookies can be described differently. After all, what they do is listen to people's behavior across multiple spaces and render them into data that is communicated between different advertising practitioners or publishers. Thinking of them this way, cookies are a *form of communication*.

Montulli pointed this out as well when he says, "We were designing the next-generation communications system" (cited in Schwartz, 2001). Cookies have introduced new layers of communication whereby websites send dozens or hundreds of cookies that conduct processed listening to people's behaviors across the web. This new form of communication has turned people's behavior into data—the message—that is communicated between non-human actors operated by multiple actors. Cookies opened an architecture of multiplicities of users, commercial actors, communication channels and messages all orchestrated in multiple rhythms at the back-end. Cookies are part of a new territory where they communicate people's behavior and create a dynamic database with profiles that can be monetised.

Furthermore, cookies requests through the HTTP protocol are performed automatically by people's browsers, not according their requests. The 'topics' (predefined behaviors of people on websites) communicated by cookies are unknown and silenced to people. As Joseph Turow argues, "by not requiring the computer user's permission to accept the cookie, the two programmers were legitimating the trend toward lack of openness and inserting it into the center of the consumer's digital transactions with marketers" (2012: 48). This makes cookies a form of

unsolicited bulk communication conducted without a human interface (because they are conducted by non-human actors), meant for direct marketing (personalized ads). Sounds familiar, right?

So what type of communication is operated by cookies while plugged into your body? The main difference between the type of cookies is who gets to listen to you. First-party cookies are sent and operated by the publishers/websites that people request when they type the URL that is displayed on their browser's address bar. These cookies communicate with people's browsers without their knowledge but they are sent from the website they requested. Third-party cookies are a different story. These cookies are sent by other companies, which are unrelated to the website you type. Third-party cookies were developed immediately after first-party cookies and are operated by internet advertising networks such as DoubleClick but also by data brokers such as Acxiom, Experian, Epsilon, CoreLogic, Datalogix, including insurance companies and many, many more.

Advertising networks are companies that work with multiple websites to have better insights of what and where people do things across many spaces. This enables them to have richer profiles, and then monetize them. They have become the main technology used as part of behavioral advertising, which is an:

> [A]dvertising that is based on the observation of the behavior of individuals over time. Behavioral advertising seeks to study the characteristics of this behavior through their actions (repeated site visits, interactions, keywords, online content production, etc.) in order to develop a specific profile and thus provide data subjects with advertisements tailored to match their inferred interests. (A29WP, 2010: 4)

Both first- and third-party cookies listen to people's behavior continuously across multiple spaces to create profiles that then suit specific segments/audiences. But it is people's repetitive actions, the ones that they do the most, that are most valuable for advertisers because they indicate 'profile' characteristic that can be monetised. From people's behaviors, advertisers build a unique profile which consists of: political affiliation, religious belief, sexual identity and activity, race and ethnicity, education level, income, purchasing and search habits, your mobile-phone brand and operating system, physical and mental health, location, film and music preferences and much more.

Cookies, then, are (bulk) communications conducted by non-human actors (people's browsers and publishers or advertising networks) who 'talk' to each other about pre-defined 'topics' (specific behavior criteria of people) and create "a flow of communication back and forth between that hard drive and the website's

server" (Debusseré, 2005: 76). According to Matthew Goldberg, in the United States, computers can also be considered as users and therefore cookies can be defined as electronic communication (Goldberg, 2005: 262). These non-human actors, then, listen to people's behavior in different spaces and turn this knowledge into data that becomes the message of that communication channel. This message is then (re)assembled in a specific rhythmedia; commodified, monetized and traded in the 'back-end' market.

Third-party cookies, and the data (people's behavior) they communicate with actors other than the first-party server that users request, is a practice that Montulli and Kristol did *not* favour in the first IETF cookie standard they drafted in 1997. In cases of 'unexpected cookie sharing', as they call it:

> A user agent should make every attempt to prevent the sharing of session information between hosts that are in different domains. Embedded or inlined objects may cause particularly severe privacy problems if they can be used to share cookies between disparate hosts. (Montulli and Kristol, 1997: 17)

Three years later, in the improved version of the IETF cookie standard, however, the tone was more relaxed regarding third-party cookies and ad networks. Montulli and Kristol addressed issues of 'protocol design' by arguing that "[t]he intent is to restrict cookies to one host, or a closely related set of hosts" (2000: 20). By phrasing it as 'set of hosts' Montulli and Kristol legitimized advertising networks practice. Behavioral advertising facilitated by third-party cookies helped to reduce the uncertainty that advertisers were looking for when trying to establish which ads fit to which audience and whether they listened to or clicked them. As Omer Tene and Jules Polonetsky argue:

> An ad network typically places a cookie on a user's computer, which the network can subsequently recognise as the user moves from site to site. Using this identifier, the network can create a user profile based on the range of sites the user visits. Increasingly, in a process known as "cookie synching," many third party cookies that advertising networks and exchanges use are linked to enable the availability of data across multiple platforms. (2012: 291)

'Cookie-synching' enable advertising networks to identify people by merging people's behaviors across multiple separate websites into one identity, and this is facilitated by real-time-bidding (more on this below). This new way of listening to people and producing profiles/segments (knowledge) not only helped to stabilize the advertising industry targeting practices but also, importantly, offered an

efficient and successful way to fund the internet. One of the main ways that the cookies standard managed to not be considered as a disturbance to the system (like spam) was by bypass the problem of burdening bandwidth. Cookies have avoided being 'bulk' (like spam) thanks to browser being designed in a way that automatically discards them. It does so according to certain **filtering** procedures—after a certain number of cookies are sent or after they have been on people's devices for a certain amount of time. In the first IETF cookie standard document that Montulli and Kristol drafted, they argue that:

> Because user agents have finite space in which to store cookies, they may also discard older cookies to make space for newer ones, using, for example, a least-recently-used algorithm, along with constraints on the maximum number of cookies that each origin server may set. (1997: 7)

Default design settings of browsers enable the cookie communication not to be considered as bulk, producing it as necessary sound and not noise. Although the tech and advertising industries were trying to sell cookies as a necessary tool for the internet, others thought differently. Privacy-concerned people classify this unsolicited communication designed to track people's online behavior as spyware. It is all about categorization, and cookies are much easier to digest. The advertising industry wanted to legitimize and authorize cookies, and they did that in every way they could. While there were various claims supported with research about the way spam is a burden on the bandwidth, similar research on how cookies burden the system cannot be found to date. An example of how spyware is a more accurate description of what digital advertisers have been doing can be seen with the accompanying technology to cookies called web-bug/beacon/pixel tag.[15] This technology was developed at the end of the 1990s. A web-bug is an invisible graphic that is automatically downloaded to people's computers (without their knowledge) and enables an advertising company to produce more accurate user profiles. The process starts by sending the cookie and then the web-bug provides more accurate information on the kind of behavior the user performs on the pages they visit. This means that further wires are plugged into people's bodies to listen even deeper to their every rhythm and produce richer profiles.

According to Richard Smith from the digital rights NGO Electronic Frontier Foundation (EFF), the reason web-bugs are invisible to people is "[t]o hide the fact that monitoring is taking place" and that "[t]he Internet advertising community prefers the more sanitized term 'clear GIF' " (1999). They were not the only organization concerned about this, the Article 29 Working Party (A29WP),

which was (until May 2018) the European advisory board on topics related to the protection of privacy and personal, was also worried about this kind of invisible and automatic data processing. As they argue at the end of the 1990s, "[b]rowsers often send more information to the Web server than strictly necessary for establishing the communication" (1999: 4). This means that the production of data subjects is conducted in a rhythmedia that is silenced for the people, leaving them unaware of these procedures. This creates power asymmetries between people and the companies that listen to them, that are enabled by asymmetrical architectures.

Although these listening technologies are spying on people by measuring, recording, archiving, and monetizing people's behavior for various purposes without their knowledge, the companies that operate such silent communication channels do not consider them to be spyware. As Danny Meadows-Klue, chairman of the IAB United Kingdom, said in 2001, "Cookies have been branded as spyware tools, or some kind of subversive software … But it's what we use everyday" (Reuters, 2001). Presenting them as everyday work that advertisers do was yet another way to normalize these spying activities and frame them in a harmless way.

The definition of spyware, as Laura DeNardis (2007) argues, is disputed among software developers and marketing companies who do not think their technologies should be categorized as such. So, although cookies and their accompanying technology web-bugs can be considered as spyware, malware and spam, they are not categorized as such. The main reason for this is that their utility has been portrayed as legitimate and vital for the web's business model. This legitimization occurred with the transition from more traditional media revenue models, such as subscription, to the provision of free content funded by advertising. As DeNardis argues:

> A segment of Internet marketing firms and advertising distributors adopted spyware approaches for financial gain, earning commissions when consumers viewed advertisements or for transactions resulting from advertisements. (DeNardis, 2007: 700)

Because they were the main funding source of the web, this revenue model meant that the advertising industry had more power in shaping how online communication would be defined, performed and managed. Such power is illustrated in the industry's ability to influence the IETF cookie standard. According to Schwartz (2001), in 1997, the IETF working group recommended that people should have control and decide for themselves what kind of communication they wanted to be a part of. They recommended that web browsers should have a visual display

of such forms of communication (cookies), while providing information about their contents and purposes. This would give people a tool to listen to their own bodies and understand its hidden parts. This design option would enable people to know about various forms of communication conducted in the 'back end' and provide them with more tools to control and manage them (Kristol and Montulli, 1997: 15). Such a design would destabilize the power asymmetric, giving people more power to understand and engage differently on the web. However, for these suggestions, the IETF and David Kristol were bullied by the advertising and tech industry, which thought differently:

> Each argument caused further delay—time in which the advertising companies became more powerful and the market crystallized around the two leading browsers. Mr. Kristol was not surprised, then, that neither Netscape nor Microsoft took to heart the recommendation that browsers block cookies unless instructed not to. He acknowledged that there was little he could do to persuade companies to adopt the voluntary standards. 'There's no Internet police going around knocking on doors and saying, "Excuse me—the software you're using doesn't follow I.E.T.F. standards"'. (Schwartz, 2001)

There is no 'internet police' because the soft-law approach was presented as a better solution. As tech companies (especially those who designed web-browsers) and the advertising industry became more powerful their arguments about not needing to be policed became the standard, and all this received the seal of approval and **license** of the EU. This approach worked so 'well' that technology and advertising companies were able to ignore voluntary standards as the standards had no teeth. And the advertising industry knew this, after all, their whole profession is about selling ideas. Regulators liked these ideas because they presented economically rich futures in shiny new technologies; For them, (ad)tech will fix it. Not to mention that most regulators did not understand how all of this worked, some, to this day, still do not.

While Montulli said the new Netscape browser—Navigator 4.0—would enable users to reject third-party cookies, he also reassured the digital advertising industry that "because the vast majority of Web users never bother to change their cookie preferences, the effect on companies that use cookies as targeting tools will be minimal" (Turow, 2012: 58). Montulli commented that:

> If we were to unilaterally disable this feature, existing content on the Web would no longer work … [Also,] sites that use [cookies] tend to use them in a way that generates revenue. If you take away revenue from the sites, then the users may lose their ability to go to these sites. (Bruner, 1997)

Montulli's remarks illustrate how important it is to naturalize this business model in the discourse about the web—that people's behavior should be traded if they want to 'go to these sites'. People's online behavior is governed in a biopolitical way, by shaping the options of living appear to them (in a particular rhythmedia) through browsers' standard settings, where they can 'freely' act according to advertisers' rationales.

Similar to Bell, commercial companies are creating the standards of communication. Big companies use their powerful positions in the market to develop tools and **restructure territories** that benefit their businesses. With the EU's soft law approach, governments gave their power to commercial companies to develop, define, and enforce their own standards, under the **license** of self-regulation. It enabled a translation of EU laws according to the rationales of commercial actors. The delegation of regulation to commercial actors enables them to deploy sonic epistemological practices that order the options of living. These orderings in turn produce data subjects through mediated territories and the architecture in which they operate. This rhythmedia was made legally possible due to the artificial boundary between private and public spaces on the web; The production of the web territory.

Inventing Private and Public Spaces

Due to the fact that private or public spaces on the web have not been clearly defined in EU legislation, law makers and the private sector wanted to produce these spaces while relying on characteristics of previous media technologies that people already know, such as postal mail or the cinema. In this way, it would be easier to educate people as to what is private and public as they transfer their systems of perceptions and behaviors to the newly produced online territory. Both Article 13, which is about spam, and Article 5, which is about cookies, appeared on the Electronic Privacy (e-Privacy) Directive because they mainly deal with the privacy of specific spaces on the web.

