Europe’s hidden security crisis

How data about European defence personnel and political leaders flows to foreign states and non-state actors

Irish Council for Civil Liberties

About the authors

Dr Johnny Ryan FRHistS is a Senior Fellow of the Irish Council for Civil Liberties and the Open Markets Institute, and previously held senior roles in the technology industry, including in the RTB industry. He has written for *The Economist*, *NATO Review*, and *Studies in Conflict & Terrorism*.

Wolfie Christl is the principal of Cracked Labs, an independent Austrian research institute. He is a regular speaker at government and research cyber security and data conferences, and his research is widely cited, including in *The Financial Times* and *The Wall Street Journal*.

Acknowledgements

Thanks to Olga Cronin and Dr Kris Shrishak of ICCL, Ryan Gallagher of Bloomberg, Byron Tau of The Wall Street Journal.

Cover photograph by Luca Morvillo.

Charts and graphics by ICCL. All graphics excluding the cover photograph are free to reproduce and use, with attribution to ICCL.

Enforce

A unit of the Irish Council for Civil Liberties (ICCL). Learn more about our work on Real-Time Bidding's security and data protection harms at https://www.iccl.ie/enforce/

In this report

Summary

Real-Time Bidding (RTB) allows foreign states and non-state actors to obtain compromising sensitive personal data about key European personnel and leaders.

Key insights:

- Our investigation highlights **a widespread trade in data about sensitive European personnel and leaders that exposes them to blackmail, hacking and compromise, and undermines the security of their organisations and institutions.**

- These data flow from Real-Time Bidding (RTB), an advertising technology that is **active on almost all websites and apps**. RTB involves the broadcasting of sensitive data about people using those websites and apps to large numbers of other entities, **without security measures to protect the data**. This occurs billions of times a day.

- Our examination of tens of thousands of pages of RTB data[†] reveals that **EU military personnel and political decision makers are targeted using RTB** (page 11).

- This report also reveals that **Google** and other RTB firms **send RTB data about people in the U.S. to Russia** and **China**, where national laws enable security agencies to access the data. **RTB data are also broadcast widely within the EU in a free-for-all, which means that foreign and non-state actors can indirectly obtain them, too**.

- RTB data often include location data or time-stamps or other identifiers that make it relatively easy for bad actors to link them to specific individuals. Foreign states and non-state actors can use RTB to spy on **target individuals' financial problems, mental state, and compromising intimate secrets**. Even if target individuals use secure devices, data about them will still flow via RTB from personal devices, their friends, family, and compromising personal contacts.

- In addition, private surveillance companies in foreign countries deploy RTB data for **surreptitious surveillance**. We reveal "Patternz", a previously unreported surveillance tool that uses RTB to profile 5 billion people, including **the children of their targets**.

- Our examination of RTB data reveals **Cambridge Analytica style psychological profiling** of target individuals' **movements**, **financial problems**, **mental health problems** and vulnerabilities, including if they are likely **survivors of sexual abuse**.

[†] See selected source files here:

- **[Doc 1]** Microsoft Xandr data marketplace RTB segment list (global, including Europe), May 2021 (136.6MB)
URL: https://www.iccl.ie/wp-content/uploads/2023/10/Doc-1-Xandr-Data-Marketplace-May-2021.pdf
- **[Doc 2]** Dun & Bradstreet RTB segment list (global, including Europe), December 2021 (4.3MB)
URL: https://www.iccl.ie/wp-content/uploads/2023/10/Doc-2-as-printed-Eyeota-8-December-2021.pdf
- **[Doc 3]** Dun & Bradstreet RTB segment list (Europe only), October 2023 (81MB)
URL: https://www.iccl.ie/wp-content/uploads/2023/10/Doc-3-Dun-and-Brandstreet-Eyeota-October-2023.pdf

