Technology and Regulation

The Impacts of AdTech on Privacy Rights and the Rule of Law

Róisín Áine Costello*

AdTech, rule of law, autonomy, privacy, data protection

costelr@tcd.ie

This article argues that the AdTech market has undermined the fundamental right to privacy in the European Union and that current legislative and fundamental rights protections in the EU have been unsuccessful in restraining these privacy harms. The article further argues that these privacy consequences have imported additional reductions in individual autonomy and have the capacity to harm the Rule of Law.

"Although we feel unknown ignored
As unrecorded blanks
Take heart! Our vital selves are stored
In giant data banks" [1]

1. Introduction

Sarah Igo has speculated that the collision, or collusion, between the disclosure of personal data and the technological capacity to capture, analyse, and harness this data will be the defining feature of the twenty first century privacy landscape. While this tension between what can be known and what should be concealed is an enduring one, individuals' ability to exercise control over the boundaries of their private experience has, in the last decade, receded rather than being augmented by technological advances.[2]

This article argues that the online AdTech market, as currently constituted, has been central to this recession, and has undermined the fundamental right to privacy as it is protected in the European Union.[3] In particular, the article establishes that online markets for personal data are specifically orientated to enable large scale collection of personal data in circumstances where individuals have a limited understanding of the ways in which that information will be used, and offers no functional choice to consumers in seeking to access goods or services which do not operate such data collection practices.

1 Felicia Lamport, 'Deprivacy' *Look Magazine* (1970).
2 Sarah E Igo, *The Known Citizen: A History of Privacy in Modern America* (Harvard University Press 2018), 353.
3 Regulation (EU) 2016/679 (henceforth GDPR).

* Trinity College Dublin, School of Law.
Received 10 Sept 2019, Accepted 23 Mar 2020, Published: 14 Apr 2020

The negative privacy impacts which flow from the large-scale collection of personal data in the AdTech market are also harmful to individual autonomy - and cumulatively harmful to the Rule of Law through the diminution of individual liberty and the associated participatory capacity of individuals to engage in the democratic process. In this respect the article argues that the right to privacy is an essential component of the substantive or 'thick' conception of the Rule of Law endorsed by the Union in as much as it acts as an effective restraint on State overreach and secures a constitutionally mandated zone of individual autonomy.

The article argues that the legislative measures taken by the European Union to combat the development of the AdTech market, while motivated by the ostensible aim of securing fundamental rights, have in fact created a hierarchy in which data protection as a market-orientated right has been elevated above the socially oriented right of privacy.

As part of this development, the contractual practices which enable the AdTech landscape have proliferated largely unopposed on the understanding, only recently challenged, that they satisfy the threshold notice and information requirements required by data protection. Meanwhile, there has been a marked failure to engage in a substantive manner with the normative harms to individual privacy which may subsist alongside the satisfaction of a market orientated vision of data protection.

The article begins, in section two, with an explanation of the operation of the AdTech market and its impacts on individuals' lives before moving in section three to examine the legal landscape in which AdTech operates. Section four then examines how AdTech fits within the legal framework based on Article 8 CFR before moving, in section five, to examine how the right to privacy is impacted by the current legal and practical schema. Finally, in section six, the article expands its examination to consider how AdTech implicates negative harms

not only for privacy but also for autonomy and the rule of law.

2. What is AdTech and How Does It Impact Our Lives

The capacity, and desire, to track consumers is not new. Laurence Fontaine in a study of the notebooks of pedlars working in Europe during the fifteenth through eighteenth centuries documented the extensive, personalised notes they kept not only on their customers but on the relatives of those customers (who would expect similar deals) and the demeanour and the standing of those individuals in their communities.[4] Contemporaneously, sellers have engaged in similar attempts to measure and categorise customers and order patterns – first with simple mechanisms like turnstiles[5] and later through more sophisticated methods such as barcoding.[6]

In this context, criticism of AdTech has been dismissed on the basis that AdTech is merely the most recent evolution in a long-standing market practice of consumer surveillance, whose negative impacts are proportionate to the market efficiencies and thus individual benefits they afford.[7] Yet this is not necessarily the case[8] and a historic overview of consumer surveillance indicates that even in the context of less sophisticated, contextual, [9] consumer surveillance mechanisms, concerns abounded about the individual privacy impacts of such activity.[10]

As advertising markets moved online, such concern diminished, driven not by a reduced concern but by a market design which effectively shielded the surveillance mechanisms of the digital market from consumer scrutiny. Indeed, digital advertising networks like DoubleClick (now a subsidiary of Google) recognised the potential of the internet early on and began developing mechanisms for aggregating large and detailed consumer data sets to assess and map consumer behaviour.

The emergence of this AdTech landscape was enabled, to a significant extent, by the development of the computer cookie in 1993[11] and the subsequent move from contextual and towards behavioural advertising in the AdTech market a move which shifted activity towards the collection and aggregation of consumer data on a large scale and its deployment in a targeted, predictive manner to influence consumer behaviour and attitudes.[12]

2.1 Cookies

Cookies are small text files which are placed on a consumer's hard drive by websites which the user visits and which are accessible only to the consumer and the company or actor who placed them. [13] Cookies allow those placing them to track consumer activity on the website to which the cookie relates (through the use of first party cookies) but can also allow those placing them to track consumer behaviour across the web (through the use of analytics cookies). Crucially, cookies do not operate in a vacuum but can be linked to personally identifiable information such as a name or e-mail address provided to access a platform or service thus enabling the actor who placed the cookie to store that consumer's information so that even where a consumer deletes a cookie if they subsequently visit the site again their previous information can be re-associated with them.[14]

While this alone seems harmful to privacy, in practice analytics services and the analytics cookies on which such services rely are predominantly offered by Google and Facebook with the result that such cookies effectively operate as third-party cookies. Third party cookies are placed on consumer devices, as the name would suggest, by third parties who contract with numerous websites to learn what consumers do on sites across the web.[15]

By offering such analytics services these actors can negotiate further cookie placement agreements with hundreds or thousands of companies thus generating a substantive profile of online activity, personal characteristics and behaviours of individual consumers in an attempt to map their preferences and subsequently to target advertising to influence their preferences or choices.[16]

Currently Google and Facebook take some 65% and 90% of total digital advertising spends respectively and 20% of all advertising spends globally.[17] On Google's part this has been enabled in part by the company's acquisition of DoubleClick (now part of the Google Marketing Platform) whose cookies are found on an estimated 87% of websites.[18] Google's own databases - independent of DoubleClick prior to its absorption into the Platform include information about consumer behaviour across Google's services including the location, time and date a device is turned on, an individual's search history[19] and, controversially, the contents of communications sent via Gmail.[20]

4 Laurence Fontaine, *History of Pedlars in Europe* (Duke University Press 1996), 8 et seq.
5 Joseph Turow, *The Aisles have Eyes: How Retailers Track your Shopping, Strip your Privacy and Define your Power* (Yale University Press 2017), 114.
6 Turow (n 5) 80-81.
7 See, Reuben Binns, Zhao Jun, Max Van Kleek and Nigel Shadbolt, 'Measuring third party tracker power across web and mobile' (2010) 9 *ACM Computer Entertainment* 39; Paul Bernal, *Internet Privacy Rights* (Cambridge University Press 2014); Lilian Edwards and Geraint Howells, 'Anonymity, Consumers and the Internet: Where Everyone Knows You're a Dog' in JEJ Prins and MJM van Dellen C Nicoll (eds), *Digital Anonymity and the Law* (Asser Press 2003).
8 Leigh Gallagher, 'Ad tech has a problem. Fixing it isn't easy' (*Fortune*, 14 July 2015) https://fortune.com/2015/07/14/ad-tech-problems/ (accessed 4 March 2019).
9 On contextual advertising generally see, Kaifu Zhang and Zsolt Katona, 'Contextual Advertising' (2012) 31 *Marketing Science* 873.
10 Turow (n 5) 116.
11 On the history and development of cookies see, Rajiv C Shah and Jay P Kesan, 'Deconstructing Code' (2004) *Yale Journal of Law and Technology* 278.
12 See, Bernal (n 7) 144.
13 Lilian Edwards, 'Data Protection and e-Privacy: From Spam and Cookies to Big Data, Machine Learning and Profiling' in Lilian Edwards (ed), *Law, Policy and the Internet* (Hart 2018) 119, 126-7.
14 Turow (n 5) 92.
15 DoubleClick is the market leader in third party advertising. See, Edwards and Howells (n 7).
16 Joseph Turow, *The Daily You: How the new Advertising Industry is Defining your Identity and your Worth* (Yale University Press 2011), 34-64.
17 Matthew Ingram, 'How Google and Facebook Have Taken Over the Digital Ad Industry' (*Fortune*, 4 January 2017) https://fortune.com/2017/01/04/google-facebook-ad-industry/ (accessed 4 March 2019).
18 Lucas Graves and Rasmus Kleis Nielsen Tim Libert, Changes in Third-Party Content on European News Websites after GDPR, 2018, https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2018-08/Changes%20in%20Third-Party%20Content%20on%20European%20News%20Websites%20after%20GDPR_0_0.pdf (last accessed 10 April 2020).
19 Julian Angwin, 'Google has Quietly Dropped Ban on Personally Identifiable Web Tracking' (*ProPublica*, 21 Aoct. 2016) https://www.propublica.org/article/google-has-quietly-dropped-ban-on-personally-identifiable-web-tracking (accessed 25 February 2019).
20 John D McKinnon and Douglas MacMillan, 'Google Says It Continues to Allow Apps to Scan Data From Gmail Accounts' (*The Wall Street Journal*, 20 Sept 2018) https://www.wsj.com/articles/google-says-it-continues-to-allow-apps-to-scan-data-from-gmail-accounts-1537459989 (accessed 4 March 2019).

