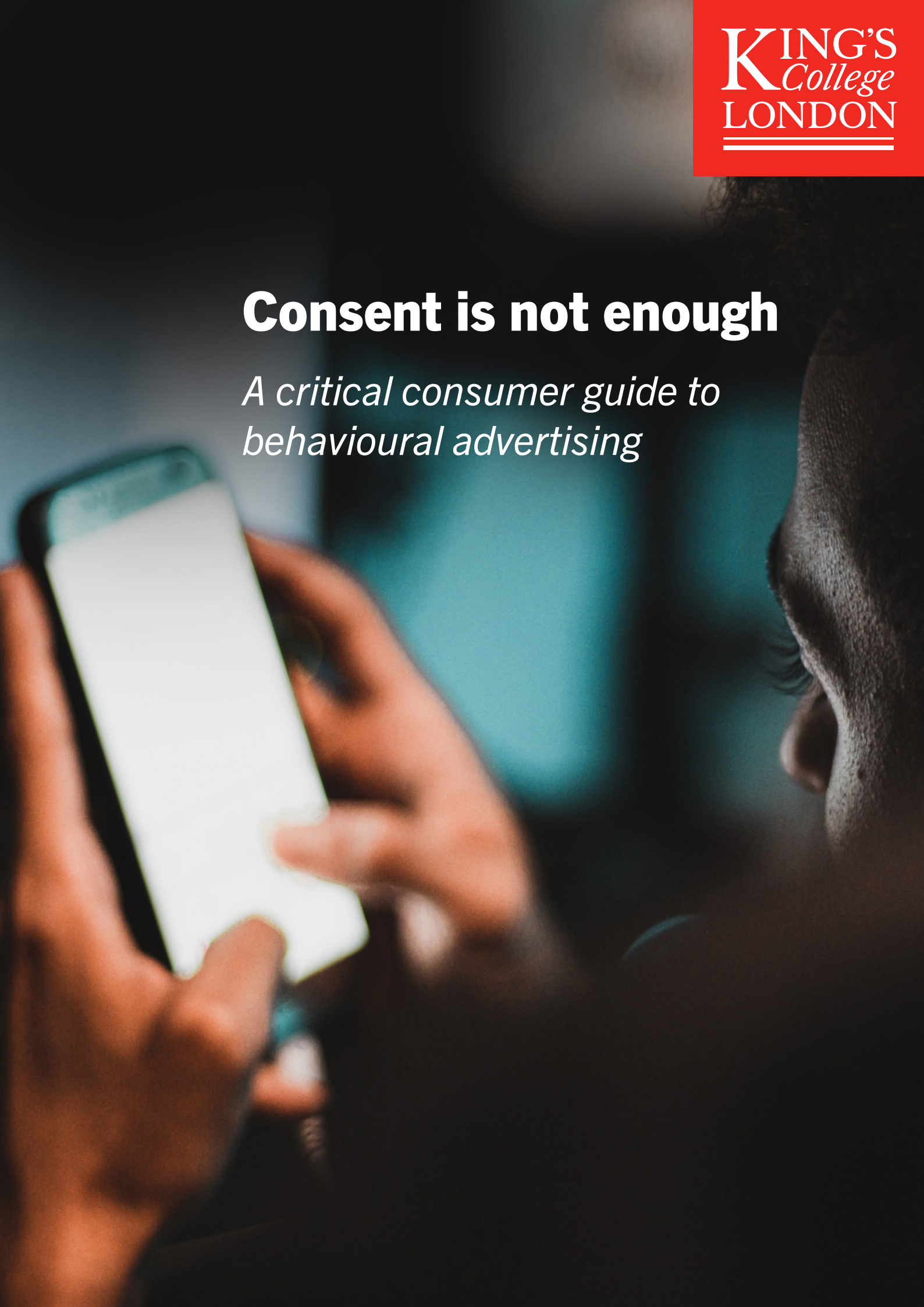
