NEW ECONOMICS FOUNDATION

BLOCKING THE DATA STALKERS

GOING BEYOND GDPR TO TACKLE POWER IN THE DATA ECONOMY

NEW
ECONOMICS
FOUNDATION

CONTENTS

EXECUTIVE SUMMARY

Ninety percent of the world's data was created in the last two years, and over 2.5 quintillion bytes of data are produced every day. Whole companies are built around principle of relentlessly collecting as much data about internet users as possible, and monetising it. Our digital selves are now marketable products. And this data is then used to market products to us. In 2018, almost half of all advertising spend will be online, rising to over 50% by 2020. And two digital giants – Facebook and Google – now control 84% of the market. The companies are hugely reliant on ad revenue, with Facebook collecting 97% of their overall revenue from ad spending while at Google it accounts for 88%.

When someone clicks a link to a webpage, between their clicking and the page loading, information about them is compiled and sent out in order for advertisers to assess the value of showing them an advert. These are called 'bid requests', and they totally fail to ensure the protection of personal data against unauthorised access. They can even include sensitive information such as a person's sexuality, or political beliefs. Bid requests on UK users are being sent out at a rate of almost 10 billion per day, or 164 per person per day, and are seen by hundreds if not thousands of advertisers.

25% of all ad spend is lost to fraud. The ad tech industry is potentially exposing every internet user to the non-consensual sharing of their data with thousands of companies who are all able to copy, share and sell the data on again. The now infamous Cambridge Analytica was one of many companies that had access to this stream of personal data.

While the General Data Protection Regulation (GDPR) addresses some privacy issues, it does not address the issue of power in the data economy generally, and the ad tech sector specifically. GDPR is limited because it focuses too heavily on individual actions, like giving consent, or lodging a complaint with the Information Commissioner's Office. Accountability for tech giants is undermined by allowing justifications such as 'legitimate interest' or 'necessity' to be used by data collection companies. GDPR also fails to protect metadata or inferred data, despite the ability of both to identify individuals, and does not adequately control the on-sell of data between firms.

RECOMMENDATIONS

We recommend going further than GDPR in a number of ways.

We recommend a ban on sending personally identifiable data out to advertising networks. Instead of relying on the sale and re-sale of personal data, when users click on weblinks, bid requests should give advertisers demographic information about the audience of the website. This would allow them to show demographically appropriate advertising, without compromising the privacy of users. Where websites do sell ad space that uses personal data, they should be required to gain explicit consent from individuals in order to do so.

This proposal would be transformational.

- It would tackle data leaks, by preventing any personal data from being sent (and therefore potentially compromised) during bid requests.
- It would reduce the commodification of personal data, by reducing the market for personal data and diminishing the ability of companies to monetise it.
- It would force tech giants to diversify their business model away from services based on constant surveillance and advertising.
- It would give power back to websites which spend time producing content and have a dedicated user base.

It would fight back against ad fraud, by halting the revenue that can come from fraudulent sites.

We also recommend:

Devices, software, and online interactions should be subject to privacy by default and design. This means they would be automatically set to not collect, share or sell on our personal data. We would then have a series of options and tools which we could use to change this default setting to specify which third parties could gather data on us securely and for what purpose.

When consenting to data collection and sharing the terms and conditions of any website or service, providers should make it clear exactly what data is being collected and who it may be shared with or sold to. This information should be standardised and consistent. To help with this, reviews of terms and conditions could be crowdsourced, or consent could be given by proxy through trusted individuals or groups, perhaps for a small fee.

Protecting people should be prioritised over corporations' business models by restricting the use of loopholes, like the GDPR 'legitimate interest' justification.

Data sharing and selling between companies without the consent of the data subject be banned, whether in the same company family (like Google and YouTube) or totally separate. We would bring an end to this by restricting the sale of third party access to our data to cases where we have given our explicit consent to grant that specific third party access.

1. INTRODUCTION

Ninety percent of the data in the world today has been created in the last two years with over 2.5 quintillion[1] bytes produced daily.[2] This data comes from every imaginable source: mobile phone location information, posts to social media sites, digital pictures and videos, purchase transactions, and sensors used to gather information as people move around, to name a few (see Figure 1).

Whereas the collection and storage of data was once a costly process, advances in network technology, computing processing, and storage have made data gathering almost free. Powerful actors, from tech firms to governments, collect all the data they can, from as many sources, in whatever way possible – whether or not they have a current use for it. Data collection practices have become so pervasive that few people know about the systems that target them in their homes, in stores, on the street, online, and pretty much everywhere they go.