The data gathered by Google in relation to its own service offerings, is collected on the basis of user consent when consumers accede to the terms of service and privacy policy attached to the relevant offering. The aggregation of both the data which Google collects through its analytics services and through its own services permits the company to build a detailed data sets for a broad swathe of online users. From this the individual characteristics and preferences of consumers can be analysed or inferred – and detailed profiles of individual consumers can be sold through DoubleClick or aggregated with further information obtained through that platform.

Similarly, Facebook's terms of service and privacy policy require users to consent to the collection, recording and potential sale of the data related to their posts, photos, shared items, group and page memberships, location and installed apps. Facebook has, in the past, also granted its advertising customers access exceeding what was contractually permissible under these terms and policies, including accessing the names of Facebook users' friends and the contents of 'private' messages without the consent of users. [21] Like Google, Facebook can combine this information with the information it obtains through its analytics services to build complex and detailed profiles for sale through the AdTech market.

Many websites may incorporate a Facebook Pixel for analytics purposes, a small piece of code which monitors consumer activity[22] even where consumers are not logged on to Facebook or are not Facebook users (a group Facebook has, rather ominously, dubbed 'non-registered users'[23]) across websites and platforms that contain a Facebook pixel or social plugin.[24]

Facebook's contribution to the erosion of consumer privacy is thus enabled not only through these contractually permitted policies (and their breach) but through these analytics services offered by the pixel. It is also enabled by Facebook's embedded social plugins- the buttons which invite visitors to a website to 'like' or 'share' items or pages online. Where these buttons appear, regardless of whether a consumer interacts with them, Facebook is collecting data related to their activity on that site.

In light of their integrated collection and analysis capabilities, Google and Facebook have become 'triple threats' – offering analytics services to other websites, collecting and aggregating large amounts of data through their own platforms and benefitting from the highly targeted profiles of consumers which they can build and auction to advertisers as a result – part of a broader model which Shoshanna Zuboff has called 'surveillance capitalism'[25] and Danielle Citron and Frank Pasquale have referred to as a central part of the 'scored society.'[26] This threat is only amplified by the further integration of these platforms with other services[27] a pattern noted by Binns et al as part of which consumers sign up or interact with other services by authenticating themselves through their Facebook or Google profiles.[28] The consumer profiles on which Facebook and Google as well as other actors in the AdTech marketplace operate are then sold for use in targeted, behavioural advertising through the real time bidding (RTB) system.

2.2 The Real Time Bidding System (RTB)

When a consumer visits a website, they are shown advertising which is targeted to them based on data gathered and aggregated by data brokers (a group which includes actors like Facebook and Google). The process of a consumer's data being broadcast, advertisers bidding for the attention of that consumer based on their data and the advertiser's ad appearing on the website being viewed by the consumer takes places in milliseconds. During this period the consumer's data is broadcast to an undefined number of advertisers who bid for the available advertising space and the consumer's attention.

This auction system is part of the 'real time bidding' (RTB) mechanism which fuels the AdTech market and operates through one of two markets. The first is Open real time bidding (Open RTB), which is used by a majority of online media providers and advertising industry participants.[29] The second, is Google's proprietary RTB "Authorized Buyers" (AB) system.[30]

The information which is sent to bidders in the auctions (using either system) is referred to as bid request data and can include; the content which the consumer is viewing, their location and a description of the device they are using to access the internet, their unique tracking identities (cookies) as well as their IP address. It may also include additional, enhanced data provided by a data broker based on an analysis and aggregation of other data and which may include the consumers income bracket, age and gender, ethnicity, sexual orientation, religion and political persuasions.

More concerningly, and as highlighted in recent complaints filed with the Irish Data Protection Commissioner[31] and UK's Information

21 Michael LaForgia and Gabriel JX Dance Nicholas Confessore, 'Facebook Failed to Police How Its Partners Handled User Data' (*The New York Times*, 12 Nov 2018) https://www.nytimes.com/2018/11/12/technology/facebook-data-privacy-users.html (accessed 4 March 2019).

22 Facebook pixel is similarly to a cookie, a code for websites which allows websites to measure and analyse their audience. See, https://www.facebook.com/business/learn/facebook-ads-pixel.

23 Günes, Acar, Brendan Van Alsenoy, Frank Piessens, Claudia Diaz, Bart Preneel, Facebook Tracking Through Social Plug-ins, Technical report prepared for the Belgian Privacy Commission 2015.

24 In Case C-40/17 *FashionID* EU:C:2019:629, [3], [23] that case the CJEU was asked to consider the integration of social plug-ins, and in particular whether the Facebook 'Like' plug-in on an online retailer's website which transferred the user's IP address and browsing string to Facebook regardless of whether user was a Facebook user or had clicked the like button rendered the appellant a joint data controller for the purposes of the GDPR. In his Opinion, Advocate General Bobek found that, having embedded plug-in in its website resulted in FashionID being considered a joint controller of the data collected though its responsibility should be limited to those operations for which it effectively co-decides on the means and purposes of processing legitimate interests and consent a finding with which the subsequent judgment the CJEU concurred. This decision is one of a growing number of a rapidly proliferating set of challenges by European regulatory and judicial bodies to the activity of actors in the AdTech market which is considered in section four.

25 Shoshanna Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Public Affairs 2019).

26 Danielle Keats Citron and Frank Pasquale, 'The Scored Society: Due Process for Automated Predictions' (2014) 89 *Washington Law Review* 1.

27 In the United States for example, Facebook has sought to integrate financial services offered by Chase, Wells Fargo, Citigroup and US Bancorp with its messenger service, Deepa Seetharaman and Anna Maria Andriotis Emily Glazer, 'Facebook to Banks: Give us your data, we'll give you our users' (*Wall Street Journal,* 6 August 2018) https://www.wsj.com/articles/facebook-to-banks-give-us-your-data-well-give-you-our-users-1533564049 (accessed 9 April 2019).

28 Binns et al (n 7). The authors proceed to note the negative competition impacts of such consolidation capabilities

29 See, 'Open Real Time Bidding' at https://www.iab.com/guidelines/real-time-bidding-rtb-project/ (accessed 4 March 2019).

30 Google Ads, 'How Ad Exchange works with Google Ads' https://support.google.com/google-ads/answer/2472739?hl=en (accessed 29 February 2019).

31 See, Brave 'Grounds of Complaint to the Data Protection Commissioner' https://brave.com/DPC-Complaint-Grounds-12-Sept-2018-RAN2018091217315865.pdf (accessed 4 March 2019).

Commissioner's Office,[32] the RTB mechanism does not permit control over the dissemination of personal information once it has been broadcast. The advertising industry has countered these complaints with arguments that it abides by its own self-regulatory standards which comply with relevant EU law, which the proceeding section now turns to consider.

2.3 How AdTech Affects our Lives

Consumers' offline lives are deeply integrated with, and are in many ways, as diverse as their digital experiences.[33] As a result, the capacity to track consumers' online activity (and by implication a certain amount of their related, offline activity) naturally generates concern about the impacts of surveillance on individual privacy and the manipulation which can result from such privacy reductions. This is perhaps best illustrated by way of comparison to comparable offline surveillance.

An individual enters a shop. On entering the shop, their name and postcode are given to the shop owner. A private detective who has been following them since they last visited the shop then also hands the shop owner a list of their previous purchases and movements – the names and addresses of the locations they have gone since their last visit to the shop, the area where they live, the types and prices of the goods and services they view most frequently. From this the shop owner can build a rough picture of the shopper's age, socio-economic status and perhaps political and religious persuasions.

As the shopper moves around the shop they are tracked by cameras which record the aisles they visit, the products they looked at and how long they considered each product. On leaving the shop they are then followed again by the private detective who records where they go and what they purchase or consider purchasing. The shopper stops into a coffee shop to meet some friends and the detective records what they eat and drink, and sits nearby listening to their conversation, he obtains a list of their other friends and the shops they enter and goods they purchase building a detailed profile of the social network of the shopper. At the end of the day the private detective gives this information to the shop owner. The shop owner now has an extensive list of the shopper's social connections, geographic movements, areas of interest and purchases from which more intimate details such as his age, gender, race, sexuality, political and religious preferences and socio-economic status can be inferred.

The shop owner can use this information himself to target the shopper with ads for his products or services, hoping by the power of suggestion to influence his preferences. But the private detective who conducted much of the data gathering and analysis for the shop owner might also take his detailed profile of the shopper and sell it to other shop owners trying to influence the shopper to purchase their goods or use their services, to political actors seeking to influence the shoppers preferences in an upcoming election, or to any number of other actors who will bid for the data in order to be able to influence the shopper.

In the online environment, the AdTech market operates on a similar basis to the shopper and those who surveil him in this example. The privacy harm is, of course, evident. What also becomes clear is the negative consequences this surveillance may have for the activities or choices the shopper feels able to make (given that he is being watched) or which he is aware he can make (given that his attention is being vied for constantly by actors who have purchased large quantities of his personal data). Further still, the real world comparison draws to the fore the authoritarian undercurrent of such pervasive surveillance and its capacity to be exploited not only by commercial but also by State actors to influence the shopper.

In a real world scenario, the shopper would not merely notice but might reasonably object to such practices and choose to conduct their business in a shop which did not employ such mechanisms. However, the equivalent prompts to the presence of such surveillance, and alternatives which avoid it, are not necessarily present or available in the digital environment. Individuals are required if not by social, then frequently by professional necessity to engage with the digital market in ways which offer them little alternative but to consent to privacy policies and terms of use which permit their data to be gathered, aggregated, broadcast and sold as part of the AdTech market.

As the decisions outlined in sections below indicate, there is a growing awareness of and unease concerning the AdTech landscape which enables this surveillance of, and influence over, consumers[34] while, as section four examines, the regulatory mechanisms which are currently present do not fully address the privacy impacts which AdTech imports.

