The ‘wild west’ of data: How UK councils share residents’ data with third party advertisers

BBC Local News partnerships

Mailbox I BBC Birmingham I B1 1AY

+44 (0)121 5676789 (Internal: 01-76789 or 01-76299)

shared.dataunit@bbc.co.uk

Contents

What's the story?

High-interest credit cards and Black Friday deals are among the adverts targeted at people seeking benefits advice on local council websites.

A BBC investigation found more than 950 advertising cookies - small text files that track people on the internet - embedded in council benefits pages.

Examples of targeted adverts on benefits pages seen by the BBC include high-interest credit cards, Black Friday deals, sports cars with features for disabled people and private funeral care plans.

The Information Commissioner's Office (ICO), an independent body set up to uphold information rights, said the setting of non-essential cookies without consent would be illegal.

It said it would look into the findings.

The advertising industry has denied using data from vulnerable residents.

Our investigation found:

- Some 54% of councils hosted third-party advertising cookies on their benefits pages
- Around 950 third-party advertising cookies on benefits pages
- More than two thirds of councils do not appear to ask for the correct form of consent under current privacy laws
- Google has previously said that it would phase out third-party cookies within the next two years on websites accessed via its Chrome browser, in response to calls for greater privacy controls

What are cookies?

Cookies are small files of text that are often used to track users around the internet. They attach themselves to our browsers when we open web pages, and are the main technology used to gather data for targeted and behavioural advertising.

Many cookies are essential and are used to improve the browsing experience. They are used for audience measurement, hosting and website design.

Third-party advertising cookies help companies deliver ads that are relevant to your browsing habits.

Before cookies are placed on a user's browser, a publisher must ask for and be given legal consent from the user under the PECR (Privacy and Electronic Communications Regulations).

A pre-ticked box on a website is not enough. The user must be offered an active decision to accept or decline cookies when they first land on a website.

What we did:

We used an open-source tool called Webxray to scan 405 council homepages and 368 council benefits pages (all the councils that had those pages) in the UK.

The tools returned data on third party advertising cookies embedded on browsers.

We also visited the benefits pages of each council website to determine what level of consent appeared.

We have allocated each council a traffic light colour based on the level of consent it sought from visitors to its benefits pages, where green represents the highest standard and red is the worst, with amber in the middle.

That colour is based on how each council's cookie consent pop-up aligned with the legal consent website publishers must obtain before non-essential cookies (such as third party advertising cookies) are placed on a user's browser - see Appendix 2 (the law) for more explanation of this.

Consent for tracking technology must be freely given, specific and informed, and involve *"unambiguous, positive action"* - such as ticking a box or clicking a link. A pre-ticked box is not sufficient to comply.

Our manual trawl of councils' benefits pages identified 21 descriptions we could apply to all of the differing cookies consents councils sought from visitors to their pages, which we matched to the colours as shown below.

Our BBC staff created this as guidance only to editors; it is not based on any official statements or guidance from data or privacy regulators.

pop up - active consent	GREEN
cookie icon - active consent	GREEN
pop up - only necessary assumed, active for analytics	AMBER
pop up - only necessary assumed, active for others	AMBER
pop up - assumed consent - only necessary used	AMBER
cookie icon - assumed consent - only necessary used	AMBER
cookie icon - assumed for necessary, others active consent	AMBER
pop up - assumed consent for analytics and necessary only	AMBER
pop up - assumed analytics - active consent others	AMBER
pop up - assumed consent analytics - active consent others	AMBER
pop up - pre-ticked box - unticked for marketing	AMBER
pop up - yes/no option	AMBER
pop up - pre-ticked box	RED
pop up - pre-ticked consent	RED
pop up - link to pre ticked box	RED
cookie icon - pre ticked box	RED
pop up - assumed advertising - active consent for analytics	RED
pop up - assumed consent	RED
cookie icon - assumed consent	RED
cookie icon - not working	RED
no	RED

What the experts said:

(More quotes in appendix)

Professor Tim Libert teaches in the privacy engineering programme at Carnegie Mellon University in the USA. He is the creator of the Webxray programme used in this investigation.

- "I've been a web developer since the late 1990s and a privacy researcher for the past seven years and this may be the most unexpected place I've seen an ad online."

- "Any evidence of deeper integration between the civil and commercial realms is cause for grave concern."