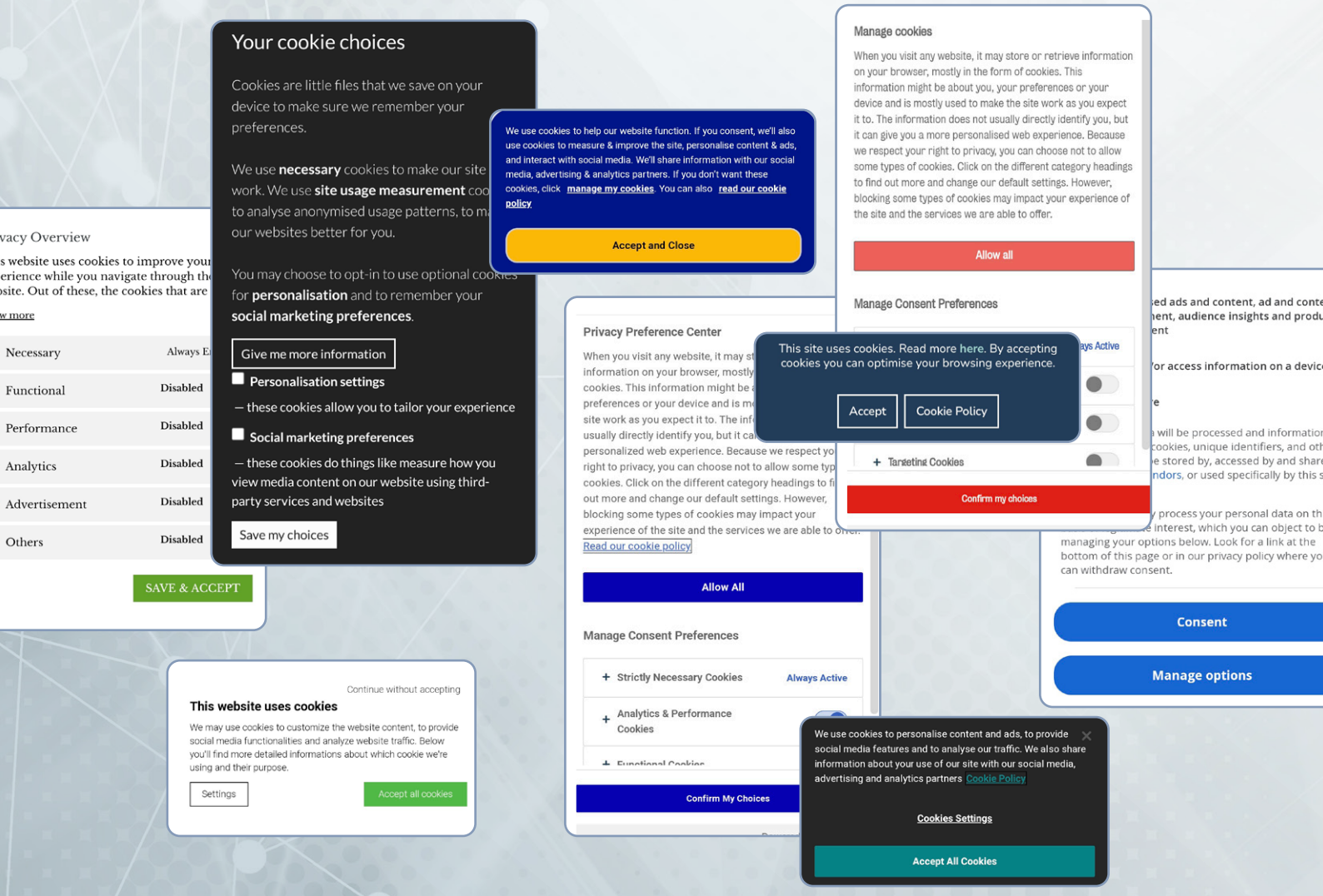