3 The Legal Landscape in which AdTech Operates

The AdTech market as detailed in the previous section has to date been governed by a mix of self-regulatory efforts in the form of the Interactive Advertising Bureau Europe Framework, which governs the Open RTB system, Google's AB Guidelines which govern that company's proprietary advertising market platform and those European rules governing the contractual permissions which enable Google and Facebook (as the examples used in this article) to collect and sell user data to advertisers.

3.1 The Interactive Advertising Bureau Europe Framework

The Open RTB system in Europe is currently subject to the voluntary Framework established by the European branch of the Interactive Advertising Bureau in its 'Europe Transparency & Consent Framework.' The IAB Framework provides an open-source, industry standard which aims to ensure actors in the digital advertising chain comply with the GDPR and ePrivacy Directive when processing, accessing or storing information on consumer devices including cookies, advertising identifiers, device identifiers and other tracking technologies.

The Framework is predicated on the collection of consent from data subjects for all subsequent data sharing to third parties during the Open RTB process[35] yet the Framework anticipates that this broadcasting of personal data to third parties may occur without consent stating,

> A Vendor[36] may choose not to transmit data to another Vendor

32 See, Brave 'Submission to the Information Commissioner' https://brave.com/ICO-Complaint-.pdf (accessed 4 March 2019).

33 Helen Nissenbaum, 'A contextual approach to privacy online' (2011) 140 *Daedelus* 32.

34 Case C-40/17 *FashionID* EU:C:2018:1039; C-673/17 *Planet49* EU:C:2019:246; Case C- 311/18 *Schrems*.

35 See, IAB Europe, 'Europe Transparency & Consent Framework' http://www.iabeurope.eu/tcfdocuments/documents/legal/currenttcfpolicyFINAL.pdf (accessed 4 March 2019).

36 In this context vendors are data brokers and buyers may be other brokers or parties interested in obtaining by purchase or license access to the data collected and analysed by such vendors.

> for any reason, but a Vendor must not transmit data to another Vendor without a justified basis for relying on that Vendor's having a legal basis for processing the personal data.
>
> If a Vendor has or obtains personal data and has no legal basis for the access to and processing of that data, the Vendor should quickly cease collection and storage of the data and refrain from passing the data on to other parties, even if those parties have a legal basis.[37]

Those broadcasting bid data are thus afforded significant discretion in determining whether those to whom they broadcast their data possess a "justified basis for relying on that Vendor's having a legal basis for processing personal data" effectively circumventing the consent basis on which the Framework purports to rely and conditioning the integrity of the system on the presence, and rigour, of the vendor's assessment rather than consent or indeed the other basis for processing enumerated under the GDPR.

Motivated, no doubt, by such criticisms IAB Europe announced in 2018 it was developing a tool, in collaboration with The Media Trust, to determine whether the "consent management platforms" (CMPs) that facilitate this passing of data under the IAB Europe Framework are compliant with the Framework's policies.[38]

However, as the CNIL decision detailed in *Vectaury* (examined below) illustrates, the more fundamental concern is that it appears that such consent management platforms are themselves non-compliant with the GDPR. It is also unclear whether a reformatting of the Framework announced by IAB Europe in early 2019 to comply with GDPR can ameliorate the subsisting difficulties with the RTB system itself which broadcasts data so widely, regardless the GDPR compliance efforts of the Framework (which it should be emphasised is a voluntary standard).

3.2 Google's Authorised Buyers Guideline

Google has, thus far, declined to integrate the IAB Europe Framework into its proprietary market[39] and has instead operated its own parallel system in the Google Authoring Buyer Guideline. Similarly to the IAB Framework, the AB Guideline shifts responsibly for data protection from the data controller to those third parties to whom the data is broadcast, noting that buyers may store identifiers in order to evaluate impressions and bids based on user-data previously obtained.[40] The Guideline also permits all other callout data (with the exception of location data) to be retained by a Buyer after responding to an ad call for up to 18 months, in order to enable forecasting of the availability of inventory.[41]

The Guideline does impose limitations on how Buyers use data obtained during the bidding process but notes only that it is not permissible to use callout data to create user lists or to profile users and prohibits the association of callout data with third parties.[42] However, this ignores the practical reality that bidders for such data, of which Cambridge Analytica is an example, can and do perform a 'sync' that uses personal data obtained through the bidding process to augment existing consumer profiles.[43]

Moreover, and in a similar vein to the control issues identified with the IAB Framework, the Google Guideline provides that where a

> Buyer accesses, uses, or processes personal information made available by Google that directly or indirectly identifies an individual and that originated in the European Economic Area ("Personal Information"), then Buyer will:
>
> - comply with all privacy, data security, and data protection laws, directives, regulations, and rules in any applicable jurisdiction;
> - use or access Personal Information only for purposes consistent with the consent obtained by the individual to whom the Personal Information relates;
> - implement appropriate organizational and technical measures to protect the Personal Information against loss, misuse, and unauthorized or unlawful access, disclosure, alteration and destruction; and
> - provide the same level of protection as is required by the EU-US Privacy Shield Principles.

Buyers will regularly monitor your compliance with this obligation and immediately notify Google in writing if Buyer can no longer meet (or if there is a significant risk that Buyer can no longer meet) this obligation, and in such cases Buyer will either cease processing Personal Information or immediately take other reasonable and appropriate steps to remedy the failure to provide an adequate level of protection.[44]

This suggests that once personal data is transferred to a Buyer, AB has no effective control over its use. The result, as the proceeding section examines is that, the AdTech market as it is currently constituted, is operating in manner at odds with the data protection standards under the GDPR and, more fundamentally, with individual privacy.

3.3 Consumer Protection Regulation of AdTech

The most evident regulatory mechanism for the AdTech market is consumer protection, an area in which the Union enjoys an explicit competence and an established history of legislative intervention in the market. However, while the European Union has traditionally placed a high value on consumer protection, a fact reflected in the Treaty Articles,[45] and the Charter, as well as in secondary law[46] there is currently no consumer protection standards which are applicable to AdTech.

The Consumer Rights Directive,[47] which replaced the Distance Selling[48] and Doorstop Selling Directives[49] establishes requirements for information to be provided in distance contracts,[50] formal require-

37 See, IAB Europe, 'Europe Transparency & Consent Framework' http://www.iabeurope.eu/tcfdocuments/documents/legal/currenttcfpolicyFINAL.pdf, para 14.4, 14.5 (accessed 4 March 2019).
38 See, Media Trust, 'IAB Europe CMP Validator Helps CMPs Align with Transparency and Consent Framework' https://mediatrust.com/media-center/iab-europe-cmp-validator-helps-cmps-align-transparency-consent-framework (accessed 4 March 2019).
39 See, Robin Kurzer, 'IAB Europe to release updated consent framework later this year, Google to sign on' (*MarTech Today*, 12 Feb 2019) https://martechtoday.com/exclusive-iab-europe-to-release-updated-consent-framework-google-to-sign-on-230704 (accessed 4 March 2019).
40 Google Authorised Buyer Guidelines, https://www.google.com/doubleclick/adxbuyer/guidelines.html (accessed 7 March 2019).
41 Ibid.
42 Ibid.
43 Ibid.
44 Ibid.
45 Articles 39, 107 and 169 TFEU.
46 See, Stephen Weatherill, *EU Consumer Law and Policy* (2nd edn, Edward Elgar 2014).
47 Directive 2011/83/EC.
48 Directive 97/7/EC.
49 Directive 85/577/EC.
50 Directive 2011/83/EC, Article 6.

ments for distance consumer contracts[51] and a right of withdrawal but does not offer any mechanisms for the regulation of the AdTech market proper.[52] Similarly, the Unfair Consumer Contracts Directive[53] while it includes requirements that contractual terms are drafted in clear language, intelligible to the ordinary consumer is not directly relevant to AdTech.[54] New legislative measures announced in January 2019 including the Directive regulating the supply of digital content and services similarly fail to address the AdTech market.[55] Provisions governing advertising do appear in the 2006 Directive on Misleading Advertising,[56] and in the Directive on Unfair Commercial Practices[57] and while there is no reason, in principle, why these provisions could not be extended to cover AdTech, decisions considering the application of the Directives have been limited[58] and would, in any case, be restricted to the advertising facilitated by AdTech rather than the system which enables it.

3.4 Data Protection, Privacy and the Regulation of AdTech

In the absence of applicable consumer protection laws, the primary regulatory mechanisms currently applicable to the AdTech market emanate from the Union's data protection legislation. The right to data protection enjoys constitutional footing within the Union's legal schema through Article 16 TFEU as well as Article 8 CFR. From this foundation the Union has developed a comprehensive schema for the enforcement of the right to data protection, first through the Data Protection and e-Privacy Directives and more recently with the GDPR.

Of these legislative measures the ePrivacy Directive (ePD) frequently referred to, misleadingly, as the Union's 'e-Cookie' law, is the most direct regulatory mechanism applicable to the AdTech industry. The Directive requires Member States to ensure that the use of electronic communications networks to store information or to gain access to information stored in terminal equipment is permitted only where the subscriber or user concerned is provided with clear and comprehensive information regarding the purposes of the processing, and is offered the right to refuse same.[59] The Directive thus imposes informational and consent requirements on the operation and placement of cookies on consumer's devices. However, as section four examines, the capacity of the Directive to provide for substantive privacy protections, rather than threshold operational requirements for the technologies which cause privacy reductions, is limited, and in practice the right to refuse cookies has been ineffective, frequently resulting in access to a site or service being denied.