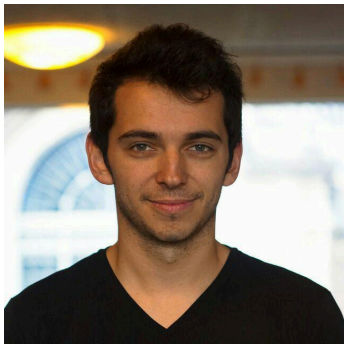
- "First and foremost, it is important to note that there is no way for a tracker to force their code onto a site short of hacking it - the site itself must place the code there. So the biggest party of responsibility is the website owner [councils] without question.

- "In my view, targeting residents through benefits pages is utterly reprehensible as the most protections should be extended to those most in need."

- "The ad-tech industry has spent the last 20 years making billions of dollars engaged in business practices which are consistently shown to be incredibly unpopular with the public.

- "At this point a final day of reckoning has yet to come, but laws like GDPR may be setting the stage for a fundamental realignment whereby the digital world will have to comply with the moral and ethical standards we've developed over centuries in the pre-digital era.

Eliot Bendineli is a technologist at Privacy International (PI)- a UK NGO focussed on privacy advocacy.



- "Having this type of profiling opens the way to control and manipulation. All of this really matters because these tools basically allow companies to have a good idea of who you are, where you live, what you're interested in, what you're doing this weekend, or if you have any mental health issues, for example."

- “When a company or a government has so much information about you, they can manipulate you. That’s what we’ve seen with Cambridge Analytica.”
- “Tracking people through benefits pages is sadly typical. It’s always the people that are already vulnerable who are going to suffer the most.”
- “The risk is that there is no control. It’s just an open way for manipulation.”

Lloyd Clark, managing director of the Council Advertising Network (CAN), which works with public bodies including around 50 UK councils and Transport for London (TfL) among others

- “We do not specifically target vulnerable people via council advertising. In addition, we automatically block all categories of advertising that could be used to target vulnerable groups. This includes ads for payday loans, gambling and alcohol.
- “What’s been built up is for the purpose that relevant information goes towards serving individuals’ relevant advertisements.
  “People appreciate relevant advertising. People don’t like irrelevant adverts.
  “But if they [advertising companies] are a bad actor, it’s certainly possible for them to behave like a bad actor.
  “That’s a general challenge for the way the technology has been put together, not with advertising per se.”
- “Given the tech furniture present right now we’re in a position where you need to really trust people because the system won’t work without it.
  “It creates a real challenge. We are reliant on people obeying the constraints that are set and the regulations that are out.
  “Unfortunately, we can’t rely on only good actors. Even the biggest can fall prey to doing immoral things. That’s what the industry is currently grappling with.”

Our findings - The UK picture:

Some **54% (199 out of 368) of councils** across the UK host third party advertising cookies through their benefits pages.

In total, the cookies were linked to **31 known companies** spread across 10 different countries (including the UK). Some 951 advertising trackers on benefits pages were found.

Some of the councils allowing third party advertising companies on their benefits pages include **Enfield, Southampton, Ealing, North Somerset, Torbay, Wirral, Redbridge, Sheffield, Solihull and Torfaen in Wales.** See our data for the full list.

- On average, five advertising cookies were found on council benefits pages.
- Countries the data were sent to include the US, Denmark, the UK, Canada, Belgium, Germany, Singapore, Sweden, Malaysia, Lithuania and Israel.

England:

Some **56%** (174 out of 312) of English councils host third party advertising cookies on their benefits pages.

The cookies were linked to at least 38 different companies in **10 countries**.

Some of the councils with the most third party advertising cookies on their benefits pages include **Enfield, Southampton, Ealing, North Somerset, Torbay, Wirral, Redbridge, Sheffield and Solihull.** See our data for the full list.

- On average, five advertising cookies were found on 56% of benefits pages. The total number of advertising trackers found was 804.
- DoubleClick - the advertising arm of Google - was the most-commonly-seen destination for this data
- Examples of data being shared include IP addresses, locations (latitudes and longitudes) and browser histories.
- Countries the data was sent to include the US, Denmark, the UK, Canada, Belgium, Germany, Singapore, Sweden, Malaysia, Lithuania and France.