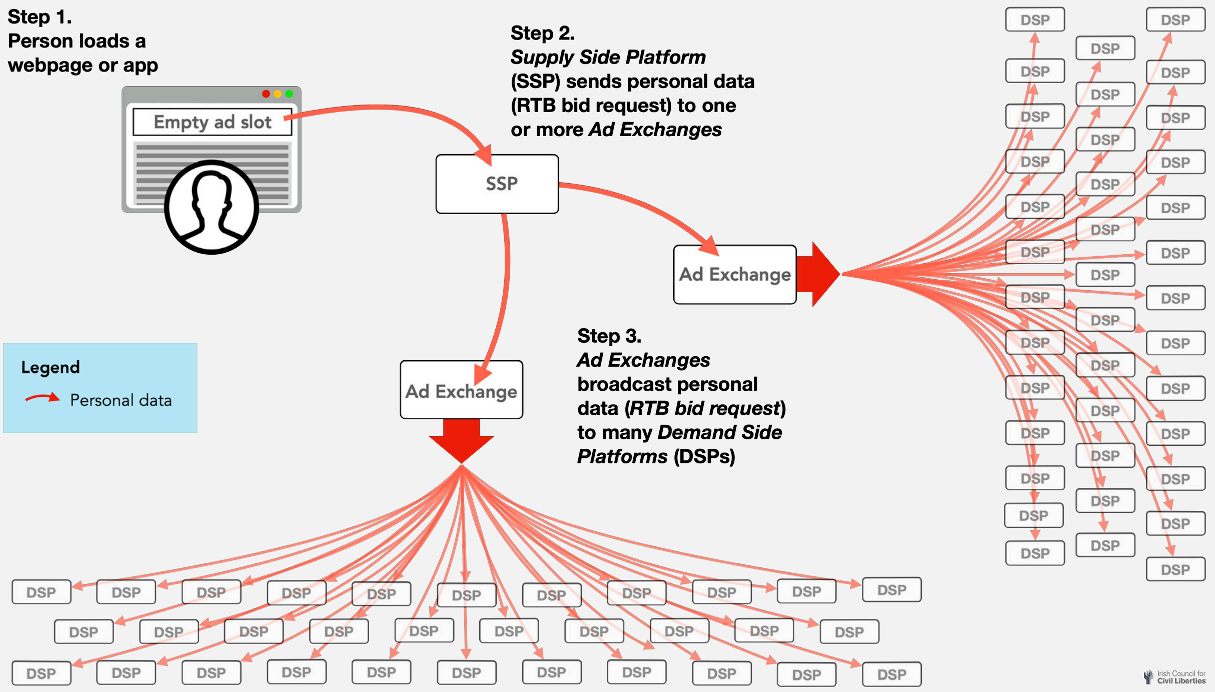
Background: RTB broadcasts EU data

Almost every time[1] a person loads new content on a website or app, instantaneous "Real-Time Bidding" (RTB) auctions determine what ads appear in front of them. RTB auctions occur in less than a second.

- RTB auctions are run by "ad exchange" companies. **Google** is the largest. They broadcast data about a person (who is viewing a website or app) to a large number of other companies, called "Demand Side Platforms" (DSPs). DSPs represent advertisers.
- Each DSP examines the broadcasted data about a person to evaluate whether to make a bid (on behalf of their clients) to have an ad appear in front of that exact person. DSPs also add the new data to their existing dossiers about the person.
- Industry technical documentation says that **"thousands" of DSPs can receive data** from one auction for just one ad slot.[2]

Very wide broadcasting of sensitive information

The sale of a single ad slot often involves an auction of auctions, with several ad exchanges running competing auctions that are coordinated by a Supply Side Platform (SSP). This increases the number of DSPs that receive the broadcasted data.



Step 1.
Person loads a webpage or app

Step 2.
Supply Side Platform* (SSP) sends personal data (RTB bid request) to one or more *Ad Exchanges

Step 3.
***Ad Exchanges* broadcast personal data (*RTB bid request*) to many *Demand Side Platforms* (DSPs)**

- Google's documentation says that **1,102 firms may receive data from Google auctions in Europe** (and far more from its auctions in the US).[3]

- **Microsoft says 1,647 firms may receive its RTB data** from its auctions.[4] Meta, Amazon and others undoubtedly do the same.

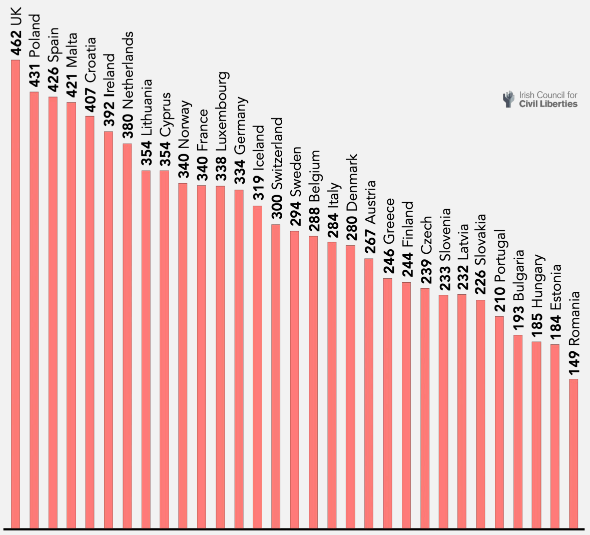
- **RTB data are broadcast without any security measures**.[5] After the broadcast there is no way to know or limit how receiving entities handle the RTB data. Nor is there any technical way to stop further distribution of RTB data. Industry documentation confirms "*there is no technical way to limit the way data is used*" after broadcast.[6] This has been confirmed by 27 EU data protection supervisory authorities,[7] and the UK.[8]

- RTB data broadcasts reveal highly sensitive information about a person including **location and movements over time,[10] what they are reading or watching or listening to, sexual interests, and personal problems** (see pages 15-17).

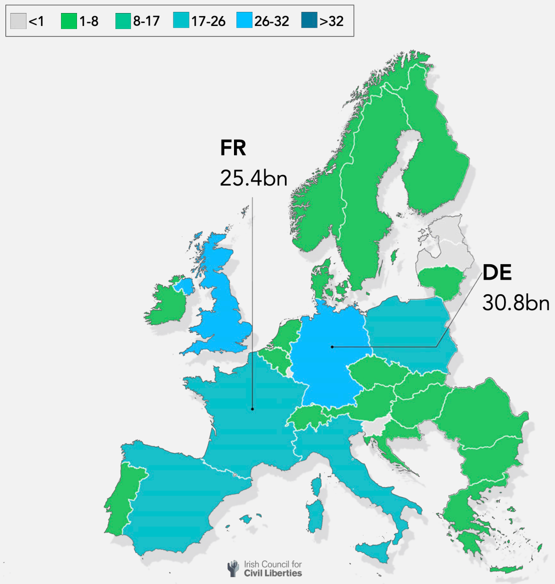
- This security problem affects not only sensitive personnel and leaders, but their **families and associates**, too. RTB data about people in Europe are broadcast **71 trillion times a year** (this figure excludes Amazon and Meta, for which we have no data).[11]

Biggest. Data. Breach. Ever. (Repeated Daily)

RTB broadcasts per person, daily



RTB broadcasts per country, daily (billions)



The chart shows industry[12] data on the billions of daily RTB broadcasts in each EEA + UK country (excluding Amazon and Meta, for which we do not have data).