There are increasing worries about the 'datafication' of society.[3,4] These debates are overwhelmingly concerned with questions of individual privacy[5] and the protection of personal data.[6] Understandably, a lot of people don't really care, feeling they have 'nothing to hide'.[7] What the 'nothing to hide' argument forgets is that "the premise [is] that privacy is about hiding a wrong. It's not. Privacy is an inherent human right, and a requirement for maintaining the human condition with dignity and respect."[8] Although the threat posed by these systems to privacy is real, it's the power they bestow that is a more serious and unaddressed issue. This manifests in the way powerful institutions hoard data and use it to nudge us towards their own economic and political ends.[9] Although the volume and ubiquity of data collection by companies is itself a major challenge, the way it's sold and shared amplifies it. This is hugely disempowering for individuals and hampers our ability to hold companies using our personal data to account (Box 1).

1.1 PERSONALISED ADVERTISING

The rationale for collecting, selling, and sharing is often based on the need to monetise our data through the provision of personalised adverts. There is perhaps nothing that exemplifies the modern data economy more than the way the ad tech industry and associated technical systems work. And while many major tech companies

FIGURE 1: DATA PRODUCED EVERY MINUTE OF 2017*

Platform	Data
Netflix	Users stream 69,444 hours of video
Snapchat	Users share 527,760 photos
LinkedIn	Gains 120+ new professionals
YouTube	Users watch 4,146,600 videos
Twitter	Users send 456,000 tweets
Texts	15,220,700 texts sent
Skype	Users make 154,200 calls
Instagram	Users post 46,740 photos
Internet data	Americans use 2,657,700 GB of internet data
Spotify	Adds 13 new songs
Uber	Riders take 45,787.54 trips
Venmo	Processes $51,892 peer-to-peer transactions
Buzzfeed	Users view 50,925.92 videos
Google	Conducts 3,607,080 searches
Wikipedia	Users publish 600 new page edits
Email	103,447,520 spam emails sent
Tumblr	Users publish 74,220 posts
Amazon	Makes $258,751.90 in sales
The Weather Channel	Receives 18,055,555.56 forecast requests
Giphy	Serves 694,444 GIFs

* Domo. (2017). *Data Never Sleeps 5.0.* Retrieved from: https://www.domo.com/learn/data-never-sleeps-5

rely on advertising for their revenues, the system is so problematic from a societal and technical perspective that we shouldn't seek to perpetuate it but to stop it.

During the twentieth century, advertising was all about companies and organisations securing the best space to show off their wares. Perhaps a strategically placed billboard, a

BOX 1. HOW DATA COLLECTION, SHARING, AND SELLING IS ALREADY RUINING LIVES

Catherine Taylor's world was turned upside down when a data broker, ChoicePoint, incorrectly linked her to a criminal charge of intention to supply methamphetamines.[10] The data broker then sold on her file many times so that the original error was replicated widely across the many digital profiles maintained about Catherine.

Luckily for Catherine she was able to find this incorrect data and through communication with ChoicePoint they removed the record. But this didn't rectify the error in all the systems that had bought her incorrect data. Catherine was forced to personally contact all the other brokers, exhausting in itself, and even file lawsuits to get the offending data removed.

The error costed her job interviews, as employers were put off by the black mark against her name. It took over four years for her to find a job. In the meantime, she was rejected for an apartment she wanted to buy and couldn't even get credit for a new washing machine.

Although Catherine was able to remove almost all the data, it took a huge toll on her personally, consumed lots of time and effort, and exacerbated her health problems. But at least she was aware of the offending data. Many people could be and are affected without realising, without knowing the reason or having the time, knowledge, and patience to resolve the issue.

particular magazine, or, more recently, a television slot. Advertisers had to go to where they thought their target market was, or, as with billboards and other public adverts, to show their products to a huge number of people in the hope that some of them would be their target audience. This meant that companies who had particular audiences could charge advertisers for access to them. For example, if they wanted to target well-off professionals, they'd go for *The Economist* or the *Financial Times*; if they wanted to reach the archetypal 'man in a van', they'd head to *The Sun*.

Initially, the emergence of the digital space didn't really change this all that much. Advertisers still went to where they thought their audience was and bought space, often through

brokers and other intermediaries. Today, however, the picture is radically different. In 2018 almost half (44%, worth $237 billion) of all advertising spend will be online, rising to over 50% by 2020.[11] Advertising has migrated online in a remarkably short space of time. But what is more remarkable is that advertisers can now target individuals wherever they are on the Internet; and that two digital giants – Google and Facebook – control 58% of the digital ad spend.[12]

A new system has been created for advertisers. No longer are they looking to spend their money in places where they think their customers are. Today, advertisers can target their audience wherever they are online, thanks to a pervasive online tracking system coupled with a new auction system for placing ads.