Local Government Association (LGA) response:

Responding to the findings, an LGA spokesperson said: “Councils take legal compliance seriously and are looking into their use of cookies in relation to the findings.”

Wales:

Some 55% (12 out of 22) of Welsh councils showed evidence of advertising trackers on their benefits pages.

The cookies were linked to **at least 23** different companies in seven countries.

On average, **11 advertising trackers were found on 55%** of Welsh benefits pages.

Some of the councils allowing third party advertising companies to track residents through their benefits pages include **Torfaen, Monmouthshire, Blaenau Gwent, Swansea, Merthyr Tydfil** and **Vale of Glamorgan**. See our data for the full list.

- On average, 11 advertising trackers were found on 55% of Welsh benefits pages, the total number of advertising trackers found was 133.
- DoubleClick - the advertising arm of Google - was the most-commonly-seen destination for this data.
- Examples of data being shared include IP addresses, locations (latitudes and longitudes) and browser histories.
- Countries the data was sent to include the US, Denmark, the UK, Canada, Belgium, Germany, Singapore and France.

Welsh Local Government Association response:

Despite requests for comment from the BBC, no response to the findings was forthcoming from the Welsh Local Government Association (WLGA).

Scotland:

Some 41% (13 out of 32) of Scottish councils showed evidence of advertising trackers loaded from their benefits pages.

Data on Scottish residents is sent to **at least two companies in two countries** through advertising trackers on benefits pages.

Some of the councils allowing third party advertising companies to track residents through their benefits pages include **South Lanarkshire, Aberdeen City, City of Edinburgh and Glasgow City**. See our data for the full list.

- DoubleClick - the advertising arm of Google - was the most-commonly-seen destination for this data.
- Examples of data being shared include IP addresses, locations (latitudes and longitudes) and browser histories.
- Countries the data was sent to include the US and Denmark.

Response from the Convention of Scottish Local Authorities (COSLA):

"Councils take their data protection responsibilities extremely seriously. If necessary, Council Data Protection Officers will liaise with the Information Commissioner's Office to establish what, if any, additional actions might be needed to fully comply with the GDPR privacy legislation.

“The use of cookies is a common and established feature on websites and is used to improve the performance or usability of these sites and to assist members of the public in finding content relevant to them.

“Council websites have published guidance on the use of cookies mentioned by the BBC and members of the public are encouraged to review that guidance on their Council website. If they have any concerns, or they are still in any doubt, they can seek further advice from their council.

“Councils will ensure that they comply quickly with any further recommendations identified by the ICO in relation to GDPR compliance. Given the concerns raised, councils will also take further steps to review the guidance on their websites with the aim of ensuring that it is clear and that a member of the public can easily opt-out or disable these cookies should they wish to do so."

Northern Ireland:

(Focus on Homepages, as Northern Irish council websites don't have benefits pages.)

91% (10 out of 11) of Northern Irish councils showed evidence of advertising trackers on their homepages,

- **On average one advertising cookie was found** on each of those 10 council homepages.
- DoubleClick - the advertising arm of Google - was the most-commonly-seen destination for this data.
- Examples of data being shared include IP addresses, locations (latitudes and longitudes) and browser histories.
- Countries the data was sent to include the US.

Northern Ireland Local Government Association (NILGA) response:

An NILGA spokesman said: "Council websites and their management across councils in Northern Ireland are individual to each council area. Therefore, specific performance and management matters should be addressed to each individual council, as appropriate. In regard to the BBC Shared Data Unit report, the findings of which would be welcome to support the ongoing management of council websites."

More reaction:

Simon McDougall, the Information Commissioner's Office's (ICO) executive director for technology policy and innovation, said:

- "The ICO has made looking at the use of ad-tech a priority. This investigation by the BBC further highlights our concerns about the lack of transparency and consent when ad-tech is used.

- "Earlier this year, the ICO published an update report into ad-tech and real time bidding (RTB). The report details our own concerns and we have continued to prioritise this work in recent months as part of our work on improving data protection practices in the sector.

- "While the ICO is keen to promote innovative uses of technology, that cannot be at the expense of people's fundamental legal rights. We will be assessing the information provided by the BBC."