- For example, **RTB data about each German internet user was broadcast roughly once per minute** that they are online in 2022, according to industry data.[13] A person in **France** will have had their online activity and location **exposed 340 times a day** on average.[14]

- **Google** operates the largest RTB ad exchange. Industry data shows it is **responsible for 21% of RTB broadcasts of EU data**.[15] Google's RTB system is live on 15.6 million websites[16] and millions of apps,[17] and broadcasts data such as what people are viewing or doing on a website or app and their "hyperlocal"[18] locations 42 billion times every day in Europe.[19]

- RTB's security problem has been evident since at least as early as 2017, when researchers proved that **for just $1,000** they could conclusively track targeted individuals' physical movements and the sensitive (including religious and sexual) apps they used using RTB.[20]

Insight

RTB data about the average person are broadcast to many entities, hundreds of times a day. There is no way to limit or know what happens to RTB data after they are broadcast.

Foreign access to EU RTB data

Foreign states and non-state actors can access compromising information about sensitive personnel and key leaders across Europe through the RTB system.

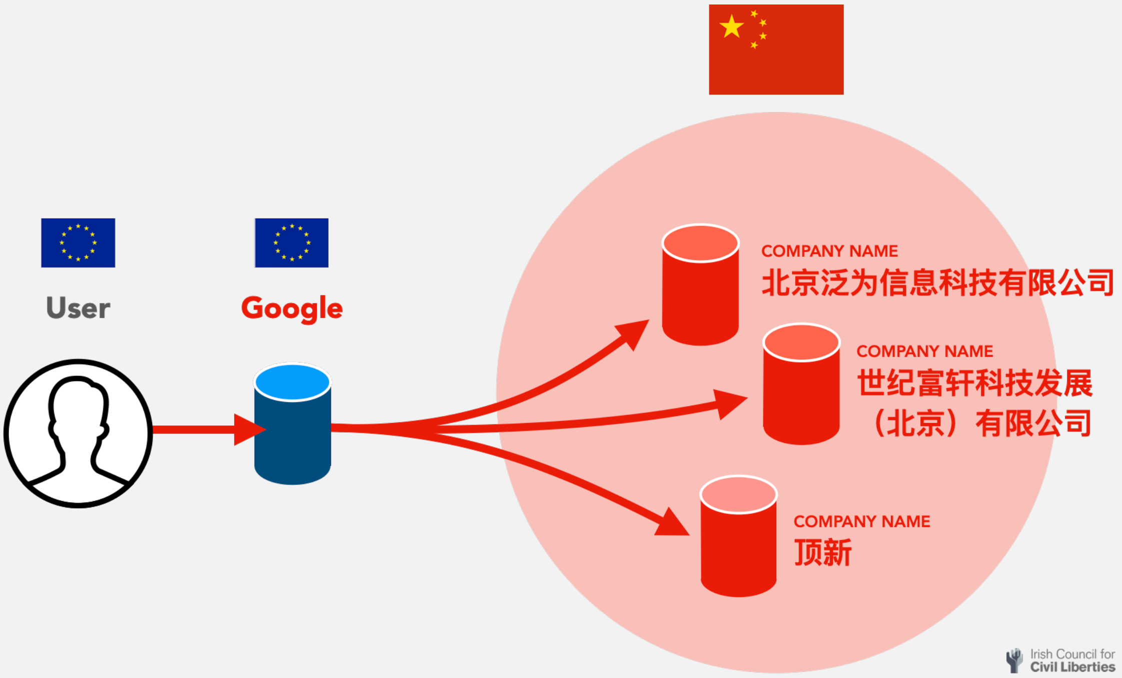
- **Google** sends European RTB data to many companies in **China**.[21] The 2021 Data Security Law of the People's Republic of China **allows the Chinese state to access EU RTB data once it is in the hands of Chinese companies**.[22]

- **Google** also sends European RTB data to **Russian companies**.[23] Russian law allows **the FSB and other security services to access any data**, including EU RTB data, collected by companies on Russian soil.[24]

- The Russian companies that Google sends EU RTB data to include **AiData, which sells profiles about Russians who visit Russian political opposition websites**.[25]

- **Microsoft's** RTB firm Xandr also sends European RTB data to **Russian**[26] and **Chinese**[27] **entities**, too. Other ad exchanges and SSPs are likely to be equally careless.

Google sends EU RTB data to China



The chart shows a small selection of the Chinese companies on Google's official list[28] of the 1,100+ companies in various locations that it sends European RTB data to.