Consent is not enough

A critical consumer guide to behavioural advertising

KING'S College LONDON

Contents



What is behavioural advertising?

During your afternoon work break in London, you open the UK Amazon website on your Chrome browser. On the landing page, you see a pop-up banner with two buttons, a yellow 'Accept Cookies' button and a white "Customise Cookies' button. Short of time, you click the yellow button. But what is it exactly that you are accepting? And how does this choice matter?

On your computer, this system has typically made use of **cookies** when you are using a browser, like Chrome. These are text files with small pieces of data that are used to identify your computer online and track your activities.

The banner is a part of an online system of **behavioural advertising**, or **AdTech**, where the advertisements you see on webpages are based on your behaviour. When you click "accept all", you are agreeing that data derived from your online activities can be used to select the ads you see.

Of course, this not only happens to you. Behavioural advertising relies on constant streams of data about many millions of consumers as they use browsers to visit websites or use apps.

On your phone, the apps that are pre-installed, or that you have installed, use so-called **SDKs,** Software Development Kits, that can share your data as you use the app – sometimes even with the app running in the background. A single app can host dozens of SDKs.

What happens when you see an ad appear is the result of **Real Time Bidding**. The ads you see are served by an advertiser who has outbid competitors to serve that ad through an automated bidding process that happens instantaneously when you arrive at a website or open an app.

Who is tracking me?

Who exactly is collecting and processing all this data?

While the AdTech system is notoriously complicated with hundreds of businesses performing different functions at any moment, it is helpful to make a basic distinction between **first parties** and **third parties.**

First parties are the online services you directly interact with – the UK Amazon site in our example. First party data includes not only the data you volunteer (like your email to login) but also what is observed from your actions (like which webpages you click on, whether you scroll to the end of a page, and where and how you move on to another webpage) as well as algorithmic inferences made using your data, such as your likely interests or tastes.

Third parties are all parties outside the first party relationship – which includes the advertisers who want to place on ad on the first party website or app to reach an audience. Of course, an online business can be both. Facebook, for example, is a first party service for Facebook users, but also tracks Facebook users and non-users across the internet as a third party. Third parties also use algorithmic inferences to profile you based on the data they collect about you.

What happens to your data once it's in the wider online advertising system is hard for anyone to understand completely – streams of data about millions of individuals are processed by a multitude of businesses. So-called **data brokers**, for example, collect personal data to sell or license on to third parties for a variety of uses. They may purchase your data that was collected for one purpose and then repurpose it for another. First party service providers may also engage in data broking, selling or sharing personal data they collect with third parties.

What is the bigger picture?

This unprecedented sharing of personal data with innumerable third parties has drawn a lot of attention from privacy organisations and regulators with major investigations underway and some **big fines** already levied for violating data privacy.

But we need to keep in mind that AdTech is just one expression of **personalisation**. The bigger story beneath the Adtech crackdown is the pervasive personalisation of services online and, increasingly, in the rest of our lives – in homes, workplaces, vehicles, and elsewhere.

Without a constant flow of their users' data, many of these personalised services cannot operate effectively or at all. Instagram or TikTok, for example, would be an unnavigable ocean of content without its recommender systems.

What's more, we have come to expect that many online services, such as social media, are 'free', without questioning whether we are in fact **'paying with our data'**.

There are a lot of risks involved in this expanding process of personalisation:

- **Loss or theft** of your data once it is in the hands of other parties;
- The **chilling effects** of constant and opaque **commercial surveillance** and its potential links with **state surveillance**;
- Unjustifiable **bias or discrimination** based on algorithmic profiling;
- **Deceptive manipulation** – including deliberately confusing online interfaces (**'**dark patterns**'**) designed to obtain consumer consent or targeted **'disinformation'** designed to interfere in democratic decision making.

> The personalisation of ordinary human life is increasing all the time: think of digital assistants like Siri, the Internet of Things ('smart' devices or machines that share data online), or the potential for 'metaverse' applications (3D virtual worlds focused on social connection). Driven by artificial intelligence and constant surveillance of individual behaviour, the personalisation of devices and services will grow.

In short: AdTech delivers personalised advertising within a complex system of **other personalised services**. Quite often personalised advertising is integrated into personalised services. In combination, they are challenging basic notions of human autonomy.

What is happening with regulation?

Over the past decade, there has been a major effort to bring AdTech's third party tracking and targeting under control. Regulators have determined that consumers are not being properly informed about how their data is used or by whom, nor are they being given fair opportunities to refuse their consent to these uses. In short, Adtech is failing to ensure proper **'notice and consent',** as required by data protection laws around the world.