As we learned in the previous chapter, in the early 20th century it was crucial for Bell and others at the NAC to demarcate public spaces, such as the street, as illegitimate commerce spaces by zoning. Here, too, constructing specific spaces as public (and thus commercial) or private on the web was paramount to enabling it to function as a commercial medium. The purpose behind such zoning strategies is, as Lessig suggests, for commerce, "and the how is through architectures that enable identification to enable commerce" (1999: 30). The production of the EU online territory was conducted by

regulating illegitimate rhythms, such as spam, and legitimizing others, such as cookies. As part of their opinion on web anonymity the A29WP compared browsing to:

> [B]rowsing in a public library or a bookshop, or wandering through the high street window-shopping … A key difference though is that while browsing in a library or wandering the high street can be done in almost complete anonymity, browsing on the Web invariably leaves a permanent and identifiable digital record behind. There is no public policy or general interest justification for such traces to be identifiable, unless the user wishes them to be so … Individuals wishing to browse the World Wide Web anonymously must be entirely free and able to do so. (1997: 9)

Despite these early acknowledgements from the European Commission that browsing is not anonymous, browsing was still constructed as moving in a public space, which was contrasted with email, which was framed as a private space. Constructing email as a private space also correlates with fundamental rights such as Article 8 of the European Convention on Human Rights and Fundamental Freedoms, which protects the right to respect for private and family life: "Everyone has the right to respect for his private and family life, his home and his correspondence" (Council of Europe, 1950). This can also be seen in the Charter of Fundamental Rights of the European Union's Article 7 'Respect for private and family life' (2000/C 364/01). Email, like the private home, can be accessed through a password that is synonymous with a key; only you, or people you trust (and the company providing the space), hold this key and can access and use this place.

In this way, email was conceived as analogous to a physical home, a space with clear boundaries that provides privacy to people's lives. It also provides privacy to the communication that connects them from that place. As the A29WP argue in relation to privacy of email screening (here again visual concepts are used for explaining listening procedures) services: "From the case law of Commission and the Court of Human Rights, it may be concluded that email communications almost certainly will be covered by Article 8 of ECHR, by combining both the notions of 'private life' and 'correspondence' " (2006: 3). Here, the A29WP argue that email is not only a private space; it is where *private life* is performed on the web (while still being ambiguous with 'almost certainly' leaving flexibility for other interpretations).

However, Internet Protocol (IP) address, for example, which is a number assigned to the computer that accesses the internet (Postel, 1980), a body

identification, is not considered to be a private space in this Directive. This is contrary to the definition of personal data according to the Data Protection Directive, mentioned above, which indicates that a natural person can be identified *indirectly* "in particular by reference to an identification number" (95/46/EC, Article 2[a]). It also contradicts the A29WP acknowledgement of "IP addresses as data relating to an identifiable person" (2007: 14), and even earlier opinions where they argue that "IP addresses attributed to Internet users are personal data[16] and are protected by EU Directives 95/46 and 97/66" (2002a: 3), and that "this address has to be considered as personal data" (2000a: 11). In addition, the A29WP also acknowledge that browsing on the web, which is conducted in a 'public' space, should be treated as a private activity. They expressed this with regard to the 'cookies Article', termed 'confidentiality of the communications', in the Directive that preceded the e-Privacy Directive, the 1997 Directive for Telecommunications Privacy (97/66/EC):

> [T]he Working Party thinks that surfing through different sites should be seen as a form of communication and as such should be covered by the scope of application of Article 5 … This form of communication should therefore remain confidential. (A29WP, 2000b: 50)

Bypassing such opinions[17] enabled portraying people as anonymous when browsing. In this way, it was possible to construct IP address and activity outside of email as conducted in a public space on the web. Consequently, this is a space where people do not have a right to reject communication, such as cookies. These opinions about the need for confidentiality when browsing were not implemented because of the new business model for the web (free access to content and services). This model required that only specific spaces and activities that would dedicated for direct financial transactions will be private, such as email and paying for online shopping. The rest of the spaces that will yield indirect revenue for funding the web through advertising will be public and, therefore, not private. Creating the notion that email is private was meant to raise people's confidence in the new EU online territory, and online commerce more broadly.

Put into context: the e-Privacy Directive was drafted during the dot-com crash, when at its peak, "all attention became focused on e-commerce, touting it as the New Economy. Users were first and foremost potential customers, and they needed convincing to buy online good and services" (Lovink, 2011: 4). After the crash, many people lost their trust in e-commerce and the web altogether. Creating a distinction between private (email) and public (web) spaces on the web was essential for the survival of EU e-commerce. Email was one of the main tools

for making purchases online making it a market-orientated medium. Therefore, it was important to keep it safe and reliable. This is highlighted in the EC's document:

> One of the most worrying consequences of spam is that it undermines user confidence, which is a prerequisite for successful e-commerce and the information society as a whole. The perception that a retail medium is affected by rogue traders can have a profound effect on the reputation of legitimate traders in the same sector. (2004: 8)

This was an attempt to persuade people to believe in this medium as a safe and private space that can be used for buying online. This comment also shows how states' regulation is directed towards 'rogue traders', whereas the rest of the advertising industry is not under such scrutiny. Reviving e-commerce was a joint interest of the European Commission and commercial actors such as browser companies, publishers and advertisers; therefore, it was important to make spam a fluid category that represented anything that could harm the efficient functioning of EU e-commerce. As Wendy Chun argues, "[t]he commercialization of the Internet, its transformation into a 'secure' marketplace, facilitates control and thus regulation: the interests of commerce and governmental regulation coincide perfectly" (2006: 67). This could not be done with precise hard-law legislation, but rather with tech and advertising industries' self-regulation.

These media practitioners were promoting notions of privacy to ensure people would trust the web as a medium where they could buy things, a new commerce territory. They created architecture designs through the default settings of browsers to ensure that when people wanted to purchase things, then their behavior was kept private, as if it was in a private space. Forms of communications that processed personal data and were meant for commercial purchases were encrypted and credentialized by a technology that Netscape developed for its web browser, Navigator, called the Secure Sockets Layer (SSL[18]). According to Thomas Haigh, in 1995 a year after cookies had been developed by Netscape, and in order for the web to be a safe commercial territory, the browser company:

> [A]dded a then-unique feature to its first browser and server systems: the optional encryption of data entered into Web pages as they were transmitted back to the server. (Netscape displayed a lock icon on the screen to let users know that the page was secured.) This advance, known as a Secure Sockets Layer (SSL), made the Web a practical platform for financial transactions and other sensitive data. (Haigh, 2008: 132)

In this way, specific behaviors on the web, those meant for economic purposes, were architecturally ordered to signal importance, because they were standardized as a default private mode. Such a mechanism was introduced to reassure people that buying things online would be kept private. By developing these two technologies in the 1990s, Netscape created a distinction between spaces where people buy online, which are private, and spaces where people live online, which are in a public space.

Through such territory design, people were biopolitically **trained** to understand their options of living online. Behaviors that were performed in public space yielded profit in an indirect way. Media practitioners listened to people's behavior in multiples spaces, turned it into data that could then be monetized, traded and exchanged. The types of data that were inferred from people's browsing repetitive behaviors were: age, location, sexual preferences, health condition, education, political views, content preferences and much more. These data could produce different types of profiles which suit different audiences that were traded between advertisers, publishers and other third-party companies. People's behavior, then, could be reordered into multiple segments of audiences, according to the online market and the bidding that traded them.

To do this efficiently, advertising and tech companies developed guidelines and technical features, which were more flexible, operated faster and were easier to enforce (by them). Keeping spam as a flexible category was important to tackle current and new emerging threats in the dynamically evolving EU web territory, while catering for online advertising, media and publishing needs. This flexibility can be illustrated in the many definitions of spam that are found *outside* legislation, showing that spam is much more than unsolicited bulk email; it just depends who and when you ask. Spam is also: illegal content, harmful content, pornography, spyware, malware, computer viruses, hacking, identity theft, illegitimate use of personal data, disruption of the network, fraud, and misinterpretation of contracts (European Commission, 2004), as well as: online gambling services, misleading and deceptive business practices, pyramid selling, and unlawful trade practices (OECD, 2005). The whole spectrum of evil things on the internet were embodied by spam and spammers.

What these multiple definitions of spam show is all the products and practices that might pose a threat to legitimate companies. Such classification has institutionalized and legitimized organizations' authority to define, enforce, and manage the online market territory. For example, pharmaceuticals, lottery and dating sites have a legitimate version and an illegitimate version. To regulate the online market, it was necessary to draw a line of legitimacy and legality by authorizing

specific products, companies and practices over others. Importantly, including spam not only with 'ordinary' direct marketing but also with porn, gambling, and other activities and products that are categorized as deviant made spam seem wholly evil. Cookies, by contrast, as the name indicates are very much wanted, as the Cookie Monster says—"C is for cookie, that's good enough for me". They are a form of communication necessary for the value-added experience of the web territory.

Making spam a resident evil was not implemented by governments, but rather by commercial companies under the European Commission's soft law approach. They did this by authorizing specific companies/websites while framing others as rogue. They also classified products, the way to circulate them (bulk) and the way to advertise them as illegitimate and, consequently, illegal. This helps to legitimize and institutionalize the online territory. But importantly, these strategies **train people's bodies** in what types of behavior are illegitimate and illegal.

Lobbying to Spam

As a global medium and a new market, states, and especially the private sector, wanted the web to be regulated, distinguishing between the legitimate companies and practices and the illegitimate ones. As Lessig argues, governments do this by indirect regulation: "it is not hard for the government to take steps to alter, or supplement, the architecture of the Net. And it is those steps in turn that could make behavior on the Net more regulable" (1999: 43–4). Since western governments try to appear as if they do not govern people's online behavior in disciplinary modes (that is the kind of things that only 'totalitarian' regimes do like Russia or China), they do so by delegating the regulation of digital territories to commercial actors. These media companies can then influence, modify and manage people's behaviors in a biopolitical way; ordering options of living whereby they can 'choose freely' within a digital space. As Lessig argues, governments are influenced by market forces, or, in this case, lobbyists from the advertising industry.

The advertising industry not only lobbied internet standards organizations such as the IETF (as shown above), it also targeted regulators to influence how the web should function. This is illustrated in Sylvia Kierkegaard's examination of the advertising industry lobbying campaign, led by IAB Europe, which pressured EU legislators to change the 'Cookie Article' (Article 5), while the final drafts of the e-Privacy Directive were being finalized. She argues that initially EU legislators proposed the opt-in mechanism, which made the digital advertising industry push for the opt-out mechanism. The advertising industry argued that this:

> [I]s a compromise between privacy protection and free enterprise. Cookies are essential to users and website owners. If prior users' consent was required, this would put them off from using the Web to search for information, products and services. This, in turn, would undermine the EU's overall strategy of building a competitive European e-commerce. (Kierkegaard, 2005: 316)

The same industry that emphasized the need for consent when it comes to receiving unsolicited communication (spam) argues that the demand for (prior) consent to cookies might damage and harm the whole EU web territory. Naturalizing cookies as the only way to make the web work was paramount. On 13 July 2001, the European Parliament's first amendments to the e-Privacy Directive proposal were to prohibit cookies altogether,[19] which was also the A29WP's suggestion in 1999:

> Cookies should, by default, not be sent or stored … This means for cookies that the user should always be given the option to accept or reject the sending or storage of a cookie as a whole. Also the user should be given options to determine which pieces of information should be kept or removed from a cookie, depending on e.g. the period of validity of the cookie or the sending and receiving Web sites. (1999: 3)

As Kierkgaard argues, "[t]he amendment caught the Commission, Interactive Advertisers and website owners by surprise because the cookie restriction would 'hinder' the growth of e-commerce and the industry's interest" (2005: 319). Consequently, the IAB, which was the most prominent lobbyist of the advertising industry in the EU, launched the 'Save our Cookie' campaign together with FEDMA and the Union des Industries de la Communauté Européenne (UNICE), which received the support of the online commerce industry. The strategy was mainly targeted towards MEPs, selling them the story that if website owners and publishers had to ask for people's consent before sending cookies, then they would lose millions of euros. The reason for the loss is the need to redesign their web pages to comply with this requirement. As they claimed, it would also harm their competitiveness compared to their non-EU counterparts, mainly the United States. Hitting the right buttons of the European Commission, they argued that this approach would harm the attempts of the EU to create a competitive EU e-commerce territory.

The final Directive was accepted by all sides on 30 May 2002, after a compromise was reached by banning spam in exchange for removing the wording accepting 'in advance' in the cookie Article and Recitals. This campaign was

successful, Kierkgaard argues, because there was no opposition from privacy interest groups since they were busy with their campaign to ban spam. Such privacy advocate groups, for example, the Coalition Against Unsolicited E-Mail (CAUCE), believed that spam is more dangerous as it can send viruses, while cookies can be deleted by browser preferences. The lobbying on people's understanding of the web worked.

The lobbying effects can be illustrated in the two most controversial sections, which are Article 5(3) and Recital 25. In Article 5(3), people are given the option to refuse cookies communication only *after* they have been sent, according to the opt-out approach. Recital 25 within this Directive takes specific note of cookies:

> However, such devices, for instance so-called 'cookies', can be a *legitimate* and *useful* tool, for example, in analysing the effectiveness of website design and advertising, and in verifying the identity of users engaged in on-line transactions. Where such devices, for instance cookies, are intended for a *legitimate* purpose, such as to facilitate the provision of information society services, their use should be allowed on condition that users are provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on the terminal equipment they are using. Users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment. (Directive 2002/58/EC, my emphases)

As Kierkgaard (2005: 321) shows, the previous versions of this Recital evolved from mandatory prior consent (Parliament amendment), to receiving information 'in advance' (Council position), to this version, whereby people get information about the purpose of cookies. As the European readers of this book probably noticed, this has not happened. This is precisely where EU legislation draws the line of legitimacy, where it authorizes cookies as a legitimate purpose because they are 'useful tools' for web design and advertising. It is also where EU legislators acknowledge that access to websites' content can be conditional on accepting cookies and identifying people. Additional lobbying effects can be found in the legitimization of the use of web-bugs in Recital 24 of the e-Privacy Directive:

> Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the *private sphere* of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms. So-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without

> their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for *legitimate purposes*, with the knowledge of the users concerned. (my emphasis)

The Recital admits that people's terminal equipment, that is, people's computers (and bodies) where web-bugs and cookies' tentacles are plugged into, are considered to be their private sphere without properly defining what it means. Such forms of communications are allowed because they operate according to 'legitimate' purposes, in other words—for economic purposes. All this means that the EU institutionalizes e-commerce, whereby the advertising industry finances users' free access to content by trading them. This solution was promoted after the dot-com crash as the new online market. However, this business model, and specifically the cost that people have to pay, was not made clear, heard, or even known to them.