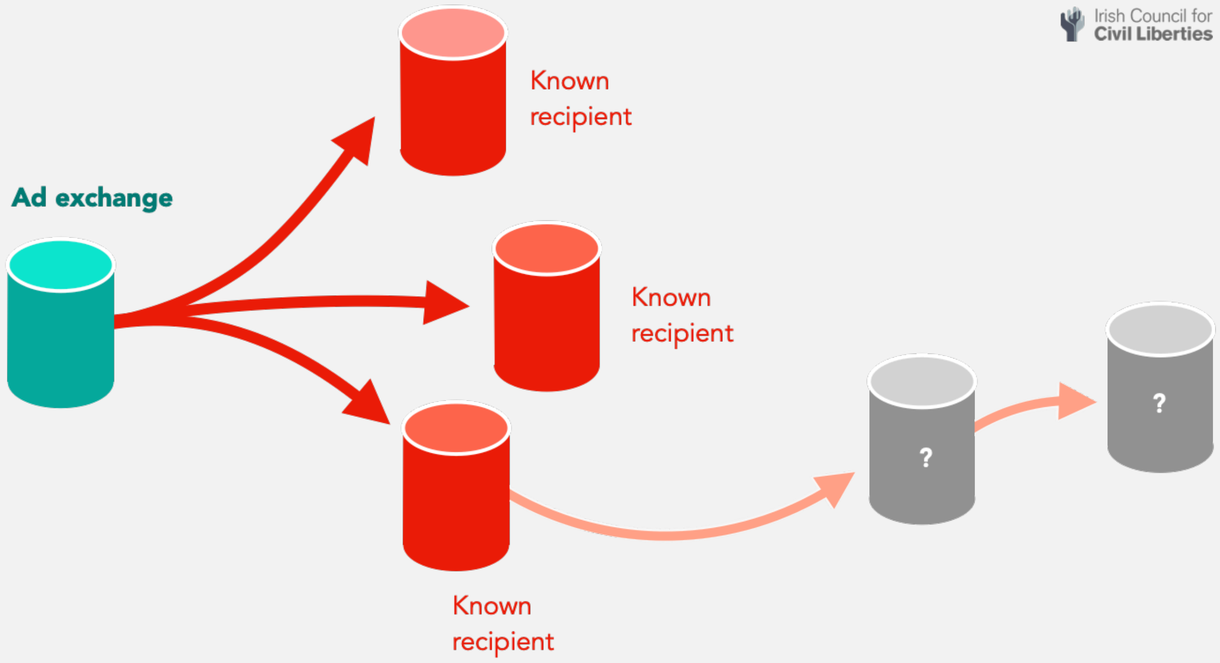
- Foreign and non-state actors can obtain EU RTB data by operating their own DSPs to receive RTB broadcasts directly. There is no control over who can operate a DSP. For example, a foreign private surveillance company (**Rayzone**) owns a DSP, which allows it to directly receive RTB broadcasts from ad exchanges and SSPs.[29] RTB data powers Rayzone's "Echo" surveillance tool,[30] which is "a fully stealth method of collection on any internet user" and offers "**mass collection of all internet users in a country**".[31]

- Similarly, another private foreign surveillance company (**Near Intelligence**) obtained masses of RTB data directly from three ad exchanges[32] through its own DSP.[33] It claims to have used this data to profile **152 million Europeans**, including their "home location", "work places", and places frequented".[34]

- Foreign and non-state actors can also obtain EU RTB data indirectly: by buying from some of the many companies that receive RTB broadcasts.[35] For example, another surveillance company (**ISA**) acknowledged it obtains RTB data indirectly via major RTB firms, which powers its "**Patternz"** surveillance system (see page 13).[36]

A data free-for-all

A large number of entities receive extraordinarily sensitive (see pages 15-17) RTB data about Europe's leaders and sensitive defence personnel. There is no way to control what they then do with those data. Thus, an ad exchange has no way to know what entities actually receive RTB data from it. This is an enormous free-for-all of very sensitive data. **Even if RTB data is only initially broadcast to companies in Europe, it will inevitably be available to foreign and non-state actors.**



Insight

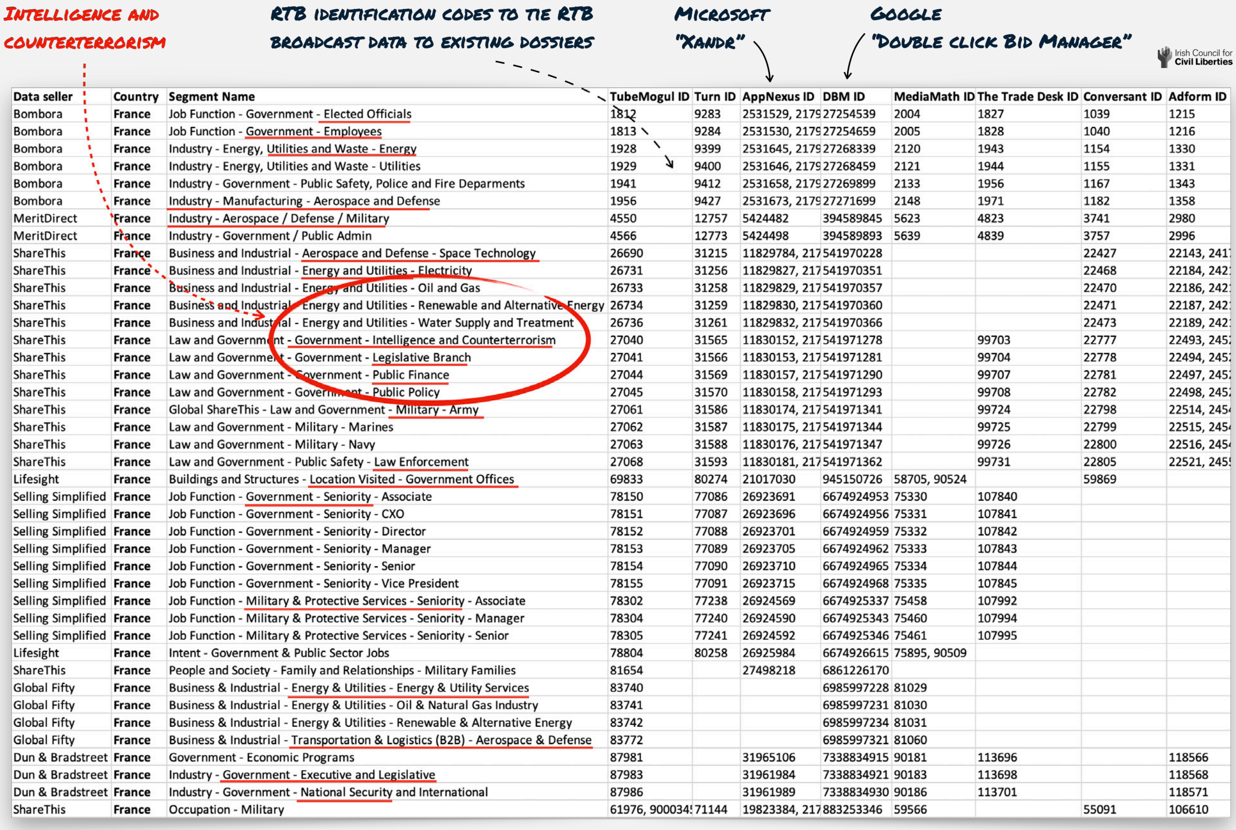
Foreign states and non-state actors can obtain EU RTB data with ease. They can do this directly, by operating a DSP, or indirectly, by obtaining the data from another entity.