It works like this:

1. When you click on a webpage, the page does not come pre-loaded with adverts that have already been placed. As you click, the website you're visiting sends a 'bid request' to one of two main ad tech channels, OpenRTB and Authorised Buyer (the latter is run by Google).

2. During this bid request, the website provides as much information about you as possible, including the webpage you're visiting, your IP address (from which your location can be inferred), and device details. It also sends various identifying information about you (the user) from previously collected data or profile data bought in from brokers, forming a detailed profile of you.

3. This profile, built from the data offered by the website, is then used by advertisers to bid in an auction for the right to show you a particular advert, which is run as a 'second-price auction'. In these auctions, the winning bid pays the price offered by the runner up (the second price), which is supposed to make the process simpler and less risky.[13]

4. The winning bidder gets to place the ad on the page you're viewing.

This process happens repeatedly as we surf the web. Bid requests on UK users, containing our personal information, are being sent out at a rate of almost 10 billion a day or 164 per person per day,[14] and are seen by hundreds if not thousands of advertisers, who could all be illegally collecting that data, without us being aware of it.

The impact of this change in the underlying system for placing adverts has had major repercussions. The system is probably the largest source of personal data potentially being illegally collected in contravention of the spirit, if not the letter, of the General Data Protection Regulation (GDPR).[15] Changing the way that advertisers find space has had a major

impact on industries that rely on advertising revenue for survival, such as newspapers and magazines.

This presents an issue of power as well as privacy since the online advertising market is extremely concentrated, with Google and Facebook having an 84% market share.[16] Both have grown their ad revenue sharply in the last decade, with Facebook growing by over 600% in the five years from 2012 to 2016. Both companies are hugely reliant on ad revenue, with Facebook collecting 97% of its overall revenue from ad spending, while at Google it accounts for 88%.[17]

The switch has therefore had a dramatic impact on our media organisations who used to fund a significant portion of their operations by selling advertising space. This model, which functioned well for over 100 years, has been decimated in the last few decades, and today, many organisations are struggling to ensure sufficient revenue to maintain their output as ad spending moves from media organisations to Facebook and Google. US presidents Donald Trump[18] and Barack Obama[19] do not have much in common, but both relied heavily on digital campaigning and have shown how the tools created for the world of adverts have been repurposed to influence our democratic system.[20]

1.1.1 THE SOCIETAL PROBLEM

We now live in a world where, unless we take active measures to prevent it, our everyday activity on the Web will continue to be recorded and tracked, with massive international companies compiling it all into detailed profiles. Our digital selves then become marketable products with advertisers able to pay tech giants and website owners to place adverts in front of us. This has created a huge incentive for these tech giants, as well as a myriad of smaller companies, to try and gather as much information about us as possible. They do this to be able to nudge and influence our decisions and behaviour to meet their own ends.

Advertisers and their marketing consultants are also seeing this as an arms race. They need to constantly develop new techniques to get our attention since we, as users, develop resistance to certain types of advertising over time. The first banner ad, placed by AT&T on Wired.com, had a 44% click-through rate, while a similar ad today would get only 0.06%.[21] And so the sector has evolved. It now uses superficial data collection on people, allowing them to personalise adverts. This has created the phenomenon of 'ad nauseam', where a product you have recently bought stalks you for weeks across the Internet. The industry knows this is a problem and believes in a future where:

> "Ads need to be bespoke […] created in real time and tailored to the individual […] [using] advanced neural networks, deep-learning and large data sets to produce insights and then rapid decisions about what advertisement should be served."[22]

Companies are starting to combine data they collect through the use of cookies[23] and existing digital profile data available from data brokers with contextual, real world data about weather, relevant events, and social media data to understand when we are most susceptible to an advert. They will then be ready to place a tailored message targeting our vulnerability or need.[24]

This is a fundamental driver of the practice of collecting as much data on us as possible so that companies can monetise it by showing us adverts. Whole companies and digital products are being built solely around this principle – indeed any free app that we have on our phone or computer is relentlessly gathering data about us, selling it to data brokers, in some instances creating their own profile of us, while delivering us personalised adverts. The reason that we should care about this is clearly articulated by this statement by the organisation Don't Spy on Us:

> "Our right to privacy forms the bedrock upon which all of our other rights and freedoms are built. The Lords Constitutional Committee (2009) agreed that: 'Mass surveillance has the potential to erode privacy. As privacy is an essential pre-requisite to the exercise of individual freedom, its erosion weakens the constitutional foundations on which democracy and good governance have traditionally been based in this country.'"[25]

1.1.2 TECHNICAL PROBLEM

Twenty-five percent of ad spend is lost to fraud,[26] with experts labelling it "one of the most profitable crimes with the least amount of risk".[27] Fifty-six percent of adverts will never be seen by a human.[28] Ad fraud often uses a technique known as domain spoofing which uses unknown websites, owned or compromised by criminals, to place ads which they then drive traffic to using botnets (collections of computers controlled by malicious code) and other tricks. Edward Snowden has also warned that the way that adverts are served, often allowing remote computers to access Flash software to display them, can also be a security risk and that "using an ad-blocker is not just a right but a duty".[29]