James Taylor, Head of Policy, Public Affairs and Campaigns at disability equality charity, Scope, said:

> "Council benefits web pages exist to give disabled people vital information and financial support. These targeted trackers are cause for concern.
>
> "Scope research found that on average, disabled people face extra costs of £583 a month. Being served an advert for a credit card or low-cost loan while applying for state financial support could lead to debt and financial insecurity.
>
> "Everyone needs to do all they can to make sure disabled people are not unfairly targeted when trying to seek out support."

The advertisers' view:

A Google spokesman said:

- "Google does not build advertising profiles from sensitive interest categories, including from sites offering benefits such as welfare or unemployment, and we have strict policies preventing advertisers from using such data to target ads.

  "Third party cookies have a variety of uses, from enabling basic site functions to serving and measuring advertising.

  "We require publishers using Google's advertising products to obtain consent for cookies from European users, and take action against non-compliant publishers including suspension or termination."

Lloyd Clark, managing director, the Council Advertising Network (CAN) - a UK advertising network whose clients includes around 50 councils:

- "We do not specifically target vulnerable people via council advertising.

"In addition, we automatically block all categories of advertising that could be used to target vulnerable groups. This includes ads for payday loans, gambling and alcohol.

"If behavioural targeting is being used (some of the adverts will be non-targeted), we would expect to see advertisers interested in targeting budget-conscious consumers - for example discount retailers or comparison sites to find lower energy tariffs."

- "Targeted and behavioural advertising comes into it based on consent. Ultimately, it's the publisher's responsibility [to ensure the correct consent is sought]. However, we provide all the recommendations and the tools that the council can use to ensure consent.
  "The majority of our clients use our tool. Some use third party tools that serve the same purpose."

- "What's been built up is for the purpose that relevant information goes towards serving individuals' relevant advertisements.
  "People appreciate relative advertising. People don't like irrelevant adverts.
  "But if there are bad actors, it's certainly possible for them to behave like a bad actor.
  "That's a general challenge for the way the technology has been put together, not with advertising per say."

- "Given the tech furniture present right now we're in a position where you need to really trust people because the system won't work without it.
  "It creates a real challenge. We are reliant on people obeying the constraints that are set and the regulations that are out.
  "Unfortunately, we can't rely on only good actors. Even the biggest can fall prey to doing immoral things. That's what the industry is currently grappling with."

How to use the data:

See below for an explainer on the data set.

Sheet 1 ('Master'):

council_name	country	number_ of_homepage_advertising_trackers	number_of _benefits_page_advertising_trackers
Enfield	England	32	30
Ealing	England	26	30
Wirral	England	28	29
Southampton	England	25	29
Solihull	England	25	28
Torbay	England	3	28
North Somerset	England	2	28
North Lincolnshire	England	27	27
Sheffield	England	26	27
Redbridge	England	25	26
Torfaen	Wales	1	26

Column A: council_code_ONS

- ONS codes used to identify every council in the UK.

Column B: council_name

- The name of the council

Column C: country

- The country in which that council is located.

Column D: consent?

- Describes the different consent processes asked for on council websites.
- Only two are valid under GDPR and PECR (see law section above): 'Pop up - active consent' and 'cookie icon - active consent'.

Column E: homepage_advertising_trackers:

- The number of identified advertising trackers on that council's homepage.

Column F: benefits_page_advertising_trackers:

- The number of identified advertising trackers on that council's benefits page

E	F
homepage_advertising_tracker	benefits_page_advertising_tracker
32	30
29	2
28	25
28	29
27	27
27	23
26	30
26	27
25	26
25	28
25	29
24	25
23	23
21	21
20	22
20	
20	20
19	16
19	1

Sheet 2 + 3 ('Homepages' and 'Benefits pages'):