Targeting Europe’s leaders and sensitive defence personnel

Our investigation highlights a widespread trade in RTB data about sensitive European personnel that exposes them to blackmail, hacking and compromise, and undermines the security of their organisations and institutions.

RTB dossiers about security and defence personnel

The screenshot shows RTB data about categories of people available from Dun & Bradstreet, a data broker company that also sells data provided by other data brokers (See Doc 3).[37] This 15,406 page spreadsheet includes people in France (and other Member States) categorised as **“Intelligence and Counterterrorism”**. These data are “observed from social sharing, searched page visits and click-backs on shared pages”.[38]



Intelligence and counterterrorism

RTB identification codes to tie RTB broadcast data to existing dossiers

Microsoft "Xandr"

Google "Double click Bid Manager"

Data seller	Country	Segment Name	TubeMogul ID	Turn ID	AppNexus ID	DBM ID	MediaMath ID	The Trade Desk ID	Conversant ID	Adform ID
Bombora	France	Job Function - Government - Elected Officials	1812	9283	2531529, 2179	27254539	2004	1827	1039	1215
Bombora	France	Job Function - Government - Employees	1813	9284	2531530, 2179	27254659	2005	1828	1040	1216
Bombora	France	Industry - Energy, Utilities and Waste - Energy	1928	9399	2531645, 2179	27268339	2120	1943	1154	1330
Bombora	France	Industry - Energy, Utilities and Waste - Utilities	1929	9400	2531646, 2179	27268459	2121	1944	1155	1331
Bombora	France	Industry - Government - Public Safety, Police and Fire Deparments	1941	9412	2531658, 2179	27269899	2133	1956	1167	1343
Bombora	France	Industry - Manufacturing - Aerospace and Defense	1956	9427	2531673, 2179	27271699	2148	1971	1182	1358
MeritDirect	France	Industry - Aerospace / Defense / Military	4550	12757	5424482	394589845	5623	4823	3741	2980
MeritDirect	France	Industry - Government / Public Admin	4566	12773	5424498	394589893	5639	4839	3757	2996
ShareThis	France	Business and Industrial - Aerospace and Defense - Space Technology	26690	31215	11829784, 217	541970228			22427	22143, 241
ShareThis	France	Business and Industrial - Energy and Utilities - Electricity	26731	31256	11829827, 217	541970351			22468	22184, 242
ShareThis	France	Business and Industrial - Energy and Utilities - Oil and Gas	26733	31258	11829829, 217	541970357			22470	22186, 242
ShareThis	France	Business and Industrial - Energy and Utilities - Renewable and Alternative Energy	26734	31259	11829830, 217	541970360			22471	22187, 242
ShareThis	France	Business and Industrial - Energy and Utilities - Water Supply and Treatment	26736	31261	11829832, 217	541970366			22473	22189, 242
ShareThis	France	Law and Government - Government - Intelligence and Counterterrorism	27040	31565	11830152, 217	541971278		99703	22777	22493, 245
ShareThis	France	Law and Government - Government - Legislative Branch	27041	31566	11830153, 217	541971281		99704	22778	22494, 245
ShareThis	France	Law and Government - Government - Public Finance	27044	31569	11830157, 217	541971290		99707	22781	22497, 245
ShareThis	France	Law and Government - Government - Public Policy	27045	31570	11830158, 217	541971293		99708	22782	22498, 245
ShareThis	France	Global ShareThis - Law and Government - Military - Army	27061	31586	11830174, 217	541971341		99724	22798	22514, 245
ShareThis	France	Law and Government - Military - Marines	27062	31587	11830175, 217	541971344		99725	22799	22515, 245
ShareThis	France	Law and Government - Military - Navy	27063	31588	11830176, 217	541971347		99726	22800	22516, 245
ShareThis	France	Law and Government - Public Safety - Law Enforcement	27068	31593	11830181, 217	541971362		99731	22805	22521, 245
Lifesight	France	Buildings and Structures - Location Visited - Government Offices	69833	80274	21017030	945150726	58705, 90524		59869	
Selling Simplified	France	Job Function - Government - Seniority - Associate	78150	77086	26923691	6674924953	75330	107840		
Selling Simplified	France	Job Function - Government - Seniority - CXO	78151	77087	26923696	6674924956	75331	107841		
Selling Simplified	France	Job Function - Government - Seniority - Director	78152	77088	26923701	6674924959	75332	107842		
Selling Simplified	France	Job Function - Government - Seniority - Manager	78153	77089	26923705	6674924962	75333	107843		
Selling Simplified	France	Job Function - Government - Seniority - Senior	78154	77090	26923710	6674924965	75334	107844		
Selling Simplified	France	Job Function - Government - Seniority - Vice President	78155	77091	26923715	6674924968	75335	107845		
Selling Simplified	France	Job Function - Military & Protective Services - Seniority - Associate	78302	77238	26924569	6674925337	75458	107992		
Selling Simplified	France	Job Function - Military & Protective Services - Seniority - Manager	78304	77240	26924590	6674925343	75460	107994		
Selling Simplified	France	Job Function - Military & Protective Services - Seniority - Senior	78305	77241	26924592	6674925346	75461	107995		
Lifesight	France	Intent - Government & Public Sector Jobs	78804	80258	26925984	6674926615	75895, 90509			
ShareThis	France	People and Society - Family and Relationships - Military Families	81654		27498218	6861226170				
Global Fifty	France	Business & Industrial - Energy & Utilities - Energy & Utility Services	83740			6985997228	81029			
Global Fifty	France	Business & Industrial - Energy & Utilities - Oil & Natural Gas Industry	83741			6985997231	81030			
Global Fifty	France	Business & Industrial - Energy & Utilities - Renewable & Alternative Energy	83742			6985997234	81031			
Global Fifty	France	Business & Industrial - Transportation & Logistics (B2B) - Aerospace & Defense	83772			6985997321	81060			
Dun & Bradstreet	France	Government - Economic Programs	87981		31965106	7338834915	90181	113696		118566
Dun & Bradstreet	France	Industry - Government - Executive and Legislative	87983		31961984	7338834921	90183	113698		118568
Dun & Bradstreet	France	Industry - Government - National Security and International	87986		31961989	7338834930	90186	113701		118571
ShareThis	France	Occupation - Military	61976, 900034	71144	19823384, 217	883253346	59566		55091	106610