The ad tech industry is potentially exposing every person who uses the Internet not only to fraud but also to the non-consensual, and often unwitting, sharing of their data with thousands of companies who are all able to copy, share, and sell the data on again. The now infamous political consultancy Cambridge Analytica used to be one of many companies that had access to this stream of personal user data. It was accused of using Facebook profile data without permission to create a system to target specific voters in the USA. A recent case against tiny French data broker CNIL found that it had illegally collected over 24.7 million records of people and their geolocation and almost 43 million other pieces of personal data through the bid process.[30,31] This practice is illegal because those receiving bid requests are not allowed to collect and record the personal data they receive; they can only use the data to bid in real time to place an advert. Because of the obvious challenge of identifying if and when advertisers are actually recording the data they receive, we believe that the case against CNIL represents only the very tip of a massive iceberg.

The bid request during the auction process totally fails to ensure the protection of personal data against unauthorised access. As already explained, when you click on a link to a page, between you clicking and the page loading, information about you is compiled and sent out as a bid request for advertisers to assess the value of showing you an advert. However, these requests broadcast more data than is justified for advertising purposes, and can include sensitive information such as sexuality, ethnicity, or political opinions.

Cases brought by Brave[32] and Privacy International[33] to the Information Commissioner's Office (ICO) are now forcing the industry to confront the way in which data is shared in this space.

1.2 GENERAL DATA PROTECTION REGULATION

The GDPR is an important international development in the regulation of data and the protection of people, but it does not address the question of power dynamics and is primarily focused on "individual control over data flows".[34] The GDPR's main route for maintaining any accountability over the companies that collect and exploit our data is limited because it focuses too heavily on individual actions, like giving consent or lodging a complaint with the ICO. The GDPR should not, therefore, be considered a panacea to all our concerns about data, privacy and power.

The GDPR has a number of key flaws:

- It places an overwhelming burden on the individual to take action.
- It requires a review of complex terms and conditions which individuals in practice don't have the time to read and/or can't understand.
- Accountability is undermined by allowing justifications such as 'legitimate interest' or 'necessity' to be used by data collection companies.
- It doesn't protect metadata or inferred data, despite the ability of both to identify individuals.
- It doesn't adequately control on-sell of data between firms.
- It leaves open the risk of fraud and misuse of data by leaving the storage and encryption of the data in the hands of the company, not the individual.

The GDPR has given us a framework to challenge the unauthorised sharing of personal data. But at a more fundamental level, while it addresses privacy issues, it does not address the issue of power in the data economy generally, and the ad tech sector specifically.

If we are to dismantle the structures that create tech monopolies and pose a threat to society, we shouldn't limit our judgements regarding data processes to whether they are GDPR compliant. As legal scholar Frank Pasquale highlights, accountability in the digital economy should question whether these tools should be developed at all and, at the very least, what limits should be placed on their use and commercialisation.[35]

This paper looks at two types of intervention:

- A series of interventions to address the current limitations of, and to go beyond the GDPR.
- An intervention which bans the sharing of personal data for advertising and addresses one of the main roots of the concentrated digital power in the hands of Google and Facebook, as well as the commodification of our digital selves, and of the Internet itself.

2. GOING BEYOND GDPR

Data protection legislation – which is actually concerned with the protection of *people* rather than data – is premised on notions of individual agency and consent. This cannot work if users don't understand, or don't take the time to read the terms and conditions they are signing up to. Reports show that most people don't read the long list of terms and conditions they accept when signing up to new digital services.[36] Twenty-five percent of people are unaware that the monetisation of their personal data forms the core digital platform business model, while 45% are unaware the companies use that data to provide personal ads.[37]

Data should be gathered and shared on the basis of consent from the data subject, with exceptions in certain sensitive cases like criminal proceedings or national security. However, relying on individuals to read and understand the multitude of terms and conditions that we accept without consideration every day is unrealistic, unproductive, and uneconomic. To take one example, if everyone who installed Flash, a software program to deliver animations and applications, read the licence agreement, it would consume 1500 person years of effort every day, 24 hours a day.[38] Imagine how that would scale if we took into account all the digital agreements we enter into every day. This leaves us with a dilemma to resolve: How can we effectively rely on consent to protect people from data exploitation?