This discrepancy between data protection rights and substantive privacy protections lies at the heart of the Union's legislative mechanisms as they apply to the regulation of AdTech. Despite the proliferation of ostensibly privacy orientated legislation during the last two decades, the Union's legislative product while seemingly indicative of a strong commitment to privacy is, on closer examination, notable for its emphasis on market-oriented threshold regulations in the form of information and notice requirements rather than substantive interventions to protect consumer privacy writ large.[60]

The separation of the right to data protection from its ostensible root in the right to privacy, and the continuing ambiguity in the jurisprudence of the CJEU as to the relationship between the two rights has hardly helped matters.[61] However, it is also a distinct product of the legislative preference within the Union for market oriented rather than socially oriented rights protections. Indeed, Antoinette Rouvroy and Yves Poullet have criticized the recognition of the right to data protection, distinct to the traditional fundamental right to privacy on this basis arguing that such division obscures the essential relationship between the rights and estranges data protection from the fundamental values of human dignity and individual autonomy which should justify its existence through its derivation from a privacy interest.[62]

This concern is well placed. While the right to data protection is understood as derived from the right to privacy in the Union's law, the Recitals to the GDPR emphasise only the trade and market-orientated functions of the right, neglecting the social and normative roots of data protection in privacy and that right's function in securing individual dignity and the development of individual personality.[63]

The e-Privacy Directive similarly emphasises in its Recitals the market-based functions of its provisions and while the proposed e-Privacy Regulation includes wording in its explanatory memorandum which makes explicit reference to the right to privacy under Article 7 as distinct from the right to data protection, the Recitals to the Regulation refer to data protection and privacy interchangeably. Moreover, the substance of its guarantees relate largely to interoperability, and digital infrastructures as part of the digital single market with little concern for deeper normative impacts. [64] As such, the provisions of the e-Privacy Regulation appear, in fact, to be a mere extension of the GDPR's focus on market oriented data protection in a differentiated context.

This legislative prioritisation of data protection over privacy is particularly problematic in the context of AdTech. Data protection on a close doctrinal analysis could be considered not to be a right as much as a series of mandatory safeguards which must be present in order to legally infringe privacy rights proper. The GDPR and e-Privacy Directive are thus not so much rights standards in themselves but the enabling frameworks for permissible reductions in rights to individual privacy.

While this is not objectionable *per se*, the use of rights language obfuscates the relationship between data protection and privacy while the promotion of data protection over privacy exposes the alienation of data protection from the justificatory basis of privacy and its ideological foundations in individual autonomy. In practice, the result has been that the contractual practices which form a crucial part of the AdTech landscape have proliferated largely unopposed on the basis that they satisfy current data protection requirements without

51 Ibid, Article 8.
52 Ibid, Article 9-16.
53 Directive 93/13 [1993] OJ L095/29.
54 Ibid, Article 5. Ambiguity in relation to the meaning will be resolved in favour of the consumer under this provision.
55 Council of the European Union, Council and Parliament agree on new rules for contracts for the sales of goods and digital content (2019).
56 Directive 2006/114 [2006] OJ L376/21.
57 Directive 2005/29/EC.
58 Case C-281/12 *Trento Sviluppo* EU:C:2013:859; Case C-122/10 *Ving Sverige* EU:C:2011:299; Case C-428/11 *Purely Creative* EU:C:2012:651.
59 Article 5; Acar (n 23).
60 Gloria Gonzalez Fuster, *The Emergence of Personal Data Protection as a Fundamental Rights of the EU*, vol 16 (Law, Governance and Technology Series, Springer 2014), 243-5.
61 On this see, Juliane Kokott and Christoph Sobotta, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2013) 3 *International Data Privacy Law* 1.
62 Antoinette Rouvroy and Yves Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in Yves Poullet Serge Gutwirth, Paul De Hert, Cécile de Terwangne andSjaak Nouwt (ed), *Reinventing Data Protection?* (Springer 2009).
63 Recitals 2, 3.
64 Recital 1, 20 – 24.

reference to the deeper impacts which they occasion for privacy.

Cumulatively, this reduction of individual privacy leads in turn to the creation of a population whose preferences and proclivities can be exploited to influence not only individual preferences but also political opinions importing negative consequences for democratic participation, and in turn the Rule of Law. However, before these broader impacts are examined, it is necessary to consider how the current AdTech landscape is accommodated within the current Article 8 framework and the specific shortcomings of the Union's data protection legislation in regulating AdTech.

4. How does AdTech fit within the Article 8 Privacy Framework?

In accordance with Article 6 GDPR, processing of personal data is lawful only if and to the extent that at least one of the listed conditions are present, namely that the data subject has given consent for one or more specific purposes or the processing is necessary for; the performance of the contract,[65] compliance with a legal obligation or to protect vital interests of data subject, for performance of a task carried out in the public interest or the purposes of the legitimate interests pursued by the controller or a third party.

Under the Regulation consent is one the primary grounds for lawful processing of personal data, a position emphasised by Article 7 GDPR, which requires data controllers to demonstrate that the data subject has consented. When assessing the legitimacy of consent the Regulation emphasises in Article 4(11) that consent must be a freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she through a statement or by a clear affirmative action signifies agreement to the processing of personal data relating to him or her, a position reaffirmed in Recitals 42 and 43.[66]

That the collection and sale of consumer data by data brokers as part of the RTB process involves the processing of personal data is evident. The question then is whether such collection satisfies the requirements of consent under Article 6(a) GDPR or is permissible under an alternative ground for lawful processing.

4.1 Adequate Consent under Article 6 and Article 4(11) GDPR

The operation of the RTB system, and the voluntary self-regulatory structures which seek to provide a governance structure for it, ostensibly operate on the basis of consent. However, it is not clear that the IAB Framework or Google AB Guidelines satisfy the GDPR's definition of consent, as the *Vectaury*[67] decision of the French Commission Nationale de l'informatique et des libertés (CNIL) demonstrates.

In January 2019, the CNIL found *Vectaury*, a French AdTech firm, had collected data to create consumer profiles subsequently auctioned through the RTB system without consent. The decision was significant because it found that the validity of consent obtained directly through apps that embed *Vectaury*'s consent management platform and the validity of consent collected elsewhere and signaled to *Vectaury* through use of the IAB Europe Consent Framework ultimately failed to meet the consent criteria required by the GDPR.

The CNIL found consent obtained through consent management platforms was insufficient because it was not informed, specific or affirmative as required by Recital 32 and Articles 4 and 6 GDPR. Crucially, the decision found that consent obtained through the IAB Europe Framework is inherently invalid as consumer consent cannot be passed from one controller to another controller through a contractual relationship.[68] This, of course has broader implications for the operation of consent based AdTech models more generally. The decision also specifically queried whether, in light of the opacity of the RTB system, consumers could be considered to have given valid consent to a process they did not understand or are unaware of and explicitly stated that its decision should be read as placing not only *Vectaury* but the AdTech ecosystem as a whole on notice that existing market practices may violate the requirements of the GDPR. The decision noted separately that the collection of geolocation data for advertising purposes, by *Vectaury*, presented particular risks as it revealed the movements and habits of consumers and could be used to imply sensitive categories of data.[69]

The decision cogently illustrates the false narrative of consumer consent on which the AdTech industry relies and has implications beyond the IAB Framework. For example, Google has traditionally required publishers to collect consent on its behalf for advertising profiling in a similar manner to the IAB's Framework.[70] While Google have stated they will audit this collection for compliance with consent requirements[71] it is no longer clear that this will be sufficient.

IAB Europe responded to the CNIL judgment stating it merely provides a technical, voluntary standard in accordance with which its members may choose to be but are not required to be bound and suggesting that *Vectaury* had fallen foul of the regulator as it had not adequately adopted and complied with the Framework rather than the error subsisting with the Framework itself.[72] However, this conveniently ignores the central, contractual criticism on which the CNIL decision rests – that there is no refuge in packaged, contractual passing of consent and that consumers have not consented to the use of their data in a broader AdTech ecosystem when they agree to use a service or app.

The CNIL decision also congrues with recent CJEU jurisprudence in *Wirtschaftsakademie*[73] and *Planet49*. In *Wirtschaftsakademie* a preliminary reference from the German Courts asked whether the failure by

65 See also, Recital 44 and Article 7(4) which provides that when assessing whether consent is freely given utmost account shall be taken of whether the performance of a contract, including the provision of a service is conditional on consent to the processing of personal data that isn't necessary for the performance of that contract.

66 Recital 42 requires that processing based on the data subject's consent should be demonstrable by the data processor and in the context of a written consent, safeguards should be put in place to ensure that the data subject is aware of the fact that and the extent to which consent is being given by them. Recital 43 provides that in assessing whether consent has been freely given, consent should not be considered to have been given where there is a clear imbalance between the subject and controller.

67 Commission Nationale de l'informatique et des libertés, 'Décision n°MED-2018-042 du 30 octobre 2018' at https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000037594451&fastReqId=974682228&fastPos=2 (accessed 1 March 2019).

68 Ibid.

69 As defined under Article 9 GDPR.

70 Natasha Lomas, 'Google accused of using GDPR to impose unfair terms on Publishers' (*Tech Crunch*, 1 May 2018) https://techcrunch.com/2018/05/01/google-accused-of-using-gdpr-to-impose-unfair-terms-on-publishers/ (accessed 5 March 2019).

71 Lara O'Reilly, 'Google Wants Publishers to Get Users' Consent on Its Behalf to Comply With EU Privacy Law' (*The Wall Street Journal*, 22 March 2018) https://www.wsj.com/articles/google-wants-publishers-to-get-users-consent-on-its-behalf-to-comply-with-eu-privacy-law-1521749003 (accessed 5 March 2019).