Furthermore, publishers avoided their obligation to provide the reasons why they collected and processed individuals' data though obfuscation: they list the purposes in the contract sections of their terms of service. This section, called 'terms of use' or 'terms and conditions', relies on the fact that most people do not read these long, laborious, and jargon-laden texts. The texts are designed to be impenetrable, meaning if you have a job, dog, families and basically a life, you are not able to have enough time to read all of them. Additionally, even if you did understand, it would take months to go over all the included clauses, which are changed frequently on top of being hard to read. Importantly, these contracts do not include how collected data are used, when, and the other actors involved. In addition, according to Article 5(3), member states are supposed to police and enforce breaches of confidentiality in commercial spaces, which many times are located on servers that are not residing in Europe. In some cases, when people removed browser cookies, their access to the publishers' website was blocked.

This is all a matter of how legitimacy is understood on the web. Up until the 2000s, big companies' communications were classified as spam by European Union citizens. It was "reported by ISPs in most Member States that 80% of spam cases in Europe originate with the big American sites such as Amazon, Travelocity and Barnes & Noble, with whom the recipients have previously had direct contact" (European Commission, 2001: 89). To legally bypass what people perceive and define as spam, the second paragraph of Article 13 legitimizes and prioritizes big companies, and their marketing practices. Article 13(2) says that, if a person has bought something from a company on the web, the company can send

heradvertisements regarding the same kind of product or service, and it will not be categorized as spam. This falls under 'inferred consent': "consent which generally can be inferred from the conduct and/or other business relationships of the recipient" (OECD, 2005: 18). A single purchase may, therefore, be taken legally as the basis for a long-term relationship.

Framing spam as dangerous was a good diversion that allowed the cookie campaign to pass without objection. This was achieved by portraying spam as a form of communication that was not requested, sent for economic purposes in covert ways, which had the ability to track people and invade their private space while exploiting their data. The exact same definition, however, can also be applied to cookies. It is just a matter of which economic purpose is considered to be the legitimate one. In other words, spam and cookies are the same communication practice. Spam is categorized by commercial companies (advertising and media industries, ISPs, and publishers) as an unwanted form of communication and automatically removed outside of people's digital experience. Cookies, on the other hand, are usually categorized as wanted forms of communication (by online publishers, website owners, and the advertising industry) and sent into people's computers. In both forms of communication, people are not aware of such actions and they are conducted without their consent.

It is important to note that EU legislation and enforcement are not always effective. This makes sense because the soft-law approach creates an environment where enforcement instruments will be useless. As Mayer and Mitchell argue about the 2002 e-Privacy Directive—"In practice the directive has had little effect; member states have not taken any measures to enforce compliance, and in many cases they have treated browser cookie settings as adequate implementation" (2012: 418). Therefore, rather than regulating, these pieces of legislation create a discourse that naturalizes and institutionalizes the roles of each participant in the online automated market. It cements the central role of commercial actors in creating, defining, managing, and enforcing the online market. Nevertheless, the role of people in this online market had to be learned; new data subjects had to be produced, and the ways in which was done is elaborated below.

Composing the Data Subject

In the first half of this chapter I outlined how the EU web was reordered to produce a new territory. By redrawing boundaries of private and public spaces, the

digital advertising industry gained legitimacy and authority to enact power. Their power was to shape the web's architecture in a way that would enable them to conduct listening and create dynamic archives from the knowledge they produced. This knowledge then produced specific subjects who would behave in desirable ways. Several procedures were made to (re)produce EU citizens into data subjects, objects (their behaviors), communication channels, and **filters**. These procedures were mainly conducted by the advertising and tech industries and the European Commission to **train people's bodies** in using and understanding the web in a particular way: to shape them according to their data subjects role(s). This was achieved in three main ways: one, standardizing web metrics; two, providing 'control' mechanisms to control people; and three, educating for safety.

During the production of the EU digital territory, the advertising and tech industries wanted to produce people as data subjects that navigate within default setting architectures that structure their possible ways of living. They mainly wanted to be able to listen to their behaviors across the web, while **measuring** them using standardized tools and units. This enabled these media practitioners to train and institutionalize *themselves* in their profession's practice of commodifying people and their behavior. It also enabled them to statistically map human behavior online and establish categories for deviant and non-human behaviors. In addition, people were given 'control' mechanisms when they used the web, but here control was enacted *on* people rather than *by* people.

The concept of control was used against people as these options were predetermined, limited, and designed in a way that narrowed and managed the way they used and understood the web. Control also meant that, once people consented to cookies or expressed consent by using default settings, they were also made responsible for their actions. People were responsible even if they did not know the meanings or repercussions of such 'actions'. Finally, people went through an educational program designed by the EU called *The Safer Internet Action Plan*, that spanned between 1999 and 2013. Here, too, the word 'safe' was used not *for* the safety of people but rather to maintain the safety *of* commercial actors involved in the online market. The plan also educated people on behaviors that could jeopardize the safety of the EU online territory. These three procedures that produced EU data subjects will be examined in the following sections.

Standardizing Metrics

In the late 1990s and early 2000s, the need to fund the web gave birth to a project led by advertising trade associations. These **new experts** wanted to

clear the mess of multiple **measuring** methods and create standards that would allow advertisers to listen to people's bodies and then categorize, quantify, record their behaviors and, importantly, trade them. They wanted to be able to develop and standardize listening tools, units and capacities. As discussed above, some authorization was already achieved on another front, which was the production and **restructuring of the EU online territory**. The training of advertisers was necessary to institutionalize their profession on the web, and to create standards for the production of data subjects. Standardized metrics and measuring practices also helped in persuading brands to spend money on digital advertising. This was achieved by showing that the web is a profitable business that has wider and deeper listening capacities enabling more accurate and richer profiles and audiences to buy and sell.

The advertising industry has been interested in people's behaviors since its early days. As Adam Arvidsson argues, the production of people's "tastes, habits and preferences—was driven by the publishing industry" (2006: 46). Arvidsson observes that, because publishers were relying on advertising as their main economic source, even as early as the 19th century, they needed more information about their audiences to then sell them to advertisers. Now, more than a hundred years later, publishers rely more than ever on advertisers as they turned to a business model of free content rather than subscription. As Joseph Turow explains, "[i]n the mid- and late 1990s, publishers were in a race to show advertisers who had the most users, and if they wanted that kind of scale they couldn't charge a fee" (2012: 41). But nothing is really free.

As Thomas Novak and Donna Hoffman argue, at that time, the advertising industry's revenue model for the web was still unclear and it was not certain that companies would be able to generate money from advertising. The advertising industry, they argue, lacked "standards for what to measure and how to measure it … *standardising the Web measurement process is a critical first step on the path toward the successful commercial development of the Web*" (Novak and Hoffman, 1997: 1–2, emphasis in original). Just as doctors had to be trained to listen using a stethoscope, advertising practitioners needed to be trained to use online listening devices. Standard **measuring** practices to examine people's digital bodies were needed to produce data that could be traded efficiently between different types of media practitioner.

To establish consistent, comparable and accurate measuring methods and tools, the IAB in collaboration with the American Association of Advertising Agencies (AAAA), the Media Rating Council (MRC), and the Advertising Research Foundation (ARF) conducted a two-phase project. The first phase was

conducted between May and December 2001, whereby the IAB commissioned PricewaterhouseCoopers (PwC[20]) to examine several companies and identify the common audience and advertising delivery **measurement** metrics, definitions of measuring units and reporting. The companies that participated in this phase consisted: ad networks and ad-serving organisations (Avenue A, Engage, DoubleClick), destination sites (Forbes.com, CNET, *New York Times* Digital, Walt Disney Internet Group) and portal sites (AOL, MSN, Terra Lycos and Yahoo!). PwC's findings were published to the advertising industry on January 15, 2002, and each company had a choice whether to adopt the **measurement** guidelines proposed.

Phase two was conducted during 2003 and 2004, whereby the IAB processed PwC's findings and drafted standards from these to the whole advertising industry. This resulted in a document, published in September 2004, titled 'Interactive Audience Measurement and Advertising Campaign Reporting and Audit Guidelines'. The list of participants includes international ad servers such as AdTech (Germany), ALLYES (China) and Predicta (Brazil), and other participants such as: 24/7 Real Media, AOL, Disney Internet Group, DoubleClick, Forbes.com, Google, NY Times Digital, MSN, CNET Networks and Yahoo!.

All the companies PwC studied used the same five metrics to measure people's behavior: ad impressions, clicks, unique visitors, total visits, and page impressions. According to the PwC study, the definition of clicking was the most consistent of all the methods, and meant "a user-initiated action of clicking on an ad element, causing a re-direct to another web location. A click does not include information on whether or not the user completed the redirect transaction" (PwC, 2001: 13). The click, as Turow argues, was a "tangible audience action that media buyers and advertisers could use as a vehicle to ease their historical anxiety over whether people notice their persuasive message or, even more, care about them" (2011: 36). Clicking was an action that could be quantified and indicate people's preferences and behaviors across the web. This could then be easily used for trade.

Unique visits are measured by cookies (divided by new or repeated visits) or IP addresses. Both cookies and IP addresses identify specific people and tune in deeper to understand how frequently they have conducted an action to make more accurate measurements. In this way, people's rhythms matter because excessive behavior (repeated visits) which are not tied to a particular person can provide wrong analysis of the amount of people who actually visited that space. This is another reason why it was important to identify people – to avoid mismeasurement. Therefore, being anonymous can actually harm the accurate and credible measurement of people's behavior and consequently the ad industry's business.

Total visits, called 'sessions' are determined in various ways, but are mainly calculated by using three time-based rules that the digital advertising industry have developed: *Activity*, which calculates the user's activity data, *sampling* user activity over several days during a specific period (a measurement some companies outsource), and *statistical analysis* of the behavior (PwC, 2001: 24). In this way, people's behavior was collected, categorized, and recorded in different temporalities, by different media practitioners according to different **measuring** practices.

Ad and page impressions are measurements of people's viewing of an advertisement or a web page, respectively, which are listened to by two methods: web server logs or web-bugs. Web server logs are a type of dynamic archive that stores information about people's activity. These log files are automatically created whenever someone does an action on a website. These actions and those that follow are recorded and, importantly, tend not to be accessible to normal internet users. Using this measuring technique, digital advertisers decide which amount of time can be considered as an 'activity'—An impression. In this way, advertisers wanted to establish which repetitions have a value, a practice Facebook has developed further in their ad auction, as the next chapter shows.

Bodies that Count

Measuring people's behaviors was a central practice of the digital advertising industry. Through these measurements, the body and its abilities were conceived. Browsers have been holding a crucial position in this context as they function as devices providing sonic tools for producing knowledge about bodies. At the same time, they *are* people's body. With this dual function, every browser design choice, and especially default settings, is crucial; it sets the tone of the body. Every feature that browsers are automatically designed to do, directly shape how people can behave on the web.

As discussed above, developers like Montulli identified the power of default settings, and in this section we will unpack why. Browsers are important in introducing new ways to know people and their behaviors and enable redrawing the boundaries between the private and public spaces of their body. The metrics are measured using the technology (cookies, web bugs, and, more recently, fingerprinting) that browsers provide or operate. Browsers enable both the measuring and recording of knowledge, but also accelerate the listening process into milliseconds. This helped in creating different temporalities that can serve content and advertisements in the 'real-time bidding' (RTB) market (more on RTB below).

Contrary to the previous chapter, where Bell developed and maintained the media technology apparatus, when it comes to the web, the measuring devices and units, as well as the infrastructure of each of these fields is controlled and managed by different companies. The metrics are measured using the technology that browsers provide or operate, such as web server logs and cookies. Advertising content and technologies (such as cookies, web-bugs, pixels) are sent to people by either the first- or third-party server or the client. In this way people's bodies are being penetrated by various technologies to measure and record as much data on them as possible. These measurements are conducted continuously, because the more you know, the more you can monetize.

Bringing back the dilemma of accuracy of **measurement**, the digital advertising industry was conflicted on how to measure which bodies are human, and therefore should count. The IAB pushed for the client-initiated method of measurement, which relies on the user's browser, to become the standard. As the IAB argues, this method creates a direct connection between people and the ad server, it requires:

> [C]ounting to use a client-initiated approach; server-initiated ad counting methods (the configuration in which ad impressions are counted at the same time the underlying page content is served) are not acceptable for counting ad impressions because they are the furthest away from the user actually seeing the ad. (2004: 5)

Considering browsers to be more precise in indicating people's actions and reactions to content established them as the standard measurement device. Here the notion of the body becomes complicated. Usually, people come to practitioners on their own initiative to solve some kind of bodily malfunction. In the case of digital advertisers, the person's body 'requests' to be listened to, but without her knowledge. This was made possible by the browser's default settings, which creates a situation in which people technically request their bodies to be listened to. Yet most people have no idea that such practices are being conducted.