D	E	F	G	H
page_domain	3P_element_domain	3P_domain_owner	3P_domain_owner_country	category_of_tracker
aberdeencity.gov.uk	bootstrapcontent manag	StackPath	US	general
aberdeencity.gov.uk	cloudfront.net	Amazon Web Services	US	hosting
aberdeencity.gov.uk	doubleclick.net	DoubleClick	US	advertising
aberdeencity.gov.uk	google-analytics.com	Google Analytics	US	audience measurement
aberdeencity.gov.uk	google.com	Google	US	unknown
aberdeencity.gov.uk	googleapis.com	Google APIs	US	code
aberdeencity.gov.uk	govdelivery.com	GovDelivery	US	linked to advertising
aberdeencity.gov.uk	govmetric.com	Unknown	UK	customer relationship managemer
aberdeencity.gov.uk	gstatic.com	Google	US	hosting
aberdeencity.gov.uk	jsdelivr.net	jsDelivr	US	code
aberdeencity.gov.uk	typekit.com	Typekit	US	font
aberdeencity.gov.uk	typekit.net	Typekit	US	font
aberdeenshire.gov.uk	google-analytics.com	Google Analytics	US	audience measurement
adur-worthing.gov.uk	aspnetcontent managem	Microsoft	US	hosting
adur-worthing.gov.uk	cludo.com	Cludo	DK	advertising
adur-worthing.gov.uk	google-analytics.com	Google Analytics	US	audience measurement
adur-worthing.gov.uk	jquery.com	jQuery Foundation	US	code
adur-worthing.gov.uk	siteimprove.com	Siteimprove	DK	linked to advertising
adur-worthing.gov.uk	siteimproveanalytics.io	Siteimprove	DK	linked to advertising

Columns A-C, and column I:

- Same as above.

Column D: page_domain

- The domain of the council website scanned.

Column E: 3P_element_domain

- The domain of the third party advertising company detected.

Column F: 3P_domain_owner

- The owner (company) of that third party advertising domain.

Column G: 3P_domain_owner_country

- The country in which that owner (company) is based.

To Use:

- On the 'Master' sheet you can filter by council to see the amount of advertising trackers present on the homepage and benefits page of your council/s.
- You can also see whether your council/s ask for consent in a legally-appropriate manner.
- On the 'Homepages' and 'Benefits pages' sheets, you can filter by council to find a list of companies and owners with whom residents data is being shared. You can further filter by category for comparison. This study is based solely on the 'advertising' category.
- Note: multiple instances of the same council/s will appear on the 'Homepages and 'Benefits pages' sheets. This reflects the fact that there is one line for each third party domain detected.

Appendix 1 (further quotes):

Professor Tim Libert teaches in the privacy engineering programme at Carnegie Mellon University in the USA. He is the creator of the Webxray programme used in this investigation and an expert on the societal impacts of privacy-compromising information flow on the internet.

- "I've been a web developer since the late 1990s and a privacy researcher for the past seven years and this may be the most unexpected place I've seen an ad online.

"While I have seen trackers on public websites before it was almost always been to gain insights into audience behavior to improve a site, never for advertising. So this is very surprising to me."

- "From a democratic standpoint, societies operate under the philosophy that all citizens have equal value and each vote is counted once. No man or woman has greater value than another under the law. Companies, however, do not view people as equal.

"Some people are more desirable because they are wealthy and may spend more on luxury goods. Others are more desirable as they are poor and may have few options in life and may be exploited.

"These are not new trends. What is new is the application of micro-targeted advertising from the commercial realm being applied to the civic realm.

"Political advertisements are not new, but political advertisements tailored to individuals, that are hidden from the rest of society, is new, and is very troubling.

"Any evidence of deeper integration between the civil and commercial realms is cause for grave concern."

- "As is often the case where something in society goes fundamentally off course, as it has here, there are many places to assign blame.

  "First and foremost, it is important to note that there is no way for a tracker to force their code onto a site short of hacking it - the site itself must place the code there.

  "So the biggest party of responsibility is the website owner without question.

  "Otherwise, the big ad-tech companies have spent two decades systematically dismantling the old ways of doing advertising which were fairly de-centralized.

  "They have remade the global media environment in such a way that a handful of companies based in the US are now at the center of nearly all media consumption around the globe.

  "This level of power and control means websites have far fewer options, so the issue of monopoly control in areas such as social media, search, and video needs to be addressed as well."

- "Web pages have a finite size so there is a limit on how many advertisements can be on a page.

  "By targeting ads to specific users both the website and advertiser can make the best use of the limited screen space. Likewise, advertisers can segment populations to extend favorable offers to certain classes of customers and exclude others.

  "In my view targeting residents through benefits pages is utterly reprehensible as the most protections should be extended to those most in need.

  "The main value advertisers get from this data is the ability to segment the vulnerable in ways that they can be treated differently in a commercial context."

- “In some cases tracking can be used to improve the design of a website or to see what types of pages are the most popular.