72 Townsend Feehan, The CNIL's *Vectaury* Decision and the IAB Europe Transparency & Consent Framework (2018).

73 Case C-210/16 *Wirtschaftsakademie* EU:C:2018:388.

Facebook and *Wirtschaftsakademie* (the administrator of a fan page on the platform) to inform visitors that cookies were placed on their device by Facebook constituted a breach of the (then) Data Protection Directive. In particular the appellant's asked whether they could be considered a joint controller with Facebook.[74] The Court noted that though Facebook placed the cookies in accordance with its contract with *Wirtschaftsakademie*, the appellant had benefitted from that placement and was involved in the subsequent analysis in as much as it decided the parameters of the information collected based on its interests and was thus a joint controller of the data and required to institute its own system for informing users of the page that cookies were placed on their devices.[75]

The decision in *Planet49* added to this nascent body of precedent. In that case, the CJEU was asked to consider whether online cookie consents with default pre-ticked boxes submitting to the use of cookies was permissible under the GDPR and e-Privacy Directive. In his Opinion in the case, Advocate General Szpunar noted that the requirements of consent under the GDPR include that consent is active, freely given, separate (i.e. not bundled) and informed, requiring the provision of clear and comprehensive information concerning the duration and operation of the cookies and whether third parties have access to the information collected. The AG noted that these conditions were not met where pre-ticked cookie consent boxes were used.[76] The Court agreed noting that the GDPR standard of consent as freely given, specific, informed and unambiguous was not satisfied in such circumstances.

In the context of the AdTech industry the implication of these decisions would seem to be that where a consent management platform, or otherwise delegated or default consent mechanism is used, a third party who benefits from the data collected and analysed is to be considered a data controller and must satisfy the consent thresholds of the GDPR anew. Given the apparent problems posed by a consent-based processing of user data in light of these decisions it is thus necessary to consider whether the legitimate interest ground under Article 5 might offer an alternative means of legitimate processing.

4.2 Legitimate Interests under Article 6 GDPR

As an alternative to consent, under the GDPR personal data may also be processed on the basis of legitimate interests under Article 6(f). Article 6(f) operates in addition to the more general principle of legitimate interests outlined in Article 5 which provides that personal data shall be processed lawfully, fairly and in a transparent manner and collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes. Supplementing Article 6(f), Recital 47 (though non-binding) notes that there should be a relationship between the data controller and data subject on which a legitimate interest is based such as where the data subject is a client, or is in the service, of the data controller. The Recital notes, however, that the existence of a legitimate interest requires careful assessment, including an assessment of the reasonable expectations of the data subject at the time and in the context of the collection of the data.

While this might seem, *prima facie*, to offer a readily available alternative to a consent-based processing in the context of AdTech, any reliance on legitimate interests for the operation of the RTB system would be misplaced. RTB data is broadcast to an undefined list of bidders, who, though they are directed and legally required not to retain or further use such data,[77] are not actively policed by the bid broadcaster to ensure this. Once a bidder is not successful, they no longer have a legitimate interest in processing the data but may retain it. Equally, the data may be received by bidders who have no interest in the segment or consumer data being auctioned but nonetheless receive the data through the RTB system.

The CNIL has previously found that that ticking a box labelled *"I agree to the processing of my information as described above and further explained in the Privacy Policy"* did not satisfy the consent requirements under the GDPR because it attempted to require consent for over one hundred processes and set personalise ads as a default setting.[78] That decision, directed against Google[79] also noted that the processing could not be considered a legitimate interest of the company under Article 6(f) such that consent was not required . The CNIL noted that Google's was particularly intrusive due to the number of services offered by the company, and the quantity and nature of the data processed and combined.

This mirrors the opinion expressed by the Article 29 Working Party that the legitimate interest basis does not cover situations where the processing is not genuinely necessary for the performance of a contract but rather relates to the ancillary use of data and is achieved through terms unilaterally imposed on the data subject. [80] In particular, the Opinion noted that the legitimate interest premise is not a suitable legal basis on which to compile a profile of consumer tastes and choices as the controller has not been contracted to carry out profiling, but rather to deliver particular goods or services and the inclusion of such terms in the contract does not make them necessary for it.[81] This critique is echoed by Frederik Borgesius who notes "the fact that a company sees personal data processing as useful or profitable does not make the processing 'necessary'[82] to provide the contracted service to the user.

4.3 Explicit Consent under Article 9 GDPR

Even where it was possible to establish that processing was permitted on the basis of legitimate interest, under Article 9 GDPR, processing of "special categories" of personal data requires explicit consent if that data has not been "manifestly made public" by the data subject and no other exception applies.[83] Special categories of data include;

74 Case C-210/16, [15].
75 Case C-210/16, [40] noting that as non-Facebook users could visit the page in that circumstance the responsibility of the administrator of the page would be even greater.
76 C-673/17 *Planet49*.
77 See, Article 5.
78 Ibid. It is worth noting in this respect that the Article 29 Working Party in its 2012 Report on Cookie Consent noted that by default social plug-ins should not set a third part cookies in pages displayed to non-members, Article 29 Working Party, Opinion 04/2012 on Cookie Consent, 2012).
79 Commission Nationale de l'informatique et des libertés, 'Déliberation SAN-2019-001 du 21 janvier 2019' https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001_21-01-2019.pdf (accessed 5 March 2019).
80 Article 29 Working Party on Data Protection, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 2014), 16.
81 Ibid.
82 Frederik Zuiderveen Borgesius and Joost Poort, 'Online Price Discrimination and EU Data Privacy Law' (2017) 40 *Journal of Consumer Policy* 347, 360.
83 The exceptions provided in Article 9(2) include (a) explicit consent, (b) necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law as authorised by member state law (c) protect vital interests (d) carried out in the court of its legitimate activities and with appropriate safeguards by a foundation, association or other non-profit body for phi, religious, trade union aim with regard to its current and former members only (e) relates to

racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and the processing of genetic data or biometric data for the purpose of uniquely identifying a natural person or data concerning health or an individual's sex life or sexual orientation. In addition, Recital 51 requires that personal data which are by their nature sensitive merit specific protection in a context where their processing could create significant risks to fundamental rights and freedoms.

As the CNIL decision in *Vectaury* noted, and as Sandra Wachter[84] has argued elsewhere, the collection and aggregation model used by AdTech at present effectively allows individual characteristics or preferences which are classified as 'special categories' of data under GDPR to be deduced or inferred through aggregation and analysis. The result should therefore be, on a purposive reading of the Regulation, that the enhanced, explicit consent requirements under Article 9 are triggered even where the initial data collected are non-sensitive but where their combination with other data, or their geographic of temporal record is such as to allow the imputation of sensitive categories of data.

However, both the IAB Framework and the AB Guidelines permit data to be processed with, at most, implicit consent based on the consumer's previous consents or continued use of a service. This is insufficient under the GDPR in accordance with the threshold established for consent but specifically impermissible in the context of sensitive categories of personal data.[85] This does not appear to have deterred Facebook[86] or its companies WhatsApp[87] and Instagram[88] or Google[89] from processing special categories of data under Article 9 GDPR with basic, rather than explicit permission.

Complaints filed by NOYB against all four companies allege their data collections models fail to specify the legal basis on which data is processed, as required under Articles 6 and 9. In particular the complaints note that the contracts used simply list all possible grounds for lawful processing under Article 6 leading to the assumption that processing is based on consent by failing to indicate on what other Article 6 basis the processing is conducted. However, the privacy policies of the companies only note that they process data of their users as necessary "to fulfil our terms" importing an association with Article 6(b) and (f) which is not clarified. Moreover, such companies do not inform their users of the actual uses to which their data may be put, including sensitive data, as required under Articles 12 and 13.

personal data which are manifestly made public by the data subject (f) establishment, exercise or defence of legal claims (g)necessary reasons of substantial public interest (h) necessary for the purposes of preventive or occupational medicine (i) processing in necessary for reasons of public interest in health.

84 Sandra Wachter, 'Affinity Profiling and Discrimination by Association in Online Behavioural Advertising' (2019) 35 *Berkeley Technology Law Journal* Forthcoming.

85 Commission Nationale de l'informatique et des libertés, 'The Restricted Committee of the CNIL imposed a sanction of 150,000 € against Facebook Inc and Facebook Ireland' https://www.cnil.fr/en/facebook-sanctioned-several-breaches-french-data-protection-act (accessed 5 March 2019).

86 NOYB, 'GDPR: noyb.eu filed four complaints over "forced consent" against Google, Instagram, WhatsApp and Facebook' 25 May 2018 https://noyb.eu/4complaints/ accessed 5 March 2019. The complaints appear to have been removed - an article based on the complaints is available at https://www.theguardian.com/technology/2018/may/25/facebook-google-gdpr-complaints-eu-consumer-rights

87 Ibid.

88 Ibid.

89 Ibid.

4.4 Failure to Inform Data Subjects under Articles 12 and 13 GDPR

Article 12 GDPR requires the data controller to take appropriate measures to provide any information about how data will be used to be provided in an intelligible and easily accessible form using clear and plain language. In addition, Article 13 GDPR provides that where personal data are collected, the controller shall provide the data subject with a range of information including, but not limited to, the purposes of processing, the recipients or categories of recipients of the data, the period for which the data will be kept (and how such a period is determined) and the existence of automated decision making including profiling which the data may be exposed to, including meaningful information about means used. Recital 39 further notes that any processing of personal data should be lawful and fair, and clarify what personal data are collected, used, consulted or otherwise processed and to what extent are those data processed by others.

In January 2019, the CNIL fined Google for violating Articles 12 and 13 GDPR Article through its use of contractual terms which lacked transparency and provided inadequate information to data subjects – thus failing to satisfy the requirements for valid consent.[90] In particular, the CNIL found that *"essential information"* such as the data processing purposes, storage periods and the categories of personal data gathered were *"disseminated across several documents"* such that users were required to make additional investigations to find how their data is being processed in personalising advertisements.[91] The decisions noted the information which was communicated to users was not sufficiently clear to enable consent and criticised the vague and obfuscatory nature of the description and purposes of processing presented to users.