UK and EU – Current regulation is based on the General Data Protection Regulation (GDPR) and the ePrivacy Directive. In the EU, further restrictions on Adtech are probable in upcoming EU legislation and the European Data Protection Board also provides important guidance about lawful and unlawful uses of personal data. In the UK, the Information Commissioner's Office (ICO) is the data protection regulator.

Just as important as regulatory interventions, the big tech companies that provide the operating systems, web browsers and platforms that have enabled third party AdTech tracking are making changes that are starting to limit third party access to your data.

These innovations mean that, as third-party access declines, **first party data** is becoming more important than ever. The big players, who by far collect and hold the most first party data, are likely to get bigger.

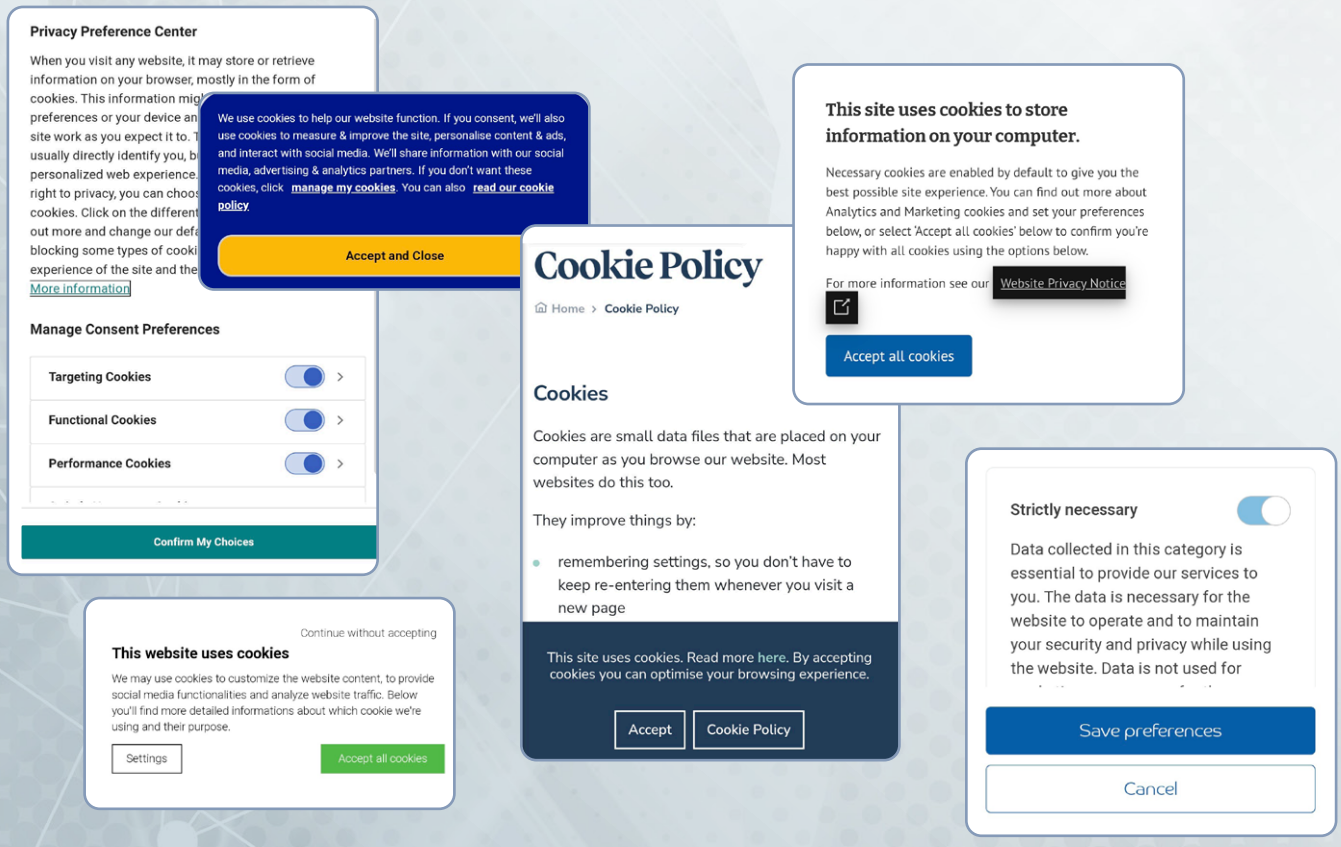
USA – While consumer data protection in the United States has lagged behind the UK and EU, a new wave of data privacy laws at the state level has radically changed the situation, including the influential California Consumer Privacy Act (CCPA). The Federal Trade Commission also has important enforcement powers.