These insights may be collected from diverse sources including RTB, and are then available for targeting using RTB. Segments are provided with RTB segment identification codes so that people they relate to can be identified by other entities via the RTB system.

- Careless use of sensitive data is a feature of the RTB industry's technical standards. The "IAB Context Taxonomy" is an RTB industry standard that categorises what target individuals are watching, reading, or listening to. The code IAB-122 marks a person's interest as "**defence industry**".[39]

- A second set of almost 2,000 RTB industry codes provide common rules for building dossiers about persons of interest once an RTB broadcast has been received. This is called the "IAB Audience Taxonomy". IAB code 885 marks a person as being in **procurement** ("purchase intent") in the "**Aerospace and Defence**" sector. Code 885 is for government. Code 876 is for the energy industry, etc.[40]

- Separately, a May 2021 list (Doc 1) of various RTB data available for purchase from various companies through the **Microsoft "Xandr"** data marketplace includes 651,463 segments, and is **19,956 pages** long.

- Doc 1 contains RTB segments for defence aerospace employees at **Airbus**;[41] engineers at UK defence and critical infrastructure protection vendor **BAE Systems**;[42] employees of **Babcock**,[43] a defence vendor that provides maintenance for the UK nuclear submarine fleet, air force, and army; and employees of **GKN Aerospace**,[44] which recently serviced the landing gear of the Dutch Airforce's F-35 fleet[45] and services JAS Gripen, F-16, and F-18 combat aircraft in Europe.

- Doc 1 includes RTB data on **French**, **German**, and **UK army**, **navy**, and **air force** personnel;[46] those countries' **judges**,[47] **politicians**[48] and personnel in sensitive industries including **nuclear energy**,[49] **aerospace & defence**,[50] and **space technology**.[51] There are also segments about people whose location reveals they were located at security conferences, hotels, restaurants, and venues.[52] One segment identifies people within six miles of a military base.[53] Segments from Oracle (subsidiary Bluekai) categorise **German civil servants**[54] and **military personnel**.[55]

- A slightly more recent segment sheet (Doc 2) provides similar segments on "**People working in defense & space**",[56] "**People who work in the military**",[57] "**People working in judiciary**",[58] etc. These are offered by various sellers, including LiveRamp (subsidiary "Pacific Data Partners").[59]

- Another list, live as of October 2023, from Dun & Bradstreet (Doc 3) includes **people categorised as "Government - Intelligence and Counterterrorism" in sixteen European countries** (Austria,[60] Belgium,[61] Czech Republic,[62] Denmark,[63] Finland,[64] France,[65] Germany,[66] Ireland,[67] Italy,[68] the Netherlands,[69] Poland,[70] Spain,[71] Sweden,[72] Switzerland,[73] and the United Kingdom).[74]