The interventions we propose seek to create conditions where our data is never collected, shared, or sold without us giving our consent. The solution lies in ensuring that people are protected by default, as well as reducing the overall amount of data being collected. This should result in fewer circumstances where our consent is needed; and where consent *is* needed, it should be easier to understand what we are consenting to. We should also encourage innovative companies, public sector organisations, and the voluntary sector to consider developing and implementing collective forms of consent.

2.1 PRIVACY BY DEFAULT

An effective foundation would be to mandate the design practices of **privacy by default** and **privacy by design**. These principles would dictate that our online interactions, as well as our devices and software, would be

automatically set to not collect, share, or sell on our personal data. We would then have a series of options and tools that we could use to change this default setting to specify which third parties could gather data on us securely and for what purpose. This would help reduce the vast quantity of data being gathered all the time, which in itself is a risk to companies and data subjects.

2.2 RETHINK CONSENT

Even with both design practices being required by legislation, companies would still be asking us to consent to allow our data to be collected. We therefore need to **re-think consent**. At a minimum, if we want to stick with our individualistic model, then when consenting to data collection and sharing, the terms and conditions of any website or service provider should make it clear, in an easily digestible graphic or table, exactly what data is being collected about us, whether it is personally identifiable and who it may be shared with or sold to. To facilitate understanding, the means of displaying the information should be **standardised and consistent**, showing exactly what data is being collected and whether it is being sold or shared with other companies.

The possibilities here are for us to **crowdsource reviews** of terms and conditions to help highlight problematic conditions and open up the potential of collective bargaining for change. When Facebook's internal company documents were published by the UK Parliament in late 2018, people started dissecting the documents and associated terms to help interpret them.[39] Imagine if this was standard for all major sites with the results publicly available and easily digestible. Unacceptable conditions would quickly surface and collective action could be mobilised.

Another way forward could be to consider giving our **consent by proxy** through trusted individuals or groups, perhaps for a small fee. Here individuals with specific knowledge or skills would review site's terms and be empowered to give consent on our behalf. Different groups would emerge with different appetites for sharing data as well as other criteria.

2.3 RESTRICT THE USE OF LOOPHOLES

The protection of people should be prioritised over corporations' business models by **restricting the use of loopholes**. Legislatures have tended to resolve the difficulties of requiring consent for all data collection and processing by granting the data industry sweeping justifications it can use to override consent requirements. This has resulted in a situation where many tech companies exempt themselves from requiring data subject consent through the 'legitimate interests' justification contained within

the GDPR. 'Legitimate interests' is the most flexible lawful basis for processing data and can be the company's own interests or the interests of third parties. These interests can include commercial interests, individual interests, or broader societal benefits. Facebook invokes "necessity for performing a contract" as a legal basis for targeting ads to its users,[40,41] while Google still collects your location even after you ask it not to, seemingly in contravention of the GDPR.[42] Legislatures should prioritise the interests of people over corporations when tackling the data economy, with data sharing subject to collection and analysis on the condition that consent has been freely given; is specific, informed, and unambiguous; and is easily rescindable. Companies, like Facebook, should not be able to rely on these blanket justifications to process data.

2.4 BAN THE SHARING AND SELLING OF DATA BETWEEN COMPANIES

We recommend that **data sharing and selling between companies without the consent of the data subject be banned**, whether in the same company family (like Google and YouTube) or totally separate. This practice can involve sharing large data sets which companies use to create profiles about us and is often done on the basis not of consent but as a 'legitimate interest' of the business. We would bring an end to this by restricting the sale of third party access to our data to cases where we have given our explicit consent to grant that specific third party access. This is an area that the ICO is investigating, saying that it is particularly concerned with the "purchasing of marketing lists and lifestyle information from data brokers[43] without sufficient due diligence, a lack of fair processing, and use of third party data analytics companies with insufficient checks around consent."[44] The ICO has already taken action against some of the smaller UK-based data brokers.[45,46] Other action to address this risk includes Privacy International's filing with French, Irish, and UK data protection authorities against seven data brokers, ad tech companies, and credit referencing agencies.[47]

3. BANNING THE SHARING OF PERSONAL DATA FOR ADVERTISING

The current auction process is not fit for purpose because it totally fails to ensure the protection of personal data against unauthorised access. This creates massive incentives for a digital panopticon, as companies collect every data point that we produce to build huge profiles of us only to show us adverts. The huge risk to us and our data is not worth the meagre reward for advertisers and the intermediaries like Facebook and Google.

We need new legislation to change the information that is permitted to be sent out by website owners seeking to have adverts placed on their site. Instead of sending lots of personal information about us to the advertising network, we propose that **nothing personally identifiable should be sent**. This would immediately stop the massive leaking of our personal information, diminish the power of the tech giants, and remove one of the major incentives for pervasive data gathering.