China – Regulatory intervention by government authorities to protect consumers in China's highly sophisticated digital economy is steadily improving, strengthened by the new Personal Information Protection Law (PIPL).

Apple has also expanded its privacy measures: Its mobile operating systems (iOS) are giving iPhone and other Apple device users options to block much third party access for advertising purposes.

Google has announced it wants to block third party tracking cookies from using its Chrome browser (delayed to 2023); Firefox and Safari already block them. Google's plans have changed a lot, but the company currently intends to use the Topics API, which picks "topics" based on your browsing behaviour each week. These topics are only stored on your own device for three weeks and cannot be used to find out who you are. This would allow third party advertising to become "anonymized". Google has also announced future changes to Android mobile operating system to make it easier to refuse third party tracking.

Facebook and **Alibaba Taobao** have also introduced new business practices that restrict direct third party access to their huge first party personal data resources.



Who is in control?

Unfortunately, data protection law was **not designed** to deal with personalised services running on big data and artificial intelligence. Despite improving regulatory enforcement and structural changes introduced by big tech companies, it often seems that we are running to stay in the same place, if not steadily losing ground – trading away our data for innovations in personalised services.

Like consumer law generally, data protection law assumes that, if you are given the right information and the right options, you can **control** how much you are tracked and what personalised advertising you receive. It is the taken-for-granted way of **legitimising** the data collected from you and the inferences made about you.

However, **notice and consent** can be manipulated in lots of ways. For instance:

Too little information about where your data goes is a problem, but too much information can be just as confusing. Web pages and apps can **overwhelm** us with excessive information about privacy choices.

Your consent to first party data collection may reach **other businesses within that first party** that you don't realise are connected, especially when it's a multi-service company, such as Alphabet (Google's owner), which operates YouTube, or Meta (Facebook's owner), which operates Instagram and Whatsapp. In China, the tech giant Alibaba operates diverse online businesses, including the popular location service Amap and the collaborative communication platform Dingtalk.

Websites and platforms can deny access to a free service if you refuse to consent to processing for advertising purposes or become a registered user with further consents required. Privacy is increasingly a **feature that can be bought**.

It takes extra time and attention to understand and make daily choices in these complex digital environments and most people do not have that time to spare. Even when the necessary information is presented fairly, we are often in a hurry and just **click the easiest option**.

Why ‘notice and consent’?

Remember those cookie banners we saw in London? You won’t see these if you had opened an Amazon.com website when in the United States or the huge Taobao retail website in China.

Aside from major commercial and cultural differences in the way websites and apps are presented to consumers, the **legal requirements** are not the same across different countries. Nonetheless, there are **striking similarities** in the way they ask to use your data. Just about everywhere, data protection laws require some version of ‘notice and consent’, sometimes referred to as consumer ‘opt in’ or ‘opt out’ rights.

With all these limitations on human capacities to navigate consent based permission systems, why is the **‘notice and consent’** model so dominant? The answer, quite simply, is that this model is built on intuitions we have had for centuries.

Imagine living at a time before the Internet and even before supermarket chains. Throughout the world, people went to local greengrocers, butchers and other shops or market stalls to make their regular purchases. These **shopkeepers and stallholders** knew a lot about their customers, including their purchasing preferences, and could use that knowledge to market their wares. “Would you like to try this one?” “Here, I kept this one specially for you.”

Whether people appreciated this accumulated knowledge being used to market or advertise products to them would naturally vary. But this everyday fact of life was based on **implicit consent**. (If you don’t like it, don’t come here.) A customer could not, after all, ask a shopkeeper not to observe and infer knowledge about her customers. That is just what human brains automatically do.

It would be rather different if a (first party) shopkeeper began telling other shopkeepers (third parties) about a customer’s purchasing preferences to help them market products to the same customer. For many people, that would be outside their **reasonable expectations** about the customer - shopkeeper relationship.