- Doc 3 contains 130,293 segments provided by various data sellers. It also includes a segment of people categorised as **"decision makers for the Government … National Security and International Affairs"** for each of the sixteen countries.[75] Other segments identify senior military officers in each country.[76]

- Doc 3 lists the price to purchase access to **"Users who are employed in the Government, specifically Government, Defense and Emergency"**.[77]

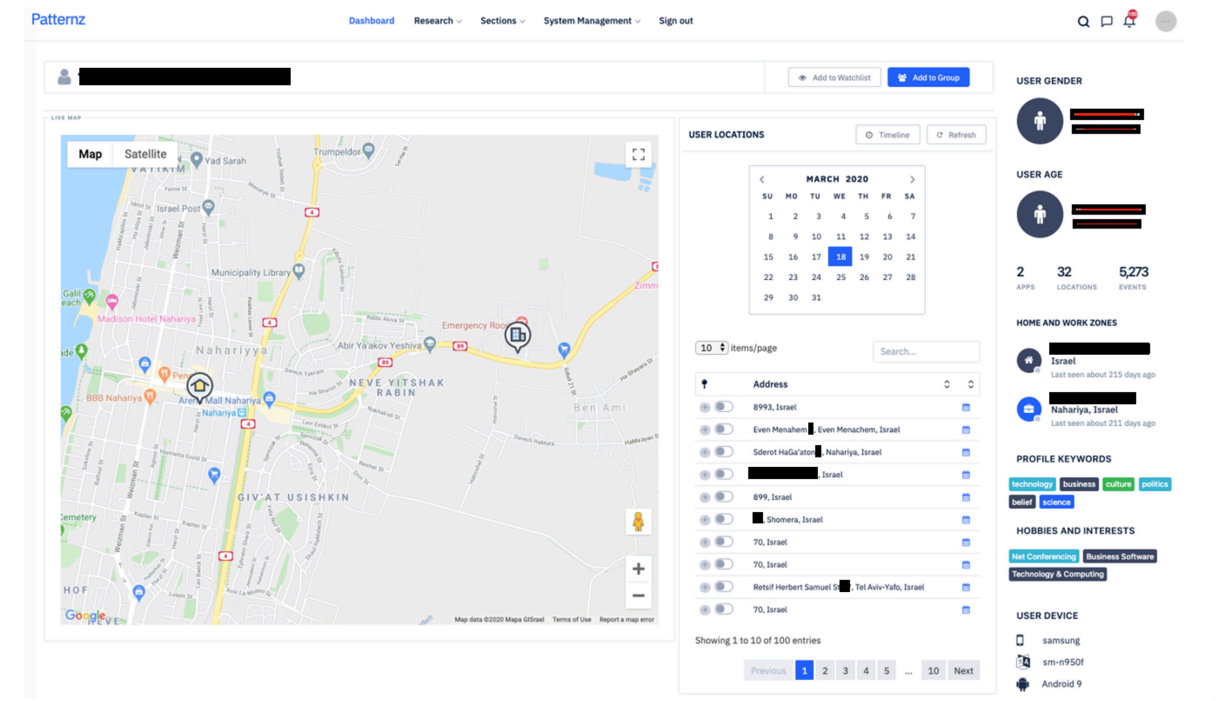
- Also present in Doc 3 are segments about **"decision makers for the political organizations"[78] in each European country**, in addition to segments of people categorised **"army"**,[79] **"navy"**,[80] and **"aerospace and defense"**.[81]

- Doc 3 also contains segments about **military spouses and families** in each country.[82]

Commercial surveillance tool "Patternz" uses RTB data to profile 5 billion devices, including the children of its targets

ISA, a private company, sells a surveillance tool called "Patternz". It claims Patternz has **profiled 5 billion people**[83] by analysing large volumes of RTB data that it says it obtains from a large number of RTB companies (including Google and Twitter).[84] Patternz creators claim "*knowhow of operating a realtime bidding platform for the last 5 years*".[85]

As the screenshot shows, Patternz provides a targeted person's current location, historical movements over several months, and who they frequently met.[86] ISA says Patternz **can identify a target's children**, co-workers, and their "driving path".



[redacted]

USER LOCATIONS

MARCH 2020

SU	MO	TU	WE	TH	FR	SA
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

10 items/page

	Address
	8993, Israel
	Even Menahem [redacted], Even Menachem, Israel
	Sderot HaGa'aton [redacted], Nahariya, Israel
	[redacted], Israel
	899, Israel
	[redacted], Shomera, Israel
	70, Israel
	70, Israel
	Retsif Herbert Samuel St [redacted], Tel Aviv-Yafo, Israel
	70, Israel

Showing 1 to 10 of 100 entries

Previous 1 2 3 4 5 ... 10 Next

USER GENDER

[redacted]

USER AGE

[redacted]

2	32	5,273
APPS	LOCATIONS	EVENTS

HOME AND WORK ZONES

[redacted]
Israel
Last seen about 215 days ago

[redacted]
Nahariya, Israel
Last seen about 211 days ago

PROFILE KEYWORDS

technology business culture politics belief science

HOBBIES AND INTERESTS

Net Conferencing Business Software Technology & Computing

USER DEVICE

samsung
sm-n950f
Android 9

Note: redactions applied to image

Insight

European personnel and leaders are categorised and targeted using RTB. At a minimum, this creates a security risk by exposing their movements and activities. The security threat is more acute, however, as the next section shows: RTB data about target individuals' job functions can also be cross-referenced with more intimate RTB data about those individuals. This exposes targeted individuals and their organisations to severe security risks.