In the context of AdTech the decision is particularly relevant, highlighting that information must be unified and should not be provided through a design which renders it deliberately challenging to build a picture of how and for what purposes individual data is used.

In similar decisions relevant to the AdTech market both a Belgian Court, and France's CNIL[92] have found that Facebook's terms do not make it sufficiently clear that apps and therefore Facebook itself systematically collect personal data when consumers visit third party websites that contain Facebook social plugins even where they do not have a Facebook account.[93] These decisions should have had a chilling effect on such activities by Facebook, and indeed other AdTech actors, however, this does not appear to have been the case.[94] Indeed, it appears that while Articles 12 and 13 are well intentioned, the requirements for simple, easily understood language, instead of increasing clarity have been used to excuse the deployment of overly simplified terms which offer a false reassurance to consumers and

90 Commission Nationale de l'informatique et des libertés, 'Déliberation SAN-2019-001 du 21 janvier 2019' https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001_21-01-2019.pdf accessed 5 March 2019.

91 Ibid.

92 Commission Nationale de l'informatique et des libertés, 'The Restricted Committee of the CNIL imposed a sanction of 150,000 € against Facebook Inc and Facebook Ireland' https://www.cnil.fr/en/facebook-sanctioned-several-breaches-french-data-protection-act accessed 5 March 2019; The 16th of February, the court of First Instance rendered its judgment in the proceedings on the merits in the case of the Authority v Facebook' https://www.dataprotectionauthority.be/news/victory-privacy-commission-facebook-proceeding accessed 5 March 2019.

93 Ibid; See also Case C-210/16, [28]-[29].

94 See, Valerie Verdoodt Brendan Van Alsenoy, Rob Heyman, Jef Ausloos, Ellen Wauters and Günes Acar, From social media service to advertising network, 2015 https://www.law.kuleuven.be/citip/en/facebook-1/facebooks-revised-policies-and-terms-v1-2.pdf.

obfuscate the true nature and extent of the dissemination of person data through the AdTech ecosystem.

4.5 Automated Decision-making under Article 22 GDPR

According to Article 22 GDPR explicit consent is required where solely automated decisions are made relating to individuals. Specifically Article 22 requires that subjects shall have the right not to be subject to a decision based solely on automated processing including profiling which produces legal effects concerning him or similarly significantly affects him or her though this does not apply under Article 22(2) where same is necessary for entry or performance of contract or based on explicit consent.[95]

Though Article 22 has not been considered by the CJEU, nor was its precursor Article 15 of the Data Protection Directive, the Article 29 Working Party has identified occasions where behavioural advertising within the AdTech market may have significant effects for the purpose of Article 22 of the GDPR, specifically where consumers are targeted with potentially damaging goods or services, such as gambling or high interest loans.[96] More concerning, is the practical reality that individuals are grouped according to imputed characteristics as part of the analysis of data and the online bidding process in a way that may constitute profiling under Article 22. Underlying these concerns, is the fact that it is not clear that actors in the AdTech system obtain the valid, explicit consent necessary for processing under Article 22, in particular in light of decisions such as *Vectaury*.

4.6 The e-Privacy Directive

In addition to the GDPR, the e-Privacy Directive (ePD), as noted in section three above, operates a particular regulatory regime applicable to the technological mechanisms which enable the AdTech market. The Directive requires in Article 5 that cookies can be set only where the consumer has been 'supplied with clear and comprehensive information' concerning the purposes of the processing and is offered the right to refuse such processing by the data controller. In practice however, this 'informed opt out' has provided little additional protection to individuals with many websites actively employing interfaces that are hostile to consumer choice, or simply blocking consumers from accessing the site or service unless the default cookie settings are accepted.[97]

The ePD Recitals were revised in 2009 to provide that users could opt in through default web browser settings.[98] This was not uncontroversial, the Article 29 Working Party noted that in 2010 three of the four major browsers had default settings which permitted cookies and that user failures to alter such settings could not be interpreted as amounting to consent[99] a suggestion which the Working Party reiterated in 2013.[100]

The CNIL's 2019 decision against Google considered above in the context of legitimate interests was also concerned with default permissions, as was the CJEU's rejection of pre-ticked boxes in its decision in *Planet49*. That latter decision is particularly relevant to the AdTech market as a result of the Court's decision that cookie data under Article 5 need not be personal in order to be covered by the Directive but rather acts to protect the users' broader 'private sphere' in the words of the Advocate General. The decision also noted the need for explicit and transparent information for consumers on the duration of cookies and whether the information they collected was available to third parties.

A reformed e-Privacy Regulation (ePR) was due to enter into force alongside the GDPR, however, as of writing the text has not been finalised. In the drafting process, however, several points of necessary reform, and controversy have emerged which would affect the AdTech industry.[101] The first is the concern highlighted by the EDPS at an early stage, that the Regulation should not permit the processing of metadata under the 'legitimate interest' ground.[102] While the understanding of consent adopted in the Regulation will be required to be equivalent to that afforded under the GDPR (a requirement pre-empted by the Court in *Planet49*) there remained concern that to allow such processing of metadata without consent would dilute existing standards of protection by permitting an over-broad opt out from consent requirements.[103] Instead, the EDPS has opined that such data should be processed only with consent or if technically necessary for a service requested by the user and only for the duration necessary for that purpose.[104]

The second concern, also flagged by the EDPS is the strengthening of Article 10 by requiring privacy protective settings by default which genuinely support expressing and withdrawing consent in a simple, binding and enforceable manner against all parties. This would also require the inclusion of Recital 24 as a substantive provision in the form of a legal requirement such that end users would be afforded the opportunity "to change their privacy settings at any time during use and allow the user to make exceptions, to whitelist websites or to specify for which websites (third) party cookies are always or never allowed."[105]

It is unclear from the draft released in November 2019 whether these concerns will be reflected in the final text. In particular, Article 10 which, in previous versions sought to provide notification and reminder requirements regarding the placement of third party cookies has been deleted in its entirety.[106] While Article 8 (and the related

95 See, also Recital 72 GDPR.
96 Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, 2017), 9.
97 As a result of this concern Acquisti has emphasised the need for a contextual understanding of privacy as part of which the default settings for privacy used by companies are tools used to affect information disclosure and attempt to contextualise privacy in a manner which orientates the status quo toward their contractual practices as part of a malicious interface design through which designers and use features that frustrate or confuse users into disclose information is also widely deployed. See, Laura Brandimarte and George Loewenstein Alesssandro Acquisti, 'Privacy and Human Behaviour in the Information Age' in Jules Polonestsky and Omer Tene & Evan Selinger (eds), *The Cambridge Handbook of Consumer Privacy* (Cambridge University Press 2018)., 187; Ralph Gross and Alessandro Acquisti, 'Information revelation and privacy in online social networks' (2005) *WPES Proceedings of the 2005 ACM workshop on Privacy in the electronic society* 71.
98 E-Privacy Directive, Recital 66.
99 Article 29 Working Party, Guidelines on Consent under Regulation 2016/679.
100 Article 29 Working Party, 'Working Document 02/2013 providing guidance on obtaining consent for cookies' (2013). Exceptions to these requirements are provided in accordance with Article 5 and Recital 25 for technical storage and access cookies and cookies which are 'strictly necessary' to provide an information society service explicitly requested by the subscriber.
101 Formal Complaint by Dr Ryan regarding IAB Europe AISBL website, 2nd April 2019 available at https://regmedia.co.uk/2019/04/02/brave_ryan_iab_complaint.pdf accessed 21 April 2019.
102 European Data Protection Supervisor, Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications, 2017), 27.
103 Ibid
104 European Data Protection Supervisor, EDPS Recommendations on Specific Aspects of the Proposed ePrivacy Regulation, 2017), 2.
105 Ibid, 2-3.
106 See, Council of the European Union, 'Proposal for a Regulation of the

Recital 20) which considers consent for cookies remains under consideration[107] the most recent draft has deleted the final sentence of Recital 20 which previously read "Access to specific website content may still be made conditional on the consent to the storage of a cookie or similar identifier."[108] The Recital now provides that monitoring of end user devices should be allowed "only with the end-user's consent and or for specific and transparent purposes" because such monitoring may reveal personal data including political and social characteristics which require "enhanced privacy protection." [109]

This view of 'cookie walls' and similar mechanisms as impermissible is in keeping with the current interpretation of the GDPR by academics[110] and more recently by the Dutch data protection regulator. In a recent decision from the Netherlands the Dutch data protection regulator found that refusing users access to websites unless they consent to cookies was impermissible under the GDPR.[111] That decision, and indeed the content of Recital 20, echo the concerns flagged by the decision in *Vectaury* that special categories of data as classified under Article 9 GDPR are discoverable through the aggregation and analysis of the data collected by cookies.

While the language of the proposed e-Privacy Regulation may thus seem strong, in reality it would achieve little more than a reproduction, albeit in explicit language, of the controls already imposed by the ePD and the GDPR.

4.7 Conclusion

It is clear, that at present there are concrete basis under both the GDPR and ePD on which to ground objections to the operation of the AdTech market. However, the impact of these basis, as well as the decisions in cases like *Planet49* and *Vectaury*, is diminished by the realities of the digital market. That such business models have perpetuated online despite these laws is indicative of a lack of effective enforcement. While it now appears that this shortcoming of enforcement is being ameliorated at a national level by more active regulatory engagement, more fundamental concerns remain.

In particular, as a practical matter for consumers there remains no functional choice for consumers to engage with providers of goods and services who *do not* employ surveillance mechanisms which operate as part of the AdTech market. At present the GDPR and ePD can only impose information requirements and consent thresholds. Neither documents, nor the policies of the Union more broadly, acknowledge that absent a market which also offers goods and services whose provision is not attendant on consenting to such collection and sale of personal data, even the most explicit and informed consent is normatively vacuous as it is given in a context in which no meaningful alternative is present.