  “This can be done without sacrificing user privacy, but websites often don’t make the effort to do it in a privacy-respecting way.

  “Other times a website may place a tracker so they may see the impact of ads they show elsewhere, such as on a social media website.

- “Simply put, the ad-tech industry has spent the last 20 years making billions of dollars engaged in business practices which are consistently shown to be incredibly unpopular with the public.

  “At this point, a final day of reckoning has yet to come, but laws like GDPR may be setting the stage for a fundamental realignment whereby the digital world will have to comply with the moral and ethical standards we’ve developed over centuries in the pre-digital era.

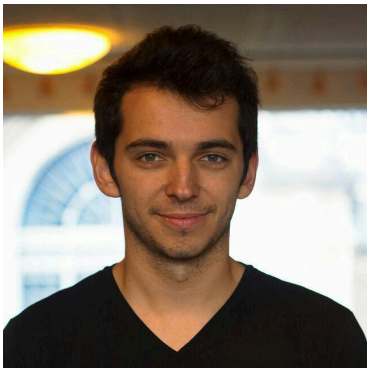
  “The ad-tech industry still seems to think they can continue to get away with undermining fundamental social norms and human rights, but the public is aware of this and both taking and demanding action.

  “In terms of taking action more people every day are using ad blockers to protect their privacy, making purchasing decisions based on privacy features, and generally being much more suspicious of companies they may have trusted much more, just 10 years ago.

  “Likewise, governments are feeling the heat from citizens who wonder why they have been left to fend for themselves against multi-billion dollar companies that don’t even pay taxes in many countries.

  “There’s no politician today who isn’t aware voters are fed up with privacy violations by tech companies and political hopefuls likewise know a great way to connect with voters is to promise action.”

Eliot Bendineli is a technologist at Privacy International (PI)- a UK NGO focussed on privacy advocacy. He leads PI's work on adtech, and is involved in work on targeted political advertisements, security and digital ID systems. Eliot was a driving force behind the publication: '[Your Mental Health for Sale: How websites about depression share data with advertisers and leak depression test results.]'



- "Basically having this type of profiling opens the way to control and manipulation. All of this really matters because these tools basically allow companies to have a good idea of who you are, where you live, what you're interested in, what you're doing this weekend, or if you have any mental health issues, for example."

"It's about the right to privacy. It's about owning your privacy, and having a private space to express yourself or to try different things. It's mandatory to be able to think freely and to be able to enjoy freedom of speech.

"When a company or a government has so much information about you, they can manipulate you. That's what we've seen with Cambridge Analytica.

"If companies know that you live in this neighbourhood and you answer questions in a certain way, they're able to come up with an ad that is targeted specifically for you and could make you vote for one person over another.

"The risk is that there is no control. It's just an open way for manipulation.

- "It's also a societal issue. A lot of people say that they have nothing to hide, or nothing to fear. But that also leads the way to data collection and technologies such as facial recognition in the streets.

  "For us it's a political and societal question: Do you want to live in a place where someone knows everything you do online, reads everything you read about and therefore can predict what you're going to do, or manipulate you to do other things?

  "People need to be aware of this."

- "Tracking people through benefits pages is sadly typical. It's always the people that are already vulnerable who are going to suffer the most.

  "If you have a good job and you're making a lot of money, and you have a phone that protects your privacy, then good for you, but if you're just using a random shared

computer in a house and you have no idea about how the internet works and how to protect yourself you're just going to be the perfect target to collect data.

"It's just opening the door to so many types of abuse."

- "The GDPR has an article about special category data - for example mental health. So if the council are sharing that type of sensitive data they don't have any legal justification for targeted advertising with that type of data.

  "But, sadly, I think it's possible they [the council] might be unaware. You can easily imagine that they don't have the budget to set up a proper website, or someone who sets it up doesn't explain how things are working.

  "Or without going into such extremes you can imagine some people set up that type of stuff, it's no big deal to make a bit of money.

  "The internet is difficult, and websites are hard to maintain. It's a full time job and even at Privacy International where we focus on that type of stuff we spend a lot of time maintaining everything we have online. We spend a lot of time making sure it's secure.

  "If you're a small council without a big budget for doing that type of stuff, then yes you're obviously a target for people who could hack your website, or at least you're open to just not being able to monitor what's been going on or what has been set up. It's possibly a lack of knowledge."