To ensure that the advertisers still have enough relevant data to allow them to decide whether to place a bid to show an ad, the bid request could still contain some information covering the features of the website. Website owners may want to include additional information in the bid request, such as keywords outlining what they cover, and potentially even some aggregated demographic information about their website. This should allow advertisers to understand what kind of person they may be placing an ad in front of. It would mirror much more closely the way that adverts are (still) placed in print publications, based on the advert's target audience matching the target audience of the publication or service.

In addition, the government should ban all website owners from selling ad space on their own sites using personal data with anything less than explicit consent, regardless of any other justification. These sites would be required to make the full profiles that the advert is based on accessible to us. We would be able to correct any data contained in the profile as well as withdraw consent for our information to be used for targeting purposes.

We need to act quickly before future legislation embeds these harmful practices while removing our control and denying accountability. The

new e-privacy regulations currently under discussion in the EU contain a worrying suggestion in recital 21 which would allow those wishing to personalise advertising to rely on the blanket exemption "necessary for providing a service."[48] This could mean that it would operate outside of any consent mechanism and that, even if we withdrew consent, they would be authorised to continue to use our personal data.

3.1 EFFECTS

The proposed solution would be transformational as it would:

1. **Tackle data leaks.** One of the largest sources of personal data leaks would be instantly stopped. Since no personal data would be transmitted during the bid request, there would be no opportunity for those receiving the bid requests, such as companies like Cambridge Analytica, to harvest that data and link it to profiles they are building on us.

2. **Reduce the commodification of personal data.** It would diminish one of the major reasons for collecting personal data, which is to sell on to brokers in order to develop sophisticated profiles to enable advertisers to target us.

3. **Force tech giants to diversify their business models.** Since the largest tech companies also hold some of the most detailed profiles about us and dominate the ad tech space, they would need to think of another business model to adapt to the new privacy-respecting advertising model. It would greatly reduce the value of the profiles that they hold, since they could no longer be monetised for adverts. These tech giants would need to find other ways to monetise their services not based on constant surveillance and advertising.

4. **Redistribute power away from the tech giants.** It would return some power to those sites and companies who have spent time producing content and have a dedicated user base. In this new world, advertisers would once again be buying space based on the destination rather than the individual.

5. **Fight back against ad fraud.** Post-reform, adverts on fraudulent sites[49] would hardly generate any revenue, thereby reducing the incentive to engage in these kinds of scams.

4. CONCLUSION

Implementing our recommendations would create a radically different data economy. It would create a world where protecting *people,* rather than exploiting their personal data, would be the prime objective.

Our interventions, which strive to go beyond the GDPR, would address the current flaws and loopholes of the legislation. We could be assured that the software and hardware we use would be protecting us by default; consent would be better understood and informed; loopholes would be challenged; data we shared with one organisation could not be sold on multiple times to other organisations; and data shared at a corporate level, with the associated fraud risks, would be minimised.

The more fundamental and radical intervention of banning the sharing of personal information for online advertising would not just stop the leaking of personal data but also radically reshape the data economy itself. It would address the commodification of personal data and require a new business model for the tech giants by challenging the monetisation of a service through the sale of personal data for advertising. It would simultaneously restore power to those who create good content online. Finally, it would address at its root the risk of fraud inherent in the ad tech system.

Only by resetting the terms on which we engage with the data economy can we hope to build a positive digital future where we can be confident that our privacy will be protected, and where we are able to navigate freely without being surveilled.

ENDNOTES

1 1x1018 or 1 billion billion or 1000000000000000000

2 Jacobson, R. (2013, April 24). 2.5 quintillion bytes of data created every day. How does CPG & Retail manage it? IBM Consumer Products Insight Blog. Retrieved from https://www.ibm.com/blogs/insights-on-business/consumer-products/2-5-quintillion-bytes-of-data-created-every-day-how-does-cpg-retail-manage-it/

3 Rudinow Sætnan, A., Schneider, I., & Green, N. (Eds). (2018). *The Politics of Big Data: Big Data, Big Brother?* Oxford: Routledge.

4 Citron, D. K., & Pasquale, F. A. (2014). The Scored Society: Due Process for Automated Predictions. Washington Law Review, 89, 1. Retrieved from https://ssrn.com/abstract=2376209

5 Mai, J.-E. (2016). Big data privacy: The datafication of personal information. *The Information Society*, 32(3), 192-199.