Just as physicians need to get closer with a stethoscope to people's bodies to listen accurately to the sounds they make and understand the malfunction, here, too, people's computers operate as their bodies. Getting closer to people through their browsers allows for closer listening and tuning in to measure their actions across the multiple spaces they navigate more precisely. It also allows the digital advertisers to listen to bodies over different periods of time, deciding which ones will be considered as a human action. This standardization meant that people's computers functioned as their bodies *and* the measuring devices that listen to their

behaviors and malfunctions. However, people were given limited mechanisms to examine their own bodies, while media and advertising practitioners could diagnose them using sonic tools.

When people perform any action on the web (even if it's silent and does not have any visual cues such as hovering over an item or spending a long amount of time on an article), their browser sends a request to have the behavior of the person tracked by three technologies, called 'tracking assets': one, web bugs (discussed above); two, an HTTP 302 request initiated by the browser when a user requests an image or rich media from the server by clicking on them (this is an independent request sent to an ad transaction logging server and might also send a web bug); three, delivery of the ad content. Furthermore, "[o]ne tracking asset may register impressions for multiple ads that are in separate locations on the page" (IAB, 2004: 6). This is how people's behavior in multiple location on one webpage is being listened to. Here the advertisers tune in deeper, trying to figure out how people engage with ads and content on a particular webpage.

The advertising industry measures people's behavior and renders it as data, objects of knowledge to mold, control and monetize. These measuring tools also help in knowing which websites, content and ads are more popular in terms of the number of people who make actions on them and, consequently, differentiate these spaces with higher rates.

In this context, processed listening is applied to individual[21] bodies through people's browsers to create profiles. But at the same time digital advertisers also search for audiences behaviors, listening to statistically measure the way groups of audiences behave in specific repetitions. Listening in these micro and macro levels simultaneously enables digital advertisers to create more accurate profiles and segments according to perceived preferences or personal traits. Examining the surveillance practices of the advertising industry on the web, Campbell and Carlson (2002) suggest that the commodification of people's privacy in exchange for people's ability to participate on the web converts them into economic subjects. They argue that privacy laws have detached information about people as objects and in opposition to individuals. Producing people as fragments of data to be recomposed into specific profiles is also carried out as part of the digital advertising practice itself. Here the code becomes the law. As Campbell and Carlson observe:

> [C]onsumer profiles constructed from our social positionalities—that is, on the basis of race, gender, age, class, education, health, sexuality, and consumptive

> behavior—become our economic selves, reflecting our value within a commercial society … effective classification equates with predictive utility the more precisely a marketing firm can classify an individual as a potential consumer, the more effectively that firm can predict (and manipulate) an individual's consumptive behavior. Ultimately, predictive utility allows marketers to reduce the risk producers face in the marketplace. (Campbell and Carlson, 2002: 596)

People's behavior, therefore, is paramount for the smooth operation of these multilayered communication channels and multi-sided automated markets. Listening to these behaviors and creating profiles and audiences can help the digital advertising reduce their uncertainty and predict their suitable matching to particular products, services, and spaces. As Bhat et al. argue, advertisers want to know the efficiency of their targeting practices, "whether their users' actual profiles match desired profiles. Knowledge of current users' profiles also enables advertisers to be more effective in future targeting efforts" (Bhat et al., 2002: 105). This is the reason why any behavior that can damage or confuse the accurate **measurements** of behavior must be controlled and avoided.

A problematic aspect of measurement for advertisers are bots (also called crawlers and spiders[22]), bodies that interfere with accurate measuring and the production of data subjects. This is similar to medical professionals who need to specialise in using the stethoscope, by navigating in "an initially confusing world of sound by differentiating the sounds of the patients' bodies from the sound produced by the tool itself and the sound of their own body" (Supper and Bijsterveld, 2015: 10). In digital spaces, the confusion goes further as advertising practitioners need to distinguish between human and non-human behaviors. Because the web is filled with robotic behaviors, it is necessary to make a distinction between them for accurate measurements to enable efficient trade in the online advertising display market.

To avoid measuring non-human traffic and maintain accuracy and consistency, the IAB developed guidelines for what it calls *filtration*. Advertising practitioners carry out this rhythmedia through three main **filtering** methods: 'basic' techniques, identification of specific suspicious nonhuman activity, and pattern analysis of people's activity. In the basic technique, advertisers use robot.txt files "to prevent 'well-behaved' robots from scanning the ad server" and exclude behaviors "from User Agent Strings[23] that are either empty and/or contain the word 'bot' " (PwC, 2001: 29). With the specific identification approach, non-human traffic is identified through the IAB Robot List. By cross checking with that list, digital advertisers are able to exclude known and authorized robot traffic from **measurements**. According to the IAB, companies need to exclude

automated page refreshes and also disclose their internal robotic traffic; for example, IT personnel testing features on websites. In this way, advertisers should be able to identify excessive behaviors associated with previously identified 'well-behaved' bots or maintenance behaviors, and exclude them from the measurement procedure. Similar to physicians, advertisers produce knowledge that establishes what constitutes a 'healthy' (human) body which should be counted, and what should not be counted.

In the third technique, the activity-based approach, advertisers are obliged to take measures against 'new' robotic or non-human activity by analysing server log files data: "Activity-based filtration is critical to provide an on-going 'detective' internal control for identifying new types or sources of non-human activity" (IAB, 2004: 7). This method tries to analyze and detect new behaviors which sound human, but are, in fact, non-human. Advertisers monitor for problematic rhythms on the web in order to establish what is considered human. Some advertisers use advanced behavioral **filtering**, which defined rules characterizing robotic behavior as a body that clicks more than 50 times during a day (PwC, 2001: 29).

Advertisers are encouraged to listen to server logs, which helps to identify abnormal behaviors in four main ways: identifying people who are performing multiple sequential activities; people with the highest levels of activity; people who act in consistent interaction attributes; and 'other suspicious activity'. Any behavior that deviates from the norm is under suspicion of being non-human—a bot.

As these methods indicate, abnormal behaviors are categorized according to frequency, repetitions, and other time-based movement variations which deviate from the norm. These thresholds have been established from an ongoing processed listening to people's behaviors across multiple spaces on the web. Importantly, these four criteria also imply that there are guidelines of specific 'legitimate' bodies' behavioral traits. These filtration guidelines standardize the distinction between human and non-human behavior on the web. According to such standards, the way humans behave is categorized as inconsistent, low-level (repetitive) activity and sporadic singular activities. Human rhythms are standardized.

Importantly, the issue of filtration points to the difficulty of measuring accurately and the need to control and manage people's behavior to avoid mistakes in calculations. This is precisely why it was so important for the advertising industry to make spam illegal through legislation, and the reason why spam's characteristics in legislation were 'automated' and categorized as 'bulk behavior'. Such non-human behaviors can damage the advertising industry's ability to make sense of their measurements, and therefore, risk creating inaccurate profiles and audiences. Therefore, making spam illegal is a regulatory tool that serves to control both

people's behaviors and advertising or technology companies that do not comply with these online market territory standards.

Measuring people's behavior is part of an online market called 'online display advertising' which is happening at the back-end of people's browsers to decide what, when, and where to 'display' things at the front-end of each person, or in advertising terms—profile. It is a multi-sided market where advertising networks argue that they trade 'inventory', advertisement slots. However, another thing that these ad networks trade are people, or as IAB calls it 'audience buying'. This means that the 'cookie communication' is conducted between advertisers and publishers, while the 'message' is people's behavior measured in standardized quantitative units, and rendered as data. One of the outcomes of this communication is the placement of an ad that matches the supposed person's profile and behavior suitable for that particular place and time, and it happens within milliseconds.

The rhythm of communication in this online market accelerates as non-human actors are introduced into the multiple channels in the back-end. The advertising industry, led by the IAB, standardized both people's behaviors and advertisement sizes,[24] by filtering, removing, and excluding these disturbances. In doing so, they reproduced people and spaces to create optimized options of living in structured architectures, a new commercial territory. Ad networks create multi-layered automated communication channels that operate by monitoring, measuring, categorizing, recording, and archiving people's online behavior. Both people *and* spaces are **measured**, to produce a dynamic archive and determine which actions and architecture design are most economically beneficial. Hence, while the fast-rhythm communication channels were legitimized as sound, other high-tempo communications were constructed as noise and categorized as spam, and, consequently, criminalized.

Bidding for Real-Time

Advertising networks were later supplemented by ad exchange to expand the new automated market and increase the rhythm's pace. According to IAB UK, ad exchange, which started to appear in 2005 as a service offered by a company called Right Media, is an:

> Online auction based marketplace that facilitates the buying and selling of inventory across multiple parties ranging from direct publishers, Ad Networks and Demand Side Platform (DSP). These automated marketplaces enable sellers to monetise inventory via acceptance of the highest bid from buyers. (IABUK, 2005: 13)

These trading practices use Real-Time-Bidding (RTB) automated bidding, a multi-layered system that started in 2010, trading people's profiles and audiences (knowledge) in 'real-time'. But the way that time and space are reproduced in this algorithmic rhythms at the back-end of this ecosystem is not mimicking real-time.

The concept of 'real-time' can be traced back the term—'Real-Time Processing' and linked to John von Neumann's 1940s computers architecture that separated the computer's processor and storage. As Robert Gehl (2011) argues, this design was a specific orchestration between the 'immediate' that was the processor or CPU, and the 'archive' where the storage of data was kept as a sort of memory. In this architecture design, different computation instructions retrieved pieces of small data from the archive to provide different output configurations. As Gehl shows, "the processor focuses on speed and discrete operations. It manipulates small chunks of data as quickly as possible, moving sequentially through each element of complex equations" (Gehl, 2011: 1230). By the 1960s computer designers aspired to create an experience whereby the computer immediately reacts to people in 'real-time', creating a feeling of instantaneity which conceals the procedures in the 'back-end'.

Trying to create the feeling of immediacy while concealing the procedures happening at the back-end is exactly what the practices processed listening and rhythmedia are about. It is about silencing and automating decisions about how media is conducted and creating a feeling that things are happening in real-time, with no intervention. But quietly in the back-end of media systems, media practitioners conduct processed listening—monitoring, measuring, recording—to produce a dynamic and ever-growing archive from people's behavior. Once this knowledge is produced it is ordered—categorized, filtered, and 'displayed' in a particular way. In this case, there is no one archive and one processor, it is personalized to each person's profile. The multiplicities of actors, spaces and temporalities is what makes processed listening and rhythmedia more suitable to the online ecosystem. In this ecosystem, there are multiple media actors, human and non-human who are repetitively (re)produced.

In RTB, new actors join this mix—Demand Side Platforms (DSP) and Supply Side Platforms (SSP). DSP is a centralized management platform technology for advertisers and companies allowing them to buy audiences in an auction across multiple suppliers. SSP is a centralized platform technology for publishers who sell audiences and spaces (the supply) to advertising networks, advertising exchanges, and DSP. The extra layers of communications created by ad networks and exchanges, as well as DSP and SSP, are mainly facilitated by third-party cookies. They create a new territory for financial trade that functions in a separate

time and space. Therefore, the name 'real-time bidding' is misleading because the system that operates it creates different temporalities, accelerated rhythms for trade which are so fast that humans cannot comprehend or notice them.

In this way, the type of things (content and ads) and options that people engage with, and the timing when they will be ordered change according to their behavior. The ordering changes according to the rhythmedia that is the most profitable for the advertisers. This means that what affects the ordering of advertisements in a particular place and time depends on the suitable audience (combining data subjects' profiles, their online behaviors, geographical location and more), as well as the highest bidding for that slot. RTB, which relies on 'real-time processing', disguises the fast-rhythm decisions that happen at the 'back-end' by non-human actors, to order the 'front-end' human experience. A frictionless experience of asymmetric power.

RTB started as a pilot project in November 2010 by IAB and other advertising technology (commonly called 'ad tech') companies who were called the 'Open RTB Consortium'. Shortly after its inception, the name was changed to the 'RTB Project'. In January 2012, the Open RTB API Specification version 2.0 was released to set an industry standard for the automated trading of the online environment. This standard involved more than 80 ad tech companies and intended to make the communication between them more efficient. The standard aimed to incorporate the support of features such as display mobile and video in one document. As the IAB say:

> The protocols outlined in this document should be considered guidelines, not absolute rules. The overall goal of OpenRTB is to create a *lingua franca* for communicating between buyers and sellers. The intent is **not** to regulate exactly how each business operates. As a project, we aim to make integration between parties easier, so that innovation can happen at a deeper-level at each of the businesses in the ecosystem. (IAB, 2012: 3)

The digital advertising industry wanted to create new communication channels that would talk to each other in the same language to bridge between the multiple advertising companies involved in this new ecosystem. Importantly, the digital advertising industry aimed to standardize its profession by not making specific rules but rather making the practices involved more economically efficient and more flexible. As always, the advertising industry showed that it is allergic to the term (and practice of) regulation, because it hinders 'innovation'.