This failure goes to the heart of the disconnect between the rights to data protection and privacy in Union law. While data protection is currently conceived of as a right, functionally it operates as the condition under which the infringement of a private right is legally permissible. As such, it is the market-oriented manifestation of privacy, imposing the threshold conditions under, and extents to which, privacy can be forfeited by individuals as the condition for market access and participation.

As such, data protection is commercially, and indeed personally, necessary. However, in the current schema of rights protection within the Union it has taken on an outsize importance to this role, effectively dwarfing the right to privacy which it is intended to enable. More fundamentally, if we consider compliance with data protection requirements as the necessary conditions for legally justified infringements of privacy, the analysis above illustrates that such conditions are being systemically violated by the AdTech market at present such that even this minimal understanding of privacy is not satisfied. The result, as the next section examines, is a perpetuation of a legal context in which privacy rights are ailing, importing consequences for individual autonomy, and the Rule of Law.

5. The Impacts of AdTech on Privacy & Autonomy

The most fundamental harm which results from the consumer surveillance on which AdTech relies is the reduction of individual privacy. It would be remiss to insist this is purely a result of the AdTech landscape, the harm has also been facilitated to no small extent by the Union's curtailing of privacy in operational terms as a result of its preference for a shallow, and market-oriented understanding of data protection as a sufficient privacy protecting mechanism and its failure to systemically analyse the compliance of the AdTech market with even those mechanisms.

By allowing the compilation of large data sets from which layered profiles of individuals' actual and inferred preferences, characteristics and activities can be assembled, AdTech allows the revelation of intimate and detailed portraits of individuals. This, in itself, is harmful in as much as the fundamental right to privacy in EU law propounded by both the CJEU and ECtHR emphasises the right as crucially linked to the development of personal identity.[112]

Where privacy is infringed, individuals' capacity for personal identity development is thus jeopardised by forcing conditions in which individuals are unable, or do not feel able to make choices which accurately or meaningfully reflect their preferences in furtherance of their personal development. This threat is compounded in the context of AdTech which actively seeks to utilise coercive and manipulative tactics to influence consumer attention and preferences, in circumstances where the means of avoiding such tactics are not present. In that context individuals experience proportionate reductions in their capacity to choose without external influences but also experience chilling effects to their exercise of uninhibited choice or action resulting in the active diminution of individual autonomy.

Autonomy in this context can be understood as mirroring the concept articulated by Raz, of 'people controlling, to some degree, their own destiny, fashioning it through successive decision throughout their

European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' (2018).

107 Ibid, 3.

108 Ibid, Recital 20.

109 Ibid, Recital 20.

110 Sanne Kruikemeier Frederik J Zuiderveen Borgesius, Sophie C Boerman and Natali Helberger, 'Tracking Walls, Take it or leave it Choices, the GDPR and the ePrivacy Regulation' (2017) 3 *European Data Protection Law Review* 353.

111 Autoriteit Perssonsgegevens, Websites must remain accessible when users refuse tracking cookies, https://autoriteitpersoonsgegevens.nl/nl/nieuws/websites-moeten-toegankelijk-blijven-bij-weigeren-tracking-cookies, 2019.

112 Case C-208/09 *Sayn Wittgenstein* EU:C:2010:806, [52]; Case C-391/09 *Malgozata Runevic-Vardyn* EU:C:2011:291, [66]. In the ECtHR see, X v Iceland App No. 6825/74 (1976); *Gaskin v UK* App No. 10454/83(1989). The State's refusal to provide the applicant access to records it held regarding his time in care was a violation of Article 8; *Ciubotaru v Moldova* App No. 27138/04 (2010); Odievre App No. 42326/98 (2003); *Karassev v Finland* App No. 31414/96 (1996); *Stjerna v Finland* App No. 18131/91 (1994).

lives.'[113] Autonomy thus requires the presence of an adequate range of morally acceptable options to choose among. In particular, Raz notes that choice between bad options may not constitute choice sufficient to facilitate autonomy at all.[114] In the context of the digital market this functional choice between viable alternatives is not present. AdTech is not only ubiquitous but systemically engrained and thus impossible to avoid, the only alternative to engaging with it being to forfeit online activity entirely. The dilemma for, and risk to, autonomy thus crystallises in this Razian articulation of the conditions for autonomy.

This understanding of autonomy also requires the presence of meaningful choice free from manipulation, coercion or excessive undue influence[115] and understands autonomy as the capacity for socially situated individuals to make choices which result from deliberative action. Once again in the digital market, AdTech obstructs such freedom, actively seeking to influence the attention and choices of consumers through its collection and analysis of data and its deployment of behavioural advertising practices.

Significantly, Raz's conception of autonomy also presupposes a concept of alienation. When Raz defines autonomy as the capacity to be the author of one's own life – to give it a shape and meaning (an articulation which accords with the understanding of privacy in EU law) - he is not only claiming that the autonomous individual must independently and actively shape her life. In addition, she must presuppose that something matters in her life. Determining oneself then must mean determining oneself *as* something.[116]

Where the capacity to exercise autonomy is hampered, individuals are unable to establish a relation to other individuals, to things, to social institutions and thereby to themselves – they are, in other words, unable to establish themselves *as* something. This inability, referred to as alienation, prevents individuals from distilling meaning from their existence.[117] The commodification of goods and domains that were previously not objects of market exchange is a common historical example of this kind of alienation. AdTech, through its obstruction of individual attempts to relate to those goods or areas which individuals use to define their selves and through its attempts to condition the preferences and thus relations of individuals to other actors actively diminishes individual autonomy and alienates individuals, preventing them from engaging in the development of personality which the right to privacy is explicitly understood as seeking to protect.[118]

Alienation understood in this way is a condition attendant on the reduction of autonomy which itself results in a further loss of individual power - alienated individuals are disempowered, not subject to their own, and vulnerable to the imposition of another's, law.[119] Alienation thus negatively impacts individual liberty, on the basis that it is only when individuals experience and are empowered to experience life as their own, governed by their own choices that they are free.[120] Under this conception autonomy, and the reduction or elimination of alienation, is not merely an individual but is also a social good, acting to ensure the individual development of personality and preference through deliberative choice and to create empowered individuals - pre-conditions central to democratic participation and thus to democratic society.[121]

The European Union's understanding of privacy as fundamentally related to the development of personality, and thus to individual autonomy, recognises that the capacity for individual development diminishes as privacy does.122 Where such restriction of individual self-development occurs, the result is that, at a societal level, individuals are impeded from critical engagement with the processes of democratic self-government due their impaired ability to fulfil their roles as active and engaged citizens. Citizenship, in a European context, is thus understood as more than a status, as a set of social practices whose fulfilment includes voting, public debate, and political opposition which are influenced by institutional mores.[123] The protection of privacy and the promotion of autonomy and individual liberty is thus constitutive of a healthy Rule of Law.

6. AdTech & The Rule of Law

The Rule of Law has been repeatedly proffered as a foundational value of the European project as part of a cluster of ideals constitutive of European political morality, the others being human rights, democracy, and the principles of the free market economy.[124] While neither the Rule of Law nor fundamental rights featured in the Treaty of Rome's text, the Union's constitutional framework has subsequently placed increasing emphasis on both, and affords them a position of centrality in its internal and external policies, featuring them not only as foundational values (identified by the Lisbon Treaty, and later manifested through the Charter and its jurisprudence) but also as central pillars of the Union's external relations.

Article 2 TEU, as the culmination of the Union's commitment to the Rule of Law as an orienting value,[125] links the Rule and fundamental rights to each other alongside the achievement and maintenance of democratic government. The implication of this grouping is an understanding of the three values as interdependent and mutually reinforcing. The Charter's preamble takes a similar stance to Article 2, positioning the Rule of Law as a shared value of the peoples of Europe in the context of fundamental rights, while recent cases linked to ongoing concerns surrounding the Rule of Law in Poland have leant further weight to the suggestion implicit in Article 2's grouping that the theory of the Rule of Law endorsed by the Union is a substantive

113 Joseph Raz, 'Autonomy, toleration and the harm principle' in Susan Mendus (ed), *Justifying toleration: Conceptual and historical perspectives* (Cambridge University Press 1988), 369.
114 Raz (n 113) 372.
115 Bernal (n 7) 24-5.
116 Rahel Jaeggi, *Alienation* (Columbia University Press 2014), 204-5.
117 Jürgen Habermas, *Justification and Application: Remarks on Discourse Ethics* (MIT Press 1993), 48.
118 Jaeggi (n 116) 4-5.
119 Jaeggi (n 116) 22-23.
120 Steven Lukes, *Marxism and Morality* (Oxford University Press 1985), 80.
121 Raz (n 113) 314 'the ruling idea behind the ideal of personal autonomy is that people should make their own lives.'
122 See Rouvroy and Poullet (n 62); *X v Iceland* Application No. 6825/74 (1976); Niemietz v Germany App No. 13710/88 (1992); *Dudgeon v United Kingdom* App No. 7525/76 (1981), [41]; *Klass and Others v Germany* App No. 5029/71 (1978); *Big Brother Watch and Others v The United Kingdom* App No. 58170/13, 62322/14 and 24960/15 (2018); Case C-208/09 *Sayn Wittgenstein* EU:C:2010:806; Case C-391/09 *Malgozata Runevic-Vardyn* EU:C:2011:291, [66].
123 Commission Communication, 'The Commission's Contribution to the Period of Reflection and Beyond: Plan D for Democracy, Dialogue and Debate' COM (2005) 494, 2-3; Andrew Williams, *The Ethos of Europe: Values, Law and Justice in the EU* (Cambridge University Press 2010), 154-156. See also, Ireneusz Pawel Karolewski, *Citizenship and Collective Identity in Europe* (Routledge 2010), 108-112 on the shift from a model of caesarean effective citizenship to one based on a deliberative model; John JH Weiler, 'To be a European Citizen: Eros and Civilisation' in John JH Weiler (ed), *The Constitution of Europe* (Cambridge University Press 1999).
124 Jeremy Waldron, 'The Concept of the Rule of Law' (2008) 43 *Georgia Law Review* 1.
125 It is beyond the scope of this work to engage substantively with the possible implications of this change in language for the justiciability of the values.