This **historic legitimacy** of shopkeeper or stallholder knowledge and marketing, based on implicit consent, that has led to the ‘notice and consent’ model now universally favoured as the basis for lawful behavioural advertising.

The big difference, of course, is that local shopkeepers or stallholders have largely disappeared into **vast, digitised retail systems** dominated by global businesses, which use advanced data analytics to observe and infer detailed knowledge about millions and millions of website and app users. Past experience is, as they say, not always a good guide to the future.

Are ‘bright patterns’ the answer?

Back to that ‘Accept All’ button we so often click. The interface itself is meant to nudge us towards data disclosure, with obvious preferred options and shaded or obscured alternatives. Naturally, most people know little about what happens to their data after they click and ‘consent’. And websites and apps often make it time consuming and difficult to find out.

Judged by this common experience, it seems that ‘notice and consent’ often fails to deliver the promise of consumer **agency** or **empowerment** in complex digital environments. One solution proposed by privacy activists and regulators is the use of mandatory standardised ‘notice and consent’ features in online interfaces, which are sometimes called ‘**bright patterns**’. Think of a standardised ‘**reject all**’ or ‘**opt out**’ button that all digital services would be required to put prominently in front of our eyes.

Eventually, such universal opt-out signals might work – although it is not yet clear what form of universal signal must be generated to be recognised by service providers as valid or how many different forms of these signals would be needed.

If workable, this kind of solution would certainly give consumers a reassurance that their first party data will not be shared with third parties for advertising purposes. On the other hand, clicking on a universal ‘reject all’ button does not provide any better understanding of the decision than clicking on an ‘accept all’ button. ‘Accept all’ versus ‘reject all’ often presents a simplified blind choice. Sometimes, we may want at least some personalised advertising.

What can I do?

The challenge of digital personalisation is much larger than the question of whether third parties have access to our data. Even if we would get rid of Real Time Bidding advertising systems, first party data collection and profiling is growing, and **ubiquitous personalisation** is here to stay.

Personalisation continues to spread through smart devices, vehicles and environments. Personalised digital assistants (a first party relationship) will tune in to your preferences from the moment you wake up. Your alarm clock will alert the kitchen to turn the coffee machine on, your Bluetooth speaker will know what music you want to hear as you have that coffee, and so on.

Crucially, a lot of these devices will be **advertising supported** – because that will make them affordable to many people. Buttons allowing you to "accept all" or "reject all" cannot prevent this personalised future. The **harder question** is not just about our privacy, but about how much control over our lives we will have left and how genuine control or autonomy should work in a heavily digitised future.

There are no easy solutions but doing nothing plainly means **progressive disempowerment**. Here are some things to consider doing:

- **Use the tools available.** Understanding digital services is not easy. On the other hand, a basic understanding of how your data is used to deliver personalisation is a digital survival skill. With a little knowledge, meaningful choices beyond 'reject all' or 'accept all' are possible.

  Know how to use the privacy settings on your iPhone or Android phone. Without the iPhone's more recent privacy controls, an Android phone might need some extra help. There are also practical ways to make your browser more privacy protective or you could choose a more privacy protective browser.

- **Privacy organisations** (for example: Privacy International, NOYB, EDRi and EFF) work to raise awareness of the opaque practices of behavioural advertising and to persuade regulators (such as the ICO) to take action. Their legitimacy depends on public engagement too. The ICO cookie reporting tool is a way for you to raise your concerns directly with the regulator.

- **New laws** directed at the harms caused by artificial intelligence, which is the engine that drives personalisation, offer one potential way forward. See for instance the UK National AI Strategy and important research institutes like Ada Lovelace and Alan Turing, which welcome public engagement. There is also important scrutiny in Parliament. Get to know what your MP is doing. Knowledgeable consumers should also be active citizens.

This report was authored by Perry Keller, Reader in Media and Information Law, King's College London and Dr Tom van Nuenen and Dr Li Yang, Research Associates, King's College London. The information used in this report draws on the final report for the King's College London 'After Third Party Cookies – Consumer consent and data autonomy in the globalised AdTech industry' research project, which was funded by the Information Commissioner's Office (ICO) research grants programme. (February 2022)