Outlining the data needed for bidding, the IAB indicates that it is recommended to have several objects which provide detailed information about

the user: The 'device object' provides information on the kind of device the person who gets the ad uses, such as mobile phone, computer hardware, the device model, the device operating system and its version, and carrier or ISP. The 'user object' provides a description of the user including unique identifiers such as year of birth, perceived gender, and keywords of interests. The 'geo object' gives description of the device's location according to IP address, GPS or home geography of the user according to registration data, including country, city, ZIP/postal code (IAB, 2012: 14, 30, 31). These specification for trade illustrate how processed listening is conducted to assemble as much data on people as possible to be able to tailor ads for the preferences that fit their profiles.

This rhythmedia is done according to specific times and spaces across the web where ads fit according to the highest bidder. Auctions are required to be conducted in a specific time, termed *tmax*, which has to be indicated in the bidding request in milliseconds: "e.g., 120 means the bidder has 120ms to submit a bid before the auction is complete". This parameter shows how there is nothing 'real' in RTB and that people's online experience is ordered according to the highest bidder. It also illustrates how the 'back-end' has its own temporality, too fast to regulate or monitor by regulators, journalists, scholars, and sometimes even the advertising associations themselves.

The latest OpenRTB 3.0 Framework came out as a draft for public consideration on September 2017. One of the features proposed in this standard is Consumer Identifier Support, which aims to use audience data in RTB, and "to solve for diverse use cases around identity including: Support for cross-device models in bid-stream, Allow for the ecosystem of 'single IDs', People-based identifiers of all types" (IAB, 2017: 30). The problem in **measurement** arises with the fact that people use multiple devices and hence the difficulty of identifying their bodies for consistent monetization is at the core here.

However, as a recent EFF report indicates (Cyphers, 2019), some advertisers conduct "shadow bidding" because the information about people's profiles is sent during the bid request but before the money goes to the 'winner'. In this way, advertisers still get information about people and can enrich their database. "Certain companies may pretend to be interested in buying impressions, but intentionally bid to lose in each auction with the goal of collecting as much data as possible as cheaply as possible" (Cyphers, 2019). People have been cheaply traded, but the cost of this market has not been thoroughly processed, and people's lives are at stake.

Even before RTB, timing in advertising was important. As Campbell and Carlson show in their analysis of the advertising network, in the late 1990s and

early 2000s, DoubleClick developed a technology called Dynamic Advertising, Reporting and Targeting (DART). After processed listening to people's behavior, rendering it into data, and assembling initial profiles, DoubleClick aggregated their behaviors into 'real-time' reports. The slogan promoting DART stated that it is a technology that "enables you to deliver the right message to the right person at the right time" (Campbell and Carlson, 2002: 598). As the slogan suggests, the right people and the right timing were key to ordering this online trading territory. But the 'right' people, spaces and timing are not naturally existing, just waiting to be sorted. Rather, they are produced by a specific rhythmedia conducted by the digital advertising industry, which orchestrates and **filters** whoever and whatever do not fit into its business model.

All these multiple layers of communication channels work in a recursive feedback loop, whereby people are the starting and end point—people's actions are monitored, **measured**, and archived in specific categories (according to criteria such as gender, age, location, preferences, marital status, health status), then rendered as input objects/data. This data is communicated through cookies, thereby becoming messages in the automated market trade conducted by ad networks, ad exchanges, DSP and SSP. The accelerated rhythm of RTB, is based on algorithms that make predictions based on inputs given by cookie communication about the kind of profile that might fit a tailored advertisement. The output is ordered in a specific location and time on the publisher's standardized space that is supposed to suit the profile of the target user, the 'right' rhythmedia. The data subject is fed back with content and arrangements through generating dynamic web pages and advertisements that are supposed to fit them, according to the highest bidder. By the end of the 1990s, as Lev Manovich observes:

> Every visitor to a Web site automatically gets her own custom version of the site created on the fly from a database. The language of the text, the contents, the ads displayed—all these can be customised by interpreting the information about where on the network the user is coming from; or, if the user previously registered with the site, her personal profile can be used for this customization. (Manovich, 2001: 60)

Publishers and advertisers listen to people in various spaces to establish a profile and then reorder the website according to this profile and what is associated with the audiences that the profile relates to; a personalized experience. This rhythmedia happens within milliseconds which is what creates the 'real-time' experience despite the many processes involved to create this immediacy sensation. All this happens at the 'back end', covertly, without people's knowledge. In

this way, the IAB's **measurement** standards documents provide the new media practitioners—digital advertisers—with training guidelines on the use of listening devices and the way to listen to people's digital bodies. At the same time, it produces the personalized experience as the preferable one for people, while disguising the cost behind it.

IAB's guidelines train different actors within the online market chain (advertising networks, advertising associations, advertising companies, data brokers, and publishers) on how to conduct *processed listening*. It teaches them how to listen to different digital bodies by using several tools (server logs, IP addresses, cookies, web bugs), at different times, to produce data subjects that they can monetise. This involves collecting, categorizing, archiving, and **filtering** data extracted from users, which can be done in different temporalities to produce subjects (knowledge) and the territories with which they engage.

As with most research, the most interesting things happen while you are trying to submit your book to your publisher before the deadline. In June 2019, The UK Information Commissioner Office (ICO), the regulator responsible for data protection, released their updated report on ad-tech and real time bidding. As they argue:

> Finally, RTB also involves the creation and sharing of user profiles within an ecosystem comprising thousands of organisations. These profiles can also be 'enriched' by information gathered by other sources, eg concerning individuals' use of multiple devices and online services, as well as other 'data matching' services. The creation of these very detailed profiles, which are repeatedly augmented with information about actions that individuals take on the web, is disproportionate, intrusive and unfair in the context of the processing of personal data for the purposes of delivering targeted advertising. In particular when in many cases individuals are unaware that the processing takes place and the privacy information provided does not clearly inform them what is happening. (ICO, 2019: 20)

Although the ICO found the advertising industry violating many data protection issues (according to the General Data Protection Regulation became enforceable in May 2018), the enforcement remains 'soft', as the conclusion of this report is made to 'express their concerns' and expect the industry to 're-evaluate their practices'. Such mechanisms, like the ICO and other data protection regulators, are meant to make citizens feel that their rights are protected whilst in reality their enforcement tools are limited. The self-regulation model of the advertising industry enables an online territory where everything goes and people are up for the highest bidder.

One of the main arguments of the advertising industry against claims of surveillance and privacy is that people are empowered by experiencing personalized spaces, engaging with content and things they are interested in. As the advertising industry argues, people are given a free choice and abilities control through various design mechanisms. But, as will be shown in the next section, 'user control' and autonomy have different meanings and functions to different actors.

User Control to Control Users

As the web developed, people were given more tools to control and manage their mediated experience. In 1997, the IETF working group, led by Montulli and Kristol, mentioned above, recommended that people should have control and the ability to decide for themselves on the way their bodies communicate their behaviors. As they argue, "[u]sers may object to this behavior as an intrusive accumulation of information, even if their identity is not evident (Identity might become evident if a user subsequently fills out a form that contains identifying information)" (Kristol and Montulli, 1997: 15). They recommended that browsers should have a visual display of such forms of communication, which, as Netscape showed with its development of SSL, is possible to do. Imagine a split screen on your browser, similar to adblocking software or tracking monitors such as Firefox's Lightbleam or the EFF's Privacy Badger. This would enable people to (partly) listen to what is happening in the back-end, to inspect their own bodies and reveal the multiple chords (cookies) connected to their bodies, as well as their sources. Now imagine this was the default setting from the late 1990s. Keep this thought with you while you read this section, it will help you listen to the distortions in the stories of the advertising industry.

By creating a default whereby browsers accepting first- and third-party cookies, and relying on the fact that people usually do not configure those preferences, this control tool was designed to persuade people to open their bodies for inspection by anyone that could. Instead of enabling people to control their own experience, it was a mechanism developed by the advertising and technology industries that did the exact opposite. In this way, first- and third-party cookies enabled these industries to processed listen into (measure, collect, record, and archive) people's online behavior. People's lives on the web became objects of knowledge that were used by various media practitioners for various purposes.

The pressures from the digital advertising influenced the way the cookie standard was baked into the web's design. Montulli and Kristol's tone regarding

the IETF cookie standard changed between the versions. Their 1997 proposal suggested that browsers should ask people whether to create a 'stateful' session, saying the default should be 'no'. In the 2000 version, their version was much softer and lenient towards browsers' defaults. In that version, they argue that, "[i]nformed consent should guide the design of systems that use cookies" (Montulli and Kristol, 2000: 18). Presenting 'informed consent' as a form of people's expression of control and autonomy was a way for tech and advertising companies to manage people's behavior, and to train them on what they could and especially could *not* do through browsers.

The issue around spam and whether communication is 'unsolicited' shows how people's autonomy on the web was framed as a binary option, boxed into consent or not. This was a way to control the way people behaved on the web but also, importantly, to train people to think that these were the only two options. Rather than asking what other things people could do in this territory, EU policy, which was influenced by lobbyists from the digital advertising and tech industries, focused on debates about how people expressed consent. In doing so, the EU legislation discourse on behaviors on the web was narrowed into standardized and automated architectures provided by browsers. In fact, it was not until 2011 that the A29WP published a document clarifying the meaning of consent; its key characteristics are: 'indication', 'freely given', 'specific', 'unambiguous', 'explicit' and 'informed'. As the EU legislators 'found out', it is more nuanced and complex then binary consent or not. As the A29WP argue:

> The autonomy of the data subject is both a pre-condition and a consequence of consent: it gives the data subject influence over the processing of data … The data controller may want to use the data subject's consent as a means of transferring his liability to the individual. (A29WP, 2011: 9)

Inspired by western liberal thought about freedom, the definition of consent always assumes a rational person making decisions based on all the information and facts available. But in the online territory, to make an informed consent people need to know how the ecosystem works: How is this ecosystem funded? Which companies are listening to their bodies? What is the value of their behaviors (data)? What kind of data do these companies use and for what purpose(s)? How might that affect people in the near and far future? How much time will this data be used for? Will this data be used in other contexts and by other companies? And much more. But even technology savvy, and technology companies' CEOs such as Mark Zuckerberg[25] have argued that they do not know how their systems work, so how can we expect people to make 'informed' decisions?

People make decisions according to their emotions, cultural background, education, cognitive abilities, financial situation, family history, different media representations they engage with, health condition, religious beliefs, gender identity and many other parameters. To assume that a decision can, in the words of EU legislation be "freely given" and "informed", is misguided and simply wrong. As Foucault argues, "freedom of behavior is entailed, called for, needed, and serves as a regulator, but it also has to be produced and organized" (Foucault, 2008: 65). As the 2016 USA presidential election and 2016 UK Brexit referendum show, many important decisions can also be influenced by micro-targeting. Thanks to the design of online platforms, which conceal what happens in the back-end, these messages are tailored, personalized and targeted through computational procedures to influence people's behavior. And these are far from rational or informed, as some reports indicated that many people searched for what the European Union means after the UK Brexit results were announced (Fung, 2016).

Consent has traditionally been used as part of a contract. You sign a contract for a house, job, or insurance, as an indication that you agree to the conditions of the product, service, or employment. Whereas these contracts are static and usually deal with one particular aspect of your life, online contracts are far from it. In fact, it will take you days, if not weeks, to read the terms and conditions of all the contracts of the online services, platforms, and apps you use (Hern, 2015). I should know, because to do the research for this book I read and archived different section on Facebook's terms, and that was when I focused on particular aspects, not all of the terms. The more I read, the more I discovered other subsections, it was never-ending. Even if you do read all these terms, and manage to understand all the legal jargon used, online services frequently change their terms without notifying people. In this way, people have no way of engaging with and understanding what they actually consent to.

Even if you do manage to make the time and read all the terms, and companies will follow the recent GDPR's Article 12 which requires them to be transparent about their procedures, it is still not enough to make an 'informed decision'. Studies from the end of the 1990s until today show that most EU citizens do not know about the existence of cookies, their management mechanisms, or how they work, and are worried about their personal data being used by third parties without their knowledge or consent (Eurobarometer, 1997, 2003, 2008; Smit et al., 2014). As Andrew McStay, who examines the revised e-Privacy Directive (2009/136/EC), argues, "[t]he simple truth is that most people do not understand the mechanisms through which behavioral advertising works" (McStay, 2013: 600).

This inability to make sense of online contracts is what Mark Andrejevic calls the 'data divide'. As he argues, "putting the data to use requires access to and control over costly technological infrastructures, expensive data sets, and the software, processing power, and expertise for analysing them" (Andrejevic, 2014). In short: we simply cannot understand how processed listening and rythmedia work and especially what happens in the back-end. We do not have the processing abilities and big (advertising) tech resources to understand the soundtrack of this online market. And here lies the power of being able to *conduct*, *know*, and then to *produce* what is happening at all the multi-layers of these mediated territories.

Consent then, is used to transfer responsibility to individuals, while presenting it as a control mechanism that people can use over their own data, meaning their own bodies. As Becky Kazansky argues, this kind of 'responsibilization' is "[e]ncouraging an emphasis on the individual as the primary locus of responsibility for protection from harm … [and has] the convenient effect of deflecting attention from its causes" (Kazansky, 2015). Another reason is that it makes us legally responsible for our actions, something that benefits commercial and governmental bodies.