6 Banwejee, S. (2018). Authorisation and access control architecture as a framework for data and privacy protection. Retrieved from https://arxiv.org/pdf/1801.05313.pdf

7 Coustick-Deal, R. (2015, December 4). Responding to Nothing to Hide, Nothing to Fear. Open Rights Group Blog. Retrieved from https://www.openrightsgroup.org/blog/2015/responding-to-nothing-to-hide-nothing-to-fear

8 Schneier, B. (2006, May 19). The value of privacy. Schneier on Security Blog. Retrieved from https://www.schneier.com/blog/archives/2006/05/the_value_of_pr.html

9 Calo, R. (2014, August 15). Everyone knows that privacy is about power. Now what?'The Center for Internet and Society Blog. Retrieved from http://cyberlaw.stanford.edu/blog/2014/08/everyone-knows-privacy-about-power-now-what

10 Pasquale, F. (2018, May). Our lives in a scored society. *Le Monde diplomatique*. Retrieved from https://mondediplo.com/2018/05/05data

11 Handley, L. (2017, December 4). Half of all advertising dollars will be spent online by 2020, equaling all combined'offline'ad spend globally. CNBC. Retrieved from https://www.cnbc.com/2017/12/04/global-advertising-spend-2020-online-and-offline-ad-spend-to-be-equal.html

12 Soper. S. (2018, September 19). Amazon increases ad market share at expense of Google, Facebook. Bloomberg. Retrieved from https://www.bloomberg.com/news/articles/2018-09-19/amazon-increases-ad-market-share-at-expense-of-google-facebook

13 Andrews, E. (2018). Rigged auctions? Why top bidders don't always feel like winners. Insights by Stanford Business. Retrieved from https://www.gsb.stanford.edu/insights/rigged-auctions-why-top-bidders-dont-always-feel-winners

14 Based on own calculations multiplying: number of UK Internet users X average number of page visits per day X avg number of ads per page X prevalence of ad blocking X use of real time bidding system

15 McCann, D., & Hall, M. (2018). Could this be the end of the wild west of targeted ads? *Huffington Post*. Retrieved from https://www.huffingtonpost.co.uk/entry/could-this-be-the-end-of-the-wild-west-of-targeted_uk_5b9bc95de4b055e62531811d

16 Garrahan, M. (2017, December 4). Google and Facebook dominance to rise. *Financial Times*. Retrievent from https://www.ft.com/content/cf362186-d840-11e7-a039-c64b1c09b482

17 Desjardins, J. (2017, May 12). Here's how 5 tech giants make their billions. *Visual Capitalist*. Retrieved from https://www.visualcapitalist.com/chart-5-tech-giants-make-billions/

18 Beckett, L. (2017, October 8). Trump digital director says Facebook helped win the White House. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2017/oct/08/trump-digital-director-brad-parscale-facebook-advertising

19 Bogost, I. (2017, January 6). Obama was too good at social media., *The Atlantic*. Retrieved from https://www.theatlantic.com/technology/archive/2017/01/did-america-need-a-social-media-president/512405/

20 Nadler, A., Crain, M., & Donovan, J. (2018, October 17). Weaponizing the digital influence machine: the political perils of online ad tech. *Data & Society*. Retrieved from https://datasociety.net/output/weaponizing-the-digital-influence-machine/

21 Greenfield, R. (2014, October 27). The trailblazing, candy coloured history of the online banner ad. *Fast Company*. Retrieved from https://www.fastcompany.com/3037484/the-trailblazing-candy-colored-history-of-the-online-banner-ad

22 Jivox. (2017). Personalised advertising wins. Raconteur. Retrieved from https://www.raconteur.net/sponsored/personalised-advertising-wins

23 A small text file (up to 4KB) created by a website that is stored in the user's computer either temporarily for that session only or permanently on the hard disk (persistent cookie). Cookies provide a way for the website to recognize you and keep track of your preferences.

24 Jivox. (2018). Omni Channel Personalisation Benchmark Report. Retrieved from https://www.jivox.com/wp-content/uploads/2018/04/Omni-channel-Personalization-Benchmark-Report.pdf

25 Don't Spy on Us. Website. Available at https://www.dontspyonus.org.uk/

26 PPC Protect. (2018). The Ultimate list of click fraud and ad fraud statistics 2018. Retrieved from https://ppcprotect.com/ad-fraud-statistics/

27 Silverman, C. (2018, November 27). 8 people are facing charges as a result of the FBI's biggest ever ad fraud investigation. *Buzzfeed News*. Retrieved from https://www.buzzfeednews.com/article/craigsilverman/3ve-botnet-ad-fraud-fbi-takedown

28 Kantrowitz, A. (2014). 56% of digital ads are never seen, says google. Adage. Retrieved from https://adage.com/article/digital/56-digital-ads-served-google/296062/

29 Lecher, C. (2015, November 12). Edward Snowden says using an ad-blocker is 'not just a right but a duty'. *The Verge*. Retrieved from https://www.theverge.com/2015/11/12/9723314/edward-snowden-ad-blocking