- "There are so many ways to display ads and so many different ways and technologies that can do that type of stuff.

  "But the relationship between the website and the ad network is not necessarily immediate.

  "Maybe the website sends it to the first ad network. Then the ad network might show it to five other networks, and all of these networks are going to share it with more people.

  "That's the whole problem we have with RTB in that if there is sensitive information in the bid requests then maybe hundreds or thousands of companies might get this information.

  "Those companies might not even bid to show you an advert. They could just collect the information and add it to an existing profile.

  "It's quite a complex web of things that are happening."

- “It’s just a wild west. There are thousands of things happening every second when you load a page and you literally have no control.

- “We're just scratching the surface. Unless you’re working for one of these companies, there’s no way to know what they're doing. There’s no way to know what type of data is being sent, to whom, how consent is even being preserved. It’s a wild west of data.

- “Everything is so broken that targeted advertising and tracking online has become what the internet is these days. Privacy is not the default option. You actually have to put a lot of work and effort in to avoid this happening.”

  “The responsibility shouldn’t be on the visitors or the users, but it shouldn't be on the website owners either. Of course they have a responsibility, but a lot of these advertising companies are doing unlawful things in terms of GDPR, and they are the ones who should be feeling the pressure right now.

  “Relying on contextual advertising is sufficient and efficient enough that websites shouldn’t have to rely on targeted ads.

  “In the end companies who buy into targeted advertising and websites who allow third parties to track users are not even touching the real value, because they’re not the ones collecting the data, building profiles and selling it to ad agencies or other clients - they’re just being abused by the system.

  “They don’t need the data they collect to just showing you adverts. A lot of this data, while it is used for advertising, of course, is also being used for many other things.

  “It might impact your credit rating if sent to a credit agency, or it might have so many effects that you just don’t foresee when you’re just browsing a website.

  “Once the data is out there, it’s in a bad place. You can reuse it into infinity. You can do what you want with it.”

Allessandro Acquisti, professor of information technology and public policy at the Heinz College, Carnegie Mellon University. His research combines economics, decision research, and data mining to investigate the role of privacy in a digital society. He co-wrote an oft-quoted academic paper this year which studied a large US media conglomerate's revenue from adverts for a week. His paper suggested that publishers who allow targeted advertising on their sites make

only 4% more ($0.0008 per ad) than non targeted, contextual advertising - such as placed adverts.

- “We can’t really say much about a website with a small amount of traffic because our data is definitely skewed to medium to large websites.
  “It’s possible that with much smaller traffic websites that don’t have as much sophistication in terms of using first party data, having contracts with advertising networks and the like, it’s possible in that case the extra value produced by selling targeted ad space may be larger. But we cannot know.”

- “From the merchant's perspective there is evidence that targeted ads and behavioural targeted ads have a higher click through rates and conversion rates than normal ads. This explains why merchants are willing to pay more.
  “If they do that it may suggest that they see comparatively larger conversion rates.”

- “Another possible interpretation is that there is value in targeted and behavioural advertising but much of the value is extracted by other intermediaries in the advertising ecosystem rather than the publishers themselves.
  “It’s possible that although merchants are paying a substantial premium, which may be justified full term, at the same time the publishers downstream at the end of the line may receive only a portion of the premium due to the fact that the other intermediaries in the advertising ecosystem are each taking their cut.”

- “To me the most interesting aspect of our study was to show how incredibly opaque the advertising ecosystem is, to the extent that it’s very hard even for the players within the ecosystem to get a precise sense of what the flows of money are.
  “This is bizarre considering the importance of this ecosystem from an international perspective.”

Lloyd Clark, managing director, the Council Advertising Network (CAN).

- “We do not specifically target vulnerable people via council advertising. If there are more trackers on benefit pages than the home page, this is because a minority of our council partners choose not to have advertising on their home pages at all.

  “But all their other webpages, like for waste and recycling or planning, will have the same number of trackers as their benefit pages.

  “In addition, we automatically block all categories of advertising that could be used to target vulnerable groups. This includes ads for payday loans, gambling and alcohol.

"If behavioural targeting is being used (some of the adverts will be non-targeted), we would expect to see advertisers interested in targeting budget-conscious consumers - for example discount retailers or comparison sites to find lower energy tariffs."