The notion of 'consent' naturalizes and normalizes digital advertising and technology companies' terms of use for their technologies and services. It teaches people the boundaries (actions and spaces) that they can operate in. This is the shift from 'power over' as Foucault presented in sovereign mode of governmentality and, to a lesser extent, discipline, into other forms of power 'from below' in the shape of biopower. Consent is a control mechanism portrayed as agency, but gives **license** to these industries to redraw the boundaries of people's bodies and the territories in which they live. It also marks the boundaries of what people can demand and expect from commercial actors and state regulators. This signals that what people could do on the web was not open for discussion, negotiations or multiple options. Portrayed as control, autonomy and power, responsibility was moved from the service or technology providers to people, who were presented as responsible for their actions because they were expected to be informed about all the repercussions of such a decision, as rational beings.

As Greg Elmer shows in his research on Netscape's Navigator and Communication web browser versions, this disruption to people's online behavior and experience has been an ongoing practice since the late 1990s: "Internet users who exert their privacy rights in cyberspace by disabling their browser's cookie preferences also significantly disable the Web's ability to offer them convenient services and relevant information" (2003: 117). Thus, the introduction of user control tools for expressing power or autonomy online was limited and managed by tech and

advertising companies' design and standards. It constructed a rhythm of repetitive movements and helped in **training people's bodies** as data subjects and their limited options of living on the EU web.

The 'control' narrative creates a contradiction, as Robert Gehl (2014) argues, because the IAB and other advertising trade associations present the subject they produce as a 'sovereign interactive consumer'—a free, autonomous and powerful self-manager when it comes to their choices on the internet. This subject is free to choose to be educated about advertising practices and go to the preference section in their browser to change the default setting. The subject is in control of their online life. As Gehl argues, "if the sovereign interactive consumer *chooses* to be educated, to understand the workings and benefits of behavioral advertising, the IAB is ready. If not, so be it" (Gehl, 2014: 109). As Gehl points, if the subject does not know about these things, then the IAB will not help educate them. In that case, it will be the subject's fault if anything related to their online behavior and profiling causes them harm in any way. Knowing is power, and here what each player knows, how deep they can listen and produce knowledge (data subjects) comes hand in hand with people's lack of knowledge about what happens to their bodies. As will be shown in the next section, the topics that EU citizens were taught through educational programs were meant to help the safety of commercial actors, not to know how things work. In this way, 'control' is a narrative tool meant to control people behavior and understandings of how the web works.

Keep Your Body Safe

An important step in creating the EU data subject was education. In the sections above, some of the educational tools were applied through architecture and design. This helps to **train people's bodies** to behave in repetition and shape their thinking and understanding of what they can do and what their responsibility is within this territory. Here, the production of data subjects continues in the shape of educating EU citizens on how to use and understand the internet in a particular way, highlighting the ways to make it more economically efficient. EU citizens are taught about **filtering** tools, rating systems, and hotlines to report bad behaviors of other. The soft-law approach meant that these technical mechanisms were designed and operated by other players in the EU—internet industry, the ISPs, and copyright holders.

In a recent report Doteveryone, a British Non-Governmental Organization (NGO) examined people's understanding of the internet. As the organization argues, "Digital understanding is not about being able to code, it's about being

able to cope. It is about adapting to, questioning and shaping the way technologies are changing the world" (Doreveryone, 2018: 5). According to the organization, there is a lot of focus on 'digital skills' (especially access) in the digital divide/inequality debate but little attention to understanding of these technologies. We do not need to know how to read code or algorithms but we do need to understand who has access to our data and more importantly how the internet shapes our lives.

As this section shows, the European Union did develop education programs, but these were not meant for people to understand how the internet works. These educational programs have helped to cement and institutionalize EU citizens' roles as consumers and products in the online market territory. Although framed as 'safety' education for people, the material that EU citizens were taught was mainly about maintaining the safety of all the organizations that create, manage, and control the internet: governments, copyright holders (of various types of content), ISPs, publishers, digital advertisers, browsers and others.

The Safer Internet Program that the European Commission developed was presented as if it is meant to keep the citizen safe. Ultimately, it meant to educate and **train people's bodies** how to behave, think and understand their positions as both data subjects but also as communication channels that need to monitor and **filter** other people's unwanted and problematic behavior and content. This was done by providing citizens with controlled listening tools to identify and police their peers' deviant behaviors. Similar to the questionnaires the NAC circulated, these tools came with pre-decided categories of what is deviant, illegal and harmful. In this way, just as NYC citizens were encouraged to report noisy people, EU citizens were encouraged to listen and identify noisy behaviors and report them through special hotlines. These education programs were primarily designed for children in schools. This was a way to start **training the digital bodies** of children from a young age about their role within the online EU territory, and, even more importantly, not to teach them other ways of behaving that might turn out to be problematic.

The first document that paved the way for the Safe Internet Programs was the European Commission's communication on *Illegal and Harmful Content on the Internet* from October 16, 1996. This document was one of the first discussions presenting the EU's attempt to control and govern the internet. Importantly, the document made clear that previous definitions of illegality persist on the internet:

> As regards the distribution of ***illegal content*** on the Internet, it is clearly the ***responsibility of Member States to ensure the application of existing laws.***

> ***What is illegal offline remains illegal online,*** and it is up to Member States to enforce these laws … the presence of illegal and harmful content on the Internet has ***direct repercussions on the workings of the Internal Market***. (Commission of European Communities, 1996: 4, emphasis in original)

This means that the legal framework remains the same and that any illegal activity that was outlined in EU or national laws persists. Additionally, older media forms and their associated laws, including copyright and distribution contracts, as well as all member states' authority to decide on what is legal and illegal on the EU internet, persist. This can also be illustrated in the main concerns the European Commission pointed out, which included protection of reputation and intellectual property. Keeping commercial bodies protected was essential. The European Commission highlighted the huge advantage the internet has for the advertising and marketing industries. As it argued, "[b]ecause of its interactive nature, and the immediacy and ease of communication, advertising messages can be targeted at audiences much more precisely than has been possible until now, and feedback obtained from current or potential customers" (Commission of European Communities, 1996: 6). This is an indication that, even at that early stage, the EU was aware of the practice of targeting people individually and turning their behavior into knowledge and commodity to enable advertising and marketing industries to support the internet's funding.

According to the document (Commission of European Communities, 1996), it is important to separate illegal from harmful content as these are different categories that require different legal and technological solutions. While illegal content is mostly linked to pornography and copyright material, when it comes to defining what exactly the European Commission means by 'harmful content', there is no clear definition. The only point mentioned is that this kind of content depends on cultural differences and, therefore, each member state can decide what is harmful according to its own cultural values and ethical standards. Similar to the discussion above on the lack of clear definitions of spam within legislation, here again, some terms are not defined and, under the soft law approach—this power is delegated to commercial actors. In this way, commercial actors are authorized to form the categories and definitions of what constitutes illegal and harmful content, and then regulate and enforce it.

One of the most important points in this document is about the education of all actors in the then new online territory to behave according to their roles: "in this highly decentralised Internet environment, ***Internet Users have a very important role to play*** in contributing to industry self-regulation" (Commission of the European Communities, 1996: 14, emphasis in original). Part of the people's

role is to detect and report illegal and harmful content to 'hotlines'. By doing so, people operate in a similar way to the telephone operators, as feedback loops helping to improve and stabilize the online trade territory. Just as the telephone operators were given controlled listening capacities to monitor each other through *Hear Yourself as Others Hear You* and counselling, here, too, people are advised to use hotlines as a peer-disciplining tool. This, the document argued, would be more effective after public education, which would include awareness activities to train people to understand how to behave on the internet. Such 'solutions', under the soft-law approach, gave a **license** to commercial actors to define illegal and harmful categories according to their economic interests.

The Safer Internet Action Plan started in 1999 and consisted of three programs: the Action Plan for a Safer Internet 1999–2004 (276/1999/EC), the Safer Internet Program 2005–8 (Safer Internet Plus) (854/2005/EC), and the Safer Internet Program 2009–13 (1351/2008/EC). The main objective of the Safer Internet action plans, according to the European Commission, was to promote and facilitate a safer environment for the development of the internet industry, as well as fighting illegal and harmful content. These were done in three main ways: one, creating a European network of hotlines and encouraging industry self-regulation and codes of conduct; two, producing **filtering** tools and rating systems; and three, raising awareness by educating citizens on how to use the internet in a safe way. The implicit aim of these programs was to train people to become efficient consumer subjects.

As the previous sections showed, part of the education program was through an individualizing design, promoted as 'personalization', and these education programs continue this project. The European Commission argued that it was desirable for people to be identified because although they are entitled to freedom of expression, people need to be accountable for their actions. Therefore, they need to be 'legally traceable' and this should be part of the European Code of Conduct. As with consent, which carried the liability onto individuals, here again it was important to train people to this role and the responsibility it carries with it. But people also need to be economically traceable to be tradable.

The European Commission argues that there needs to be a balance between the legitimate need for people to sometimes be anonymous, together with the need for them to be legally traceable. This reaffirms that the EU and media practitioners should be able to conduct processed listening to people's behavior across the web for similar reasons. This justification gave them **license** to redraw the boundaries of people's bodies. While the EU wants to be able to identify possible criminals and other problematic citizens, copyright holders want to catch

people who pirate their material, and other technology companies want to create profiles that are linked to specific individuals across the web. This prescribes limited ways of using the web that benefit authorities and commercial companies to link people to their 'offline' and 'online' identities (a strategy that Facebook will continue, as will be shown in the next chapter).

On January 25, 1999, the European Parliament approved the decision (276/1999/EC) to adopt a Multiannual Community Action Plan to promote safer use of the internet by combating illegal and harmful content on global networks. The program was set to run between 1999 and 2004. This Act promoted industry self-regulation, to create a frictionless competitive environment for the industry. As with the 'control' slogan, 'safety' was used here to maintain the digital industries' stability and carry on the same benefits these yielded offline into the online territory. People's safety was sold as 'awareness' of the things they should care about and categorize as deviant, spam, or noise.

The Safer Internet Plus Program was approved on May 11, 2005 and ran until 2008. This program stretched the scope of illegal and harmful content and included unwanted content by end-users, including unsolicited communications. This action plan was not so different from the previous one. One of the objectives of this program was "stimulating consensus and self-regulation on issues such as quality rating of websites, cross-media content rating, rating and filtering techniques, extending them to new forms of content such as online games and new forms of access such as mobile phones" (854/2005/EC). This was an attempt to map and categorize the EU online territory in a consistent way, but since most of the categorization was delegated to commercial actors, it made the online EU territory business friendly. One of the changes here, at least in terms of 'action 4—awareness raising', was that:

> Awareness-raising actions should address a range of categories of illegal, unwanted and harmful content (including, for example, content considered unsuitable for children and racist and xenophobic content) and, where appropriate, take into account related issues of consumer protection, data protection and information and network security (viruses/spam). (854/2005/EC)

Here, there is an attempt to go beyond merely illegal content, but it is not clear in what ways. Again, flexibility and ambiguity are powerful strategies for commercial companies to insert their own meanings, catering for their business models.

Although the European Commission emphasized the need to address issues of data protection and mention the e-Privacy Directive, the organization did not

offer any education regarding other options of behavior online, such as anonymity and encryption. This is contrary to the A29WP document on privacy on the internet from 2000, which concludes that "It is necessary to provide anonymous access to Internet to users surfing or searching in the Net" (A29WP, 2000a: 53). The organization also makes the recommendation to "produce privacy-compliant browsers with the most privacy-friendly default settings [and] anonymous proxy servers [that] can hide the IP address and could be offered as a free standard feature with an Internet subscription by every ISP" (ibid: 86). Such options of 'living' in the online EU territory, which promoted privacy, anonymity, and encryption, were not mentioned in the awareness, education and industry-led initiatives offered. These education programs then, promoted a design for digital bodies which could not be listened to, in order to draw a clear boundary between the front and back end.

The Safer Internet Community Program (1351/2008/EC) was approved on December 16, 2008, and ran between 2009 and 2013. Unwanted content was no longer part of this action plan's concerns and it was replaced by a new issue: harmful conduct, meaning practices such as grooming and cyber-bullying. These joined the two other issues that appeared from the start of the action plan: illegal and harmful content. This action plan was exclusively addressed towards children's internet use and ways of protecting them. Another new addition to this program was the establishment of a knowledge database that provided the means for:

> [M]aking measures to promote a safe and responsible use of the Internet, further developing supporting technologies, promoting best practices for codes of conduct embodying generally agreed standards of behavior and cooperating with industry on the agreed objectives of those codes. (1351/2008/EC)

Part of creating such a database involved collecting statistics and analyzing 'trends' happening in member states: "The knowledge base that can be used for designing efficient actions needs to be strengthened in order to better understand these changes" (EC, 2008: 2). Statistical analyses of societal behaviors were collected; however, as the document indicates the content of such data was 'only' shared with 'stakeholders' (EC, 2008: 8). This means that another sonic epistemological instrument to listen (statistically **measure**) to people's behaviors online was developed, whereby the results and what was done with them was unknown to citizens and only shared with commercial actors. Although the safer internet programs were meant to be an educational program to help reduce spam, there was no information on what this actually meant.

Options of living on the EU internet have been gradually delegated to commercial companies under the European Commission's soft law approach since 1996, three years after the mass release of the first web browser. Framed as a 'safer internet', the European Commission's action plan was meant to ensure that use of the internet was safer for the market, including the old (copyright holders and the Commission itself) and new players (ISPs, telecoms operators, publishers, advertisers and, other tech companies). People were educated to behave within the prescribed routes that were paved for them by commercial actors, and yet such design was presented as a 'free choice' to exercise their autonomy and lives online. Importantly, by providing people with limited and controlled listening capacities to monitor illegal content, they were trained to become feedback loop filters that stabilized the EU market.