30 Kruzer, R. (2018, November 21). Why a French ruling against a small mobile ad firm has ad tech on the defensive. *Marketing Land*. Retrieved from https://marketingland.com/why-a-french-ruling-against-a-small-mobile-ad-firm-has-ad-tech-on-the-defensive-252090

31 CNIL Court Decision n°MED-2018 042, (30 October 2018)
Retrieved from https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000037594451&fastReqId=974682228&fastPos=2

32 Submission to the Information Commissioner from Brave. (2018). Retrieved from https://brave.com/ICO-Complaint-.pdf

33 Privacy International. (2018, November 8). Our complaints against Acxiom, Criteo, Equifax, Experian, Oracle, Quantcast, Tapad. Retrieved from https://privacyinternational.org/advocacy-briefing/2426/our-complaints-against-acxiom-criteo-equifax-experian-oracle-quantcast-tapad

34 Morozov, E. (2014, August 10). Facebook invades your personality, not your privacy. *Financial Times*. Retrieved from: https://www.ft.com/content/dd5e5514-198d-11e4-8730-00144feabdc0

35 Pasquale, F. (2018, August 20). Odd numbers. *Real Life*. Retrieved from https://reallifemag.com/odd-numbers/

36 Berreby, D. (2017, March 3). Click to agree with what? No one reads terms of service, study confirms. *The Guardian*. Retrieved at https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print

37 Doteveryone. (2018). People, Power and Technology: the 2018 Digital Attitudes Report. Retrieved from http://attitudes.doteveryone.org.uk/files/People%20Power%20and%20Technology%20Doteveryone%20Digital%20Attitudes%20Report%202018.pdf

38 Perzonowski A. & Schultz J. (2016) The End of Ownership: Personal Property in the Digital Economy. MIT Press

39 WolfieChristl. (2018, Dec 6). [Twitter Post]. Retrieved from: https://twitter.com/WolfieChristl/status/1070695293967130632?s=03

40 @fborgesius. (2018). Checking out Facebook's new terms & conditions (a small thread). Facebook seems to invoke necessity for performing a contract (art 6(1)(b) GDPR) as a legal basis for targeting ads to its users.. Retrieved from https://twitter.com/fborgesius/status/990677575407226881?s=03

41 Facebook does use consent from users for some other purposes, such as data collection.

42 Associated Press. (2018, August 13). Google records your location even when you tell it not to. The Guardian. Retrieved from https://www.theguardian.com/technology/2018/aug/13/google-location-tracking-android-iphone-mobile

43 A Data Broker is a business that aggregates information from a variety of sources; processes it to enrich, cleanse or analyse it; and licenses it to other organisations. Data brokers can also license another company's data directly, or process another organisation's data to provide them with enhanced results.

44 Privacy international. (2018). Submission to the Information Commissioner. Request for an assessment notice of data brokers: Acxiom & Oracle (the'data brokers'). Retrieved from https://privacyinternational.org/sites/default/files/2018-11/08.11.18%20Final%20Complaint%20Acxiom%20%26%20Oracle.pdf

45 Information Commissioner's Office Press Release. (2017, November 1st). Verso Group Limited, retrieved from https://ico.org.uk/action-weve-taken/enforcement/verso-group-uk-limited/

46 Information Commissioner's Office Press Release. (2018, August 8th). Emma's Diary fined £140,000 for selling personal information for political campaigning. Retrieved from https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/08/emma-s-diary-fined-140-000-for-selling-personal-information-for-political-campaigning/

47 Privacy International. (2018). Our complaints against Acxiom, Criteo, Equifax, Experian, Oracle, Quantcast, Tapad. Retrieved from https://privacyinternational.org/advocacy-briefing/2426/our-complaints-against-acxiom-criteo-equifax-experian-oracle-quantcast-tapad

48 @MalteEngler. (2018). Wow, this is big: The new recital 21 states that processing of data for ads (e.g. via cookies) can sometimes fall under"necessary for providing a service". This is a worrying concession to demands from digital ads industry, hugely watering down the concept of "necessity". Retrieved from https://twitter.com/MalteEngeler/status/1053686542491881473?s=03

49 Sites, often with lots of clickbait, that are set up solely to get ads placed so that bots, and sometimes humans, can be used to extract revenue from placed adverts.

50 Watt T, Varrow M et al (2018) Social care funding options https://www.health.org.uk/publication/social-care-funding-options

NEW ECONOMICS FOUNDATION

WWW.NEWECONOMICS.ORG
info@neweconomics.org
+44 (0)20 7820 6300 @NEF
Registered charity number 1055254

WRITTEN BY:
Duncan McCann and Miranda Hall

COVER IMAGE:
iStock.com/peterhowell

PUBLISHED:
December 2018

ACKNOWLEDGEMENTS:
Thanks to the Joseph Rowntree Charitable Trust for funding NEF's work on the digital economy.