- "The councils have control of these categories. They can choose to put more restrictions on or not. We simplify it for the councils. They just select the categories, and we take care of the back end. Working directly with ad-tech providers can be more complicated. That can be why you see what you get inappropriate adverts."

- "The main thrust of our business is that we work with public service organisations almost exclusively. We help them take advantage of technological assets to generate income.

  "They can also use the technology to promote their own services. They could be looking for foster carers for instance. Our technology allows them to promote their message on their own website or on third party websites."

- "Targeted and behavioural advertising comes into it based on consent. Ultimately, it's the publisher's responsibility [to ensure the correct consent is sought]. However, we provide all the recommendations and the tools that the council can use to ensure consent.

  "The majority of our clients use our tool. Some use third party tools that serve the same purpose."

  "The way that our consent management platform works is that you will see a large bar at the bottom of the screen, with options to consent or review the purposes and go through the vendor list."

- "Whether we get consent or not we will make the ad call. Within the ad call we will provide the consent stage. That will say either they've agreed or not to personal advertising.

  "The ad buyer will use that consent stage to determine whether they will set [targeted adverts].

  "They are not permitted according to the regulations to use or share the data without the correct consent]."

- "What's been built up is for the purpose that relevant information goes towards serving individuals' relevant advertisements.

  "People appreciate relative advertising. People don't like irrelevant adverts.

"But if they are a bad actor, it's certainly possible for them to behave like a bad actor.

"That's a general challenge for the way the technology has been put together, not with advertising per se."

- "Given the tech furniture present right now we're in a position where you need to really trust people because the system won't work without it.

  "It creates a real challenge. We are reliant on people obeying the constraints that are set and the regulations that are out.

  "Unfortunately, we can't rely on only good actors. Even the biggest can fall prey to doing immoral things. That's what the industry is currently grappling with.

  "I think the industry will eventually move away from third party audience targeting entirely.

  "First party [audience targeting] will stay, but all the third party tracking we're seeing will simply go away. We will move from an audience tracking environment to a contextual tracking environment.

  "Experts are saying that with GDPR equivalents slowly emerging in the USA, that the writing is on the wall. Some browsers, like Firefox and Safari already don't allow it."

- "In our case, we ensure that an accurate, up-to-date consent string is always sent. We confirm periodically that our partners will only use data for ad personalisation when they receive a positive consent string and will not use the data for any other purpose.

  "Thus, when we are thinking about "risks versus rewards", the only risk to councils and residents is that a 'bad actor' will break the rules and use the data inappropriately.

  "The benefit is that councils are able to use a taxpayer-funded asset to generate income to help meet their revenue and savings targets.

  "Councils can also use our advertising tech to reach residents with crucial public service messaging. They can also use their ad space to promote local businesses and help grow their local economy.

  *"*In our model, this service is provided to the council at no cost. Our revenue comes solely from a share of the advertising income generated."

  "Because the risk is there regardless of whether councils accept advertising on their website, it seems to work against the public interest not to use a public asset to generate

- responsibly - income that will protect the delivery of public services, and to make use of the technology, free of charge, to deliver crucial public service messages to residents."

Appendix 2 (the law):

British and EU law has banned the sharing of personal data to third parties without freely given, informed and explicit consent.

The law comes from the Privacy and Electronic Communication Regulations (PECR), which sit alongside the Data Protection Act and the GDPR.

The PECR implement European Directive 2002/58/EC in UK law, also known as the 'e-privacy Directive'.

The regulations contain specific safeguards against "cookies and similar technology" (trackers).

The PECR cover any technology that stores information on a user's device or gains access to information on a user's device, by any method.

The regulations require that before tracking technology is used, "clear and comprehensive" information about its purpose must be given to the user.

This information must be easily available, and given in language that the intended audience would understand.

Consent for tracking technology must be freely given, specific and informed, and involve "unambiguous, positive action" - such as ticking a box or clicking a link.

Websites cannot legally set non-essential cookies or similar technology before the users have consented to them.

The GDPR definition of consent applies to the PECR. Article 4(11) of the GDPR says:

"'Consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

Notes:

- Main image copyright: Getty
- Images of Tim Libert and Eliot Bendineli: Free to use, credit to image subjects.