Conclusion: Brave New Web?

As you have listened throughout this chapter, a lot has happened since the previous chapter. Above all, there is just more of everything—more media companies involved, more technologies, more people, more money, and all these are entangled in many more communication channels which are mostly silent and hidden. In a way, this chapter gives you the short history of a lot of the fucked up situations we are experiencing today; from the Cambridge Analytica scandal, Brexit, online harassment and trolls, mis- and dis-information, 'fake news', content moderators, election frauds and more. This chapter showed the stages that enabled these business models and architectures to be naturalized as the *only* way to experience the web. This is how all these networked phenomena were made possible, mainly by promoting a specific business model for the web. And, as the character of the film *Anchorman*, Ron Burgundy, says—Boy, that escalated quickly.

As with the previous chapter I focused on two main areas that were the focus of media practitioners sonic epistemological strategies—territories and bodies. In the first half of the chapter I illustrated how the digital advertising industry created a new trade territory at the back-end of the web. I showed how the digital advertising industry and tech companies lobbied both the EU legislators and internet standards organizations to institutionalize and legitimize the automated data trade in the back-end. In the second half of the chapter I showed how a new data subject was produced by developing new sonic measuring devices which redraw the line of who and what is human. In addition, these data subjects had to go through educational training to maintain

the safety of commercial companies business models and at the same time to limit, narrow and control their understanding of how the web works and importantly—what they can do in/with it.

The chapter went to the nitty gritty details of how to produce territories and data subject. A lot of these details can be quite boring, long and jargon-laden (whether technical or legal), but this is precisely where the power relations are enacted. It is exactly these nuances that enabled the ad-tech industry to **restructure the online territory** by redrawing false divisions between private and public spaces and then decide what you but importantly *they* can do in each space. The biopolitical flexibility and ambiguity under the European Commission's soft-law approach enabled commercial companies to provide their own definitions according to their business models, then changing and adapting these along the way. These transitions of power gave a **license** to media practitioners to produce the EU trade territory. In this way, it was also possible for advertising associations and browsers to give **licenses** to *themselves* in the shape of self-regulation standards that they were authorised to draft, police and sanction.

A key moment in producing this online territory was creating web browsers default design which sent first and third party cookies to be plugged into people's bodies and communicate their behaviors to multiple actors—all without their knowledge or consent. Although cookies and the automated market that facilitated them through RTB created multiple communication channels and hence a burden on the infrastructure, the adtech industry standardized them to create a trade-friendly territory. The distinction between public and private spaces was paramount to legitimizing cookies as a sonic device that enabled EU citizens' digital bodies to be listened to. In doing so, they produced a rhythmedia that ordered legitimate communication while illegitimizing others. They created noise and presented it as harmonious sound.

While the scope of listening that ad-tech companies could deploy were expanded, people's listening abilities were controlled and narrowed. The lobbying of the advertising industry and the dominance of browsers also meant that, although the 1997 IETF cookie standard recommended people to be able to listen to what is happening in the 'back end' of their bodies, this suggestion did not materialize. People could only access and experience the web in a restricted and narrow way and communicate with their computers and other people without knowing what happened in other layers. The transition from subscription to free content and access by (behavioral) advertising turned people into the currency. But, as with other currencies, there was a need for a unified agreement about people's worth so they could be used, transferred, exchanged and monetized. In order to do that,

the advertising industry needed to standardize new processed listening capacities, which involved **measuring** tools and units.

The adtech industry's measurement standardization project of early 2000s aimed to make rules for the new automated online market. The larger goals were to commodify quantify, compare, transfer, monetize and bid data subjects and then trade them with other advertising companies in the accelerated rhythm territory through cookies. Measuring behaviors had to be accurate, especially in light of the amount of non-human actors such as bots, 'spiders' and routine actions that companies deployed on their services. Only the sound of human behavior counted. In this way, such filtration methods enacted and produced data subject according to assumptions of the normal human rhythm on the web. Any deviation from this was categorized as a bot.

Due to the fact accelerated bulk behaviors were considered to be bots, the adtech industry wanted to **train the digital bodies** of EU citizens to avoid behaving in ways that could confuse measuring. Therefore, they categorized fast, excessive-rhythm actions as spam. **Training digital bodies** was carried out through providing people with control mechanisms. In this way, EU citizens were trained to click 'consent' buttons without knowing what cookies were, how they worked, who were the entities that operated them, and, importantly, the consequences of this communication.

This control strategy was also conducted with another way to limit and manage people's options of living on the web, through education. The less people knew about the back-end and what they could do on the web the more power ad-tech companies had in standardizing these life settings. Discipline came in the shape of **training the body** and educating EU citizens as part of the Safer Internet Action Plans to protect commercial companies business models. As Monika Bulger and Patrick Davison from Data & Society argue, after the aftermath of Cambridge Analytica and the growth of misinformation and fake news—above all, people need to understand the environment they engage with. That means understanding what's the business model behind all these 'free' services:

> Clearly, responsibility for accessing high-quality, reliable information does not rest solely with an individual, but with institutions, technology platforms, and nations, among other actors. Situating media literacy within this complex media and information environment can provide deeper insight into how education and training can be productively leveraged to improve responsible media engagement. (Bulger and Davison, 2018: 18)

These control mechanisms and education programs **trained people's bodies** to understand that they had power and choice by clicking that they 'agree' to a business model where they are the product without their knowledge. Importantly, they carried responsibility of the consequences of every action. The term 'control', here, refers to the control of people's behavior, not to giving them control. Another part of the training was to keep people's bodies 'safe' while actually teaching them how to keep commercial companies safe. Both the terms 'safe' and 'control', then, were used in the context of the EU online territory as a way to produce data subjects and, consequently, provide economic benefit and funding for the web. But as the EFF argues:

> keep in mind that *none of this is your fault*. Privacy shouldn't be a matter of personal responsibility. It's not your job to obsess over the latest technologies that can secretly monitor you, and you shouldn't have to read through a quarter million words of privacy-policy legalese to understand how your phone shares data. Privacy should be a right, not a privilege for the well-educated and those flush with spare time. Everyone deserves to live in a world—online and offline—that respects their privacy (Cyphers, 2019).

Discouraging and making illegal bulk communication was also a way to individualize behaviors and **de-politicise** actions that could be carried out in groups. Similar to the personal experience and service that Bell's operators were encouraged to provide, here personalization as an experience is also the promoted way of living.

As the previous chapter showed, un-crowding parks that were public spaces meant for demonstration was achieved by redesigning their architecture and thus not allowing for collective civic action. This was also done with the telephone operators as Bell did not want them to be able to organise and unionise. When people are obliged to communicate in personalized spaces and not anonymously, it is easier to prevent possible demonstration and revolt through media. This was also why people were not taught how to encrypt and this option of communication was not supported or promoted. This is because technology companies and governments know that when we organize, unionize, act and protest together—we have more power.

To conclude, this chapter showed the development of more communication channels and the introduction of multiple media practitioners that deployed sonic epistemological strategies. Contrary to the previous chapter, in which Bell was the main media company, here there is a decentralization of several power nodes that

expanded their listening capacities. In the next chapter, there is a return to centralization of media power through Facebook—a company which creates a new power structure/balance through its listening capacities.

Notes

1. This metaphor has influenced the way people understand and communicate through this infrastructure of shared computer resources. The cloud metaphor is being criticised by digital rights advocates (usually with the slogan, 'there is no cloud, just other people's computers') who warn of privacy hazards that are involved in such sharing of information between computers that are located in unknown places.
2. Green Papers in the EU 'are documents published by the European Commission to stimulate discussion on given topics at European level' (European Commission, n.d).
3. This approach is contrasted with 'hard law', "legally binding obligations that are precise (or can be made precise through adjudication or the issuance of detailed regulations)" (Abbott and Snidal, 2000: 421).
4. The Interactive Advertising Bureau is a global advertising industry trade association, which was founded in 1996. The association was formed by representatives from companies such as CNET, Microsoft, Time Inc., Juno, and Turner Interactive. Its main goal is to establish standards and practices for the advertising industry. For a good historic background on the IAB, see Gehl (2014: 98).
5. The EASA was founded in 1992 to support and promote the European advertising industry's self-regulation.
6. The International Telecommunication Union (ITU) was founded in Paris in 1865 in its earlier configuration as the International Telegraph Union, and received its current name in 1934. The ITU deals with all ICT-related issues including television and broadcasting, the internet, and technological features such as 3D.
7. The Internet Society (ISoc) is an international non-profit organisation, founded in 1992 by Vint Cerf and Bob Kahn.
8. The Internet Corporation for Assigned Names and Numbers (ICANN) was founded in 1998 by Jon Postel and is a non-for-profit organization responsible for coordinating the Internet Assigned Numbers Authority (IANA) functions.
9. The World Wide Web Consortium (W3C) is an international organization, founded in October 1994 by Tim Berners-Lee. Its mission is to develop standards for the web with different stakeholders.
10. The Internet Engineering Task Force (IETF) was founded in 1986 and is responsible for drafting technical standards for the internet. These standards are not compulsory for adoption, so technology companies are encouraged but not forced to adopt them.
11. The Electronic Frontier Foundation (EFF) was founded in 1990 and "is the leading nonprofit organization defending civil liberties in the digital world" (https://www.eff.org/about).

12. By 'EU internet', I mean the way that people who are geographically located within the EU experience the internet territory. This means that people's experience of the internet is influenced by the Member State in which they live as well as EU legislation in relation to various issues such as copyright, privacy, broadcasting and more.
13. This is usually called the opt-out versus opt-in mechanisms. Opt-out means that people are automatically receiving a form of communication and then have the option to object by indicating they do not wish to receive it anymore, which is usually done by unsubscribing. Opt-in means that people are not automatically receiving a form of communication and they need to indicate whether they want to receive it or not beforehand. The former mechanism is usually more common in US legal discourses, whereas the latter is more common in EU legal discourses.
14. The first documented HTTP protocol was called HTTP V0.9, and produced in 1991 (https://www.w3.org/Protocols/HTTP/AsImplemented.html). The 1996 version mentioned above is the official version published in the IETF RFC 1945.
15. According to Smith, they are 'a graphics on a Web page or in an Email message that is designed to monitor who is reading the Web page or Email message. Web Bugs are often invisible because they are typically only 1-by-1 pixel in size. They are represented as HTML IMG tags' (1999).
16. As the A29WP argue: "As recital 26 of Directive 95/46 specifies, data are qualified as personal data as soon as a link can be established with the identity of the data subject (in this case, the user of the IP address) by the controller or any person using reasonable means. In the case of IP addresses the ISP is always able to make a link between the user identity and the IP addresses and so may be other parties, for instance by making use of available registers of allocated IP addresses or by using other existing technical means" (A29WP, 2002: 3).
17. Some of the arguments that the advertising industry presents is that with dynamic IP addresses (meaning that the address number changes from time to time) it is hard to deduce the profile of people. However, in 2010 the A29WP discarded such claims by observing that "behavioral advertising normally involves the collection of IP addresses and the processing of unique identifiers (through the cookie). The use of such devices with a unique identifier allows the tracking of users of a specific computer even when dynamic IP addresses are used. In other words, such devices enable data subjects to be 'singled out', even if their real names are not known" (A29WP, 2010: 9).
18. This protocol evolved into Transport Layer Security (TLS) during 1999 when the IETF published the first TLS standard (Dierks and Allen, 1999).
19. The exact phrasing was: 'Member States shall prohibit the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user without the prior, explicit consent of the subscriber or user concerned. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network' (Debusseré, 2005: 80).

20. PwC was given the name of the IAB's 'Measurement Task Force'.
21. Although, it took time for people to use computers individually, yet still profiles could be established.
22. These are usually programs that visit other websites to extract different types of information for different uses.
23. A user agent (browser) string is a way for the browser to identify itself.
24. For a good account of the standardization of advertisement sizes, see Gehl (2014: 95–103).
25. During the hearing of Mark Zuckerberg in the US Senate in relation to Facebook's involvement with Cambridge Analytica and the 2016 USA election meddling The CEO did not know how his company works (Sheffield, 2018).

References

Action Plan for a Safer Internet (Decision No 276/1999/EC). Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31999D0276 (Accessed on 22 March 2019).

Andrejevic, M. (2014). Big data, big questions| the big data divide. *International Journal of Communication*, *8*, 1673–1689.

Article 29 Working Party. (1997). Recommendation 3/97 on anonymity on the internet. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1997/wp6_en.pdf (Accessed on 22 March 2019).

Article 29 Working Party. (1999). Recommendation 1/99 on invisible and automatic processing of personal data on the internet performed by software and hardware. Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp17_en.pdf (Accessed on 22 March 2019).

Article 29 Working Party. (2000a). Opinion 7/2000 on the European Commission proposal for a directive of the European Parliament and of the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector. Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp36_en.pdf (Accessed on 22 March 2019).

Article 29 Working Party. (2000b). Privacy on the Internet—An integrated EU approach to online data protection. Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp37_en.pdf (Accessed on 22 March 2019).

Article 29 Working Party. (2002a). Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipments: The example of IPv6. Available at: http://www.eu.ipv6tf.org/PublicDocuments/wp58_en.pdf (Accessed on 22 March 2019).