one primarily oriented toward to the promotion of individual liberty through democratic government.[126] This understanding of the Rule of Law's practical function is particularly in the Union's commitment to a substantively enforced standard for its Member States in respecting the Rule of Law at a national level, in Article 7 TEU.[127] A reading which finds further support in the constitutional and administrative principles which underpin the EU legal order.[128]

The difficulty with any substantive theory of the Rule of Law is, of course, that its boundaries are difficult to draw, not least as a result of the ambiguous standing of fundamental rights within the Union. Ultimately, the Rule of Law has traditionally functioned to ensure individual liberty, and those fundamental rights which are necessary in enforcing and protecting such liberty must necessarily form part of a substantive theory however widely or narrowly drawn such a theory otherwise is. This is particularly so in the Union, which has explicitly grouped the preservation of democratic order, and fundamental rights alongside the Rule of Law as an orienting principle.

Liberty itself is a porous notion,[129] however, Tamanaha's four concepts of liberty provide a utile framework for assessing the coetaneous nature of liberty and the Rule of Law. Tamanaha posits a layered idea of liberty composed of:

- Political liberty, effected through democratic participation and government[130] and which accords with modern understandings of representative democracy as recognised by Article 2 TEU and enforced by Article 7 TEU,
- Legal liberty which provides that the State act only in accordance with law and in accordance with ideas of legal predictability and equality and which finds expression in the requirement that restrictions on fundamental rights be provided 'by law,'[131]
- Individual liberty which subsists where the government is restricted from infringing upon an inviolable realm of personal autonomy and which finds expression to some extent, the Treaties which seek to delimit the bounds of individual rights and the conditions for State intrusion upon the areas or activities which they protect,[132] and
- Institutional liberty, which holds that individual and therefore societal liberty is enhanced when the powers of government are compartmentalised thus preventing an accumulation to power in a single institution.[133]

In examining Tamanaha's systematisation, it is apparent that the European Union's understanding of the Rule of Law maps onto all four of the distinct categories of liberty identified. Moreover, the categories of liberty identified are coetaneous with the Rule of Law in as much as they seek to ensure an adequately restrained government which adheres to democratic principles of institutional balance, and the equal and predictable application of laws. The result is the creation of a layered, constitutional conception of the Rule of Law not only as seeking the ultimate goal of ensuring individual liberty but also of being fundamentally constitutive of liberty in a broader, political, context.

In accordance with this conceptualisation of the Rule of Law the right to privacy must form part of a minimum content of the Union's substantive conception of the Rule of Law given its centrality in securing individual autonomy and thus facilitating the individual liberty necessary for democratic participation and thus, liberty more broadly. As such, the privacy harms which AdTech imports ultimately reduce individual autonomy and alienate individuals resulting in a loss of liberty which ultimately diminishes the health of the Rule of Law within the Union.

Yet this is not the only mechanism by which AdTech impacts the Rule of Law. On a more practical level, the Rule of Law is affected by AdTech's capacity to enable the development of mechanisms of constitutional avoidance, which permit State actors to bypass limitations to or exemptions from the protective remit of fundamental rights protections through the use of private actors as their proxies. A high-profile example of this pattern in practice was the 2017 Cambridge Analytica revelations. The information uncovered during that episode should have been of little surprise to anyone familiar with the functioning of the AdTech market. Nevertheless, it offered a useful example of the manner in which AdTech harms the Rule of Law.

In 2017 it was revealed that a Cambridge academic working as a researcher for a private company, Cambridge Analytica (CA), had obtained, from Facebook, a large data set containing information relating to an unknown quantity of the company's users. This data set was the combined by the staff at CA with information from other commercial sources to build a data rich system which could target voters with personalised political advertisements based on their psychological profile.[134] The targeting system was then sold to interested actors and was bought and used by candidates for the Republican presidential nomination in the United States,[135] parties campaigning in the Brexit referendum[136] and parties running political campaigns in other jurisdictions including Brazil, India, Kenya, Nigeria and Mexico.[137]

Using the highly specific and personal data profiles sold by Cambridge Analytica, these campaign teams targeted voters on an individual level, as well as identifying and targeting voter blocks by creating

126 See, Case C-216/18 LM EU:C:2018:586; Case C216/18 *PPU Minister for Justice and Equality* EU:C:2018:586, [48]. See also, *Minister for Justice v Celmer (No 2)* [2018] IEHC 153, (Donnelly J). Subsequent to the reference in LM, Donnelly J in *Minister for Justice v Celmer* (No. 5) [2018] IEHC 639 found that the deficiencies in the independence of the Polish judiciary did not meet the threshold for refusal of surrender.

127 European Commission 'Rule of Law: European Commission acts to defend judicial independence in Poland' 20 December 2017, at http://europa.eu/rapid/press-release_IP-17-5367_en.htm (accessed 27 February 2018).

128 Theodore Konstadinides, *The Rule of Law in the European Union* (Hart 2017), 84 et seq.

129 Isaiah Berlin, *Four Essays on Liberty* (Oxford University Press 1969), 121.

130 Jean Jacques Rousseau, 'The Social Contract' in Sir Ernest Baker (ed), *Social Contract: Essays by Locke, Hume and Rousseau* (Oxford University Press 1960), Book II, 6; Brian Z Tamanaha, *On the Rule of Law: History Politics and Theory* (Cambridge University Press 2004), 34.

131 Sharon R Krause, 'Two Concepts of Liberty in Montesquieu' (2005) 34 *Perspectives on Political Science* 88; Tamanaha (n 130) 34-35.

132 Tamanaha (n 130) 35.

133 Tamanaha (n 130).

134 Carole Cadwalladr, ''I made Steve Bannon's psychological warfare tool': meet the data war whistleblower' (*The Observer,* 17 March 2018) https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump (accessed 16 August 2019).

135 Cadwalladr (n 134).

136 Alex Hearn, 'Cambridge Analytica did work for Leave.EU, emails confirm: Parliamentary committee told work went beyond exploring potential future collaboration' The Guardian 30 July 2019 https://www.theguardian.com/uk-news/2019/jul/30/cambridge-analytica-did-work-for-leave-eu-emails-confirm (accessed 16 August 2019).

137 Tactical Tech Report forthcoming: The Influence Industry: The Global Business of Using Your Data in Elections quoted in Julianne Kerr Morrison and Ravi Naik Stephanie Hankey, *Data and Democracy in the Digital Age*, 2018).

tailored messaging and content based on the personal information harvested through the AdTech market.[138] The analytics and aggregation practices used are standard industry practice in online advertising, and rely on the contractual mechanisms and current regulatory approaches which this article has examined.

While this in itself is harmful in a commercial setting, a particular threat to the Rule of Law occurs when public actors capitalise on the AdTech market's capacity to influence individuals to covertly leverage public opinion and influence political choice in a manner they would be constitutionally restrained from doing should they seek to collect and analyse data in a similar way themselves. In this context, privacy rights contribute to the Rule of Law, and seek to ensure a democratic governance, by limiting state intervention with and surveillance of citizens through private proxies.

Privacy thus reinforces the barriers between the individual and the State within the contours of civil society and on that basis is one of the strengths of the democratic model - functioning, in Westin's account, to ensure the 'strong citadels' of autonomous action and personal development which are a prerequisite for liberal democratic society.[139]

The role of online data gathering in facilitating democratic harms was, belatedly, acknowledged following the Cambridge Analytica investigation by the UK Parliament, which revealed that company and indeed Facebook itself, had targeted individuals[140] in a manner which interfered with democratic elections. However, the contributory role of privacy in militating against such data gathering within the AdTech market, and thus against democratic undercutting has yet to be explicitly recognised.

7. Conclusion

The right to privacy in the European Union is premised on an understanding of privacy as enabling the development of individual personality, and as fundamentally linked to the achievement of individual autonomy and liberty. However, this foundation has been obscured by the lack of operational force enjoyed by the right, and the legislative elevation of data protection to the exclusion of more fundamental privacy concerns.

In this context the operation of the AdTech has operated with a significant degree of freedom. While decisions such as *Vectaury* and Planet49 indicate a hardening of attitudes towards the notification and consent thresholds necessary for the data collection practices AdTech, there has not been, as yet any consideration of the need for stricter regulation of the AdTech market or the practices it operates in light of the privacy harms which its operation facilitates.

Most concerningly, there seems little awareness of the crucial nature of such reform given the right to privacy's function in securing democratic participation and as part of a substantive conception of the Rule of Law. In this respect, AdTech is more systemically problematic than is currently acknowledged, importing layered harms at an individual, and societal level. Acknowledging these impacts is the first step toward creating a sustainable online ecosystem which contributes to rather than conflicting with the attainment of individual autonomy and social goods.

138 Information Commissioner's Office, *Investigation into the use of data analytics in political campaigns*, 2018).

139 Alan Westin, *Privacy and Freedom* (Atheneum 1967), 24.

140 ICO (n 138); In March 2019 the EU adopted new rules to "prevent misuse of personal data by European political parties." The move came ahead of the European Parliament elections, which took place across the continent in May 2019, Council of the European Union, EU set to adopt new rules to prevent misuse of personal data in EP elections (2019).