Article 29 Working Party. (2002b). Document on determining the international application of EU Data Protection law to personal data processing on the internet by non-EU-based web sites. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp56_en.pdf (Accessed on 22 March 2019).

Article 29 Working Party. (2004). Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC. Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp90_en.pdf (Accessed on 22 March 2019).

Article 29 Working Party. (2006). Opinion 2/2006 on privacy issues related to the provision of email screening services. Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp118_en.pdf (Accessed on 22 March 2019).

Article 29 Working Party. (2010). Opinion 2/2010 on online behavioural advertising. Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf (Accessed on 22 March 2019).

Article 29 Working Party. (2011). Opinion 15/2011 on the definition of consent. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf (Accessed on 22 March 2019).

Arvidsson, A. (2006). *Brands: Meaning and value in media culture*. Routledge.

Berners-Lee, T., Fielding, R., & Frystyk, H. (1996). *Hypertext transfer protocol–HTTP/1.0* (No. RFC 1945). IETF. Available at: https://tools.ietf.org/html/rfc1945 (Accessed on 22 March 2019).

Bhat, S., Bevans, M., & Sengupta, S. (2002). Measuring users' web activity to evaluate and enhance advertising effectiveness. *Journal of Advertising*, *31*(3), 97–106.

Bruner, R. E. (1997). Advertisers win one in debate over 'cookies': Netscape move may settle sites concern over controversial targeting tool. *Advertising Age*. Available at: https://adage.com/article/news/interactive-advertisers-win-debate-cookies-netscape-move-settle-sites-concern-controversial-targeting-tool/68270/ (Accessed on 22 March 2019).

Campbell, J. E., & Carlson, M. (2002). Panopticon.com: Online surveillance and the commodification of privacy. *Journal of Broadcasting & Electronic Media*, *46*(4), 586–606.

Commission of the European Communities. (1987). Green paper on the development of the common market for telecommunications services and equipment. Available at: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A51987DC0290 (Accessed on 22 March 2019).

Commission of the European Communities. (1996). Illegal and harmful content on the Internet. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:1996:0487:FIN:en:PDF (Accessed on 22 March 2019).

Council of Europe. (1950). Convention for the protection of human rights and fundamental freedoms. Available at: https://www.echr.coe.int/Documents/Convention_ENG.pdf (Accessed on 22 March 2019).

Cyphers, B. (2019). Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance. EFF. Available at: https://www.eff.org/wp/behind-the-one-way-mirror#Identifiers-on-the-Web (Accessed on 3 December 2019).

Data Protection Directive. (95/46/EC). Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046 (Accessed on 22 March 2019).

Debusseré, F. (2005). The EU E-Privacy Directive: A monstrous attempt to starve the cookie monster? *International Journal of Law and Information Technology*, *13*(1), 70–97.

DeNardis, L. (2007). The history of computer security. In K. De Leeuw & J. Bergstra (Eds.), *The history of information security: A comprehensive handbook* (pp. 681–705). Amsterdam, the Netherlands: Elsevier.

DeNardis, L. (2009). *Protocol politics: The globalization of Internet governance*. Cambridge, MA: MIT Press.

Directive on Privacy and Electronic Communications (e-Privacy). (2002/58/EC). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN (Accessed on 22 March 2019).

Doteveryone. (2018). People, power and technology: The 2018 digital understanding report. Available at: http://understanding.doteveryone.org.uk/ (Accessed on 22 March 2019).

Eurobarometer. (2003). Data protection. Available at http://ec.europa.eu/COMMFrontOffice/PublicOpinion/index.cfm/Survey/getSurveyDetail/yearFrom/1973/yearTo/2003/surveyKy/325 (Accessed on 22 March 2019).

Eurobarometer. (2008). Data protection in the European Union citizens' perceptions analytical report. Available at http://ec.europa.eu/COMMFrontOffice/PublicOpinion/index.cfm/Survey/getSurveyDetail/yearFrom/2008/yearTo/2009/surveyKy/667/p/2 (Accessed on 22 March 2019).

Eurobarometer—INRA. (1997). Information technology and data privacy. Available at http://ec.europa.eu/COMMFrontOffice/PublicOpinion/index.cfm/Survey/getSurveyDetail/yearFrom/1973/yearTo/1997/surveyKy/164 (Accessed on 22 March 2019).

European Advertising Standards Alliance (EASA). (2002). The EASA statement of common principles and operating standards of best practice. Available at: http://www.easa-alliance.org/sites/default/files/EASA%20Common%20Principles%20and%20Operating%20Standards%20of%20Best%20Practice.pdf (Accessed on 22 March 2019).

European Advertising Standards Alliance (EASA). (2004a). The EASA best practice self-regulatory model. Available at: http://www.easa-alliance.org/sites/default/files/EASA%20Best%20Practice%20Self-Regulatory%20Model.pdf (Accessed on 22 March 2019).

European Advertising Standards Alliance (EASA). (2004b). Advertising self-regulation charter. Available at: http://easa-alliance.org/about-easa/charter (Accessed on 22 March 2019).

European Commission. (n.d.). Green papers. Available at https://eur-lex.europa.eu/summary/glossary/green_paper.html (Accessed on 22 March 2019).

European Commission. (2001). Unsolicited commercial communications and data protection. Available at http://ec.europa.eu/justice/data-protection/document/studies/files/20010202_spamstudy_en.pdf (Accessed on 22 March 2019).

European Commission. (2004). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on unsolicited commercial communications or 'spam'. Available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52004DC0028&from=EN (Accessed on 22 March 2019).

Federation of European Direct Marketing. (2010). European code of practice for the use of personal data in direct marketing. Available at: http://www.amd.pt/fedma.pdf (Accessed on 22 March 2019).

Franklin, M. I. (2013). *Digital dilemmas: Power, resistance, and the internet*. Oxford, UK: Oxford University Press.

Fung, B. (2016). The British are frantically Googling what the E.U. is, hours after voting to leave it. *The Washington Post*. Available at: https://www.washingtonpost.com/news/the-switch/

wp/2016/06/24/the-british-are-frantically-googling-what-the-eu-is-hours-after-voting-to-leave-it/?utm_term=.2553152787e7 (Accessed on 22 March 2019).

Gehl, R. W. (2011). The archive and the processor: The internal logic of Web 2.0. *New Media & Society*, *13*(8), 1228–1244.

Gehl, R. W. (2014). *Reverse engineering social media*. Philadelphia, PA: Temple University Press.

Goldberg, M. A. (2005). The Googling of Online Privacy: Gmail, Search-Engine Histories and the New Frontier of Protecting Private Information on the Web. *Lewis & Clark L. Rev.*, *9*, 249.

Goodman, J. W. (2006). *Telecommunications policy-making in the European Union*. Cheltenham, UK: Edward Elgar.

Haigh, T. (2008). Protocols for Profit. Web and E-mail Technologies as Product and Infrastructure. *The internet and American business*, 105–158.

Hern, A. (2015). I read all the small print on the internet and it made me want to die. *The Guardian*. Available at: https://www.theguardian.com/technology/2015/jun/15/i-read-all-the-small-print-on-the-internet (Accessed on 22 March 2019).

ICO. (2019). Update report into adtech and real time bidding. Available at: https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf (Accessed on 2 November 2019).

Interactive Advertising Bureau. (2004). Interactive audience measurement and advertising campaign reporting and audit guidelines. Available at: http://www.iab.com/wp-content/uploads/2015/06/Ad-Impression-Measurment-Guideline-US.pdf (Accessed on 22 March 2019).

Interactive Advertising Bureau. (2009). Social media Ad metrics definitions. Available at: http://www.iab.net/media/file/SocialMediaMetricsDefinitionsFinal.pdf (Accessed on 22 March 2019).

Internet Advertising Bureau UK. (2005). The guide to display advertising. Available at: http://www.iabuk.net/sites/default/files/IABGuidetoDisplayAdvertising.pdf (Accessed on 22 March 2019).

Interactive Advertising Bureau. (2012). OpenRTB API Specification Version 2.0. Available at: https://www.iab.com/wp-content/uploads/2015/06/OpenRTB_API_Specification_Version2_0_FINAL.pdf (Accessed on 30 October 2019).

Interactive Advertising Bureau. (2017). OpenRTB 3.0 Framework Launching Secure Supply Chain Standards. Available at: https://iabtechlab.com/wp-content/uploads/2017/09/OpenRTB-3.0-Draft-Framework-for-Public-Comment.pdf (Accessed on 30 October 2019).

Kazansky, B. (2015). FCJ-195 privacy, responsibility, and human rights activism. *The Fibreculture Journal*, (26 2015: Entanglements–Activism and Technology). Available at: http://twentysix.fibreculturejournal.org/fcj-195-privacy-responsibility-and-human-rights-activism/ (Accessed on 22 September 2019).

Kierkgaard, S. M. (2005). How the cookies (almost) crumbled: Privacy & lobbyism. *Computer Law & Security Review*, *21*(4), 310–322.

Kristol, D., & Montulli, L. (1997). IETF RFC 2109: HTTP state management mechanism. Available at: https://www.ietf.org/rfc/rfc2109.txt (Accessed on 22 March 2019).

Kristol, D., & Montulli, L. (2000). IETF RFC 2965: HTTP state management mechanism. Available at: https://www.ietf.org/rfc/rfc2965.txt (Accessed on 22 March 2019).

Lessig, L. (1999). *Code: And other laws of cyberspace*. New York, NY: Basic Books.

Lindberg, G. (1999). RFC 2505: Anti-spam recommendations for SMTP MTAs. *IETF*. Available at: https://tools.ietf.org/html/rfc2505 (Accessed on 22 March 2019).

Lovink, G. (2011). *Networks without a cause: A critique of social media*. Cambridge, UK: Polity Press.

Manovich, L. (2001). *The language of new media*. Cambridge, MA: MIT Press.

Mayer, J. R., & Mitchell, J. C. (2012). Third-party web tracking: Policy and technology. In *Security and Privacy (SP), 2012 IEEE Symposium on* (pp. 413–427). Washington, DC: IEEE.

McStay, A. (2013). I consent: An analysis of the cookie directive and its implications for UK behavioral advertising. *New Media & Society*, *15*(4), 596–611.

Novak, T. P., & Hoffman, D. L. (1997). New metrics for new media: Toward the development of web measurement standards. *World Wide Web Journal*, *2*(1), 213–246.

Organisation for Economic Co-operation and Development Task Force on Spam. (2005). Anti-spam regulation. Available at http://www.oecd.org/sti/ieconomy/35670414.pdf (Accessed on 22 March 2019).

Organisation for Economic Co-operation and Development Task Force on Spam. (2006) Report of the OECD Task Force on spam: Anti-spam toolkit of recommended policies and measures. Available at http://www.oecd.org/sti/consumer/36494147.pdf (Accessed on 22 March 2019).

Postel, J. (1980). DOD standard internet protocol. *IETF*. Available at: https://tools.ietf.org/html/rfc760 (Accessed on 22 March 2019).

PriceWaterhouseCoopers (PwC). (2001). *IAB online Ad measurement study*. Interactive Advertising Bureau. Available at: https://www.yumpu.com/en/document/view/21816360/pwc-iab-online-ad-measurement-study-report (Accessed on 22 March 2019).

Reuters. (2001). Europe goes after the cookie. *Wired*. Available at: https://www.wired.com/2001/10/europe-goes-after-the-cookie/ (Accessed on 22 March 2019).

Safer Internet Programme. (Decision No 854/2005/EC). Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32005D0854 (Accessed on 22 March 2019).

Sarikakis, K. (2004). Ideology and policy: Notes on the shaping of the Internet. *First Monday*, *9*(8). Available at: http://firstmonday.org/ojs/index.php/fm/article/view/1167 (Accessed on 22 March 2019).

Schwartz, J. (2001). Giving the web a memory cost its users privacy. *New York Times*. Available at: https://www.nytimes.com/2001/09/04/business/giving-web-a-memory-cost-its-users-privacy.html (Accessed on 22 March 2019).

Senden, L. A. (2005). Soft law, self-regulation and co-regulation in European law: where do they meet? *Electronic Journal of Comparative Law*, *9*(1).

Shah, R. C., & Kesan, J. P. (2009). Recipes for cookies: how institutions shape communication technologies. *New Media & Society*, *11*(3), 315–336.

Smit, E. G., Van Noort, G., & Voorveld, H. A. (2014). Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. *Computers in Human Behavior*, *32*, 15–22.

Smith, R. M. (1999). The Web Bug FAQ. *EFF*.

Spamhaus. (n.d.). Definitions. Available at: https://www.spamhaus.org/consumer/definition/ / (Accessed on 22 March 2019).

Supper, A. & Bijsterveld, K. (2015). Sounds Convincing: Modes of Listening and Sonic Skills in Knowledge Making. *Interdisciplinary Science Reviews*, *40*(2), 124–144.

Tene, O., & Polenetsky, J. (2012). To track or do not track: Advancing transparency and individual control in online behavioral advertising. *Minnesota Journal of Law, Science & Technology*, *13*, 281–357.

European Commission. (Decision 1351/2008/EC). The Safer Internet Community Programme. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008D1351 (Accessed on 22 March 2019).

Turow, J. (2012). *The daily you: How the new advertising industry is defining your identity and your worth*. New Haven, CT: Yale University Press.