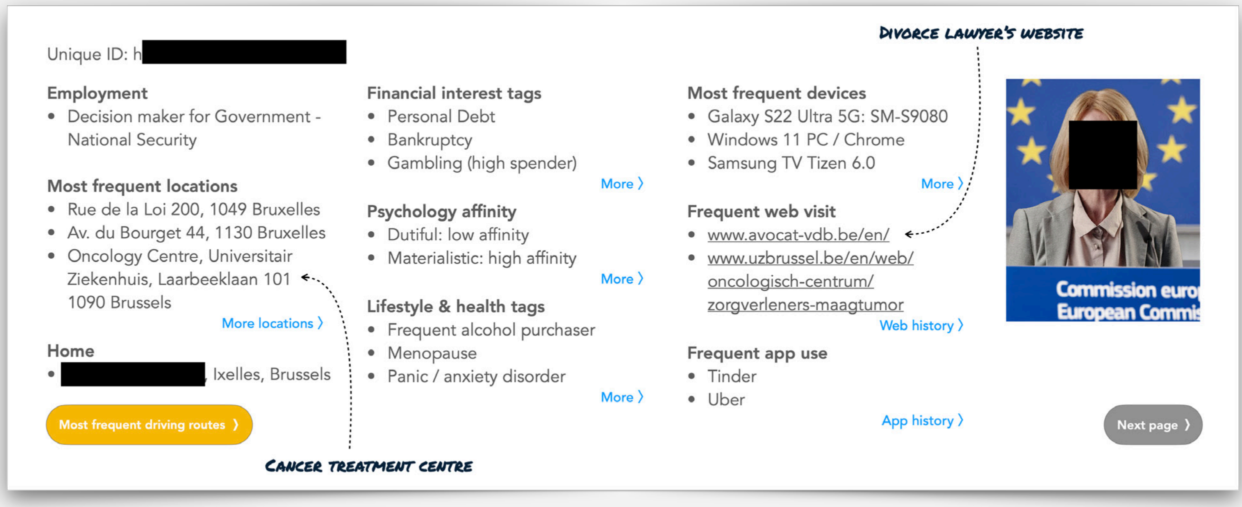
A torrent of blackmail data

RTB data not only allow foreign states and non-state actors to track key personnel and leaders' movements and online activity, but also expose intimate information about targeted individuals and their organisations to influence, blackmail, or hacking by foreign and non-state actors.

- Exploiting a person's "M.I.C.E." (their **money** problems or desires, **ideology**, vulnerabilities that can be **compromised**, and **ego**) characteristics is a well-established means of recruiting foreign intelligence assets.[87] RTB is a goldmine of insights.
- RTB industry codes indicate a target individual's **psychological condition**. For example, a **recent family bereavement** is marked by IAB Audience Taxonomy code 1502, which indicates intent to purchase funeral services).[88] A **heavy drinker** is categorised by the combination of the IAB Audience Taxonomy code for "frequent purchaser" (code PIPF3) with the code for "alcohol consumption" (code 369).
- IAB Context Taxonomy also provides psychological insights. For example, code IAB-287 denotes "**mental health**", code IAB-311 denotes "**substance abuse**".[89]

A goldmine of *kompromat* on specific leaders

The RTB security problem can enable foreign states and non-state actors to target specific leaders and personnel in Europe, and mine RTB for information about their financial circumstances, mental state, and compromising intimate secrets. **This exposes Europe's most sensitive institutions and industries to hacking, blackmail, and compromise**.



Unique ID: h[redacted]

Employment
- Decision maker for Government - National Security

Most frequent locations
- Rue de la Loi 200, 1049 Bruxelles
- Av. du Bourget 44, 1130 Bruxelles
- Oncology Centre, Universitair Ziekenhuis, Laarbeeklaan 101 1090 Brussels

More locations 〉

Home
- [redacted], Ixelles, Brussels

Most frequent driving routes 〉

Financial interest tags
- Personal Debt
- Bankruptcy
- Gambling (high spender)

More 〉

Psychology affinity
- Dutiful: low affinity
- Materialistic: high affinity

More 〉

Lifestyle & health tags
- Frequent alcohol purchaser
- Menopause
- Panic / anxiety disorder

More 〉

Most frequent devices
- Galaxy S22 Ultra 5G: SM-S9080
- Windows 11 PC / Chrome
- Samsung TV Tizen 6.0

More 〉

Frequent web visit
- www.avocat-vdb.be/en/
- www.uzbrussel.be/en/web/oncologisch-centrum/zorgverleners-maagtumor

Web history 〉

Frequent app use
- Tinder
- Uber

App history 〉

Next page 〉

DIVORCE LAWYER'S WEBSITE

CANCER TREATMENT CENTRE

Note: image is a sketch of data that be available through RTB about a specific leader (example is not a real person)

- Commercially available RTB segments in Microsoft Xandr's list (Doc 1) reveal whether a person suffers **depression** (provided by Nielsen,[90] Epsilon,[91] LiveRamp,[92] comScore,[93] Oracle,[94] and many others), or other conditions such as **chronic pain**,[95] **substance abuse**,[96] and **anxiety disorders** (provided by OnAudience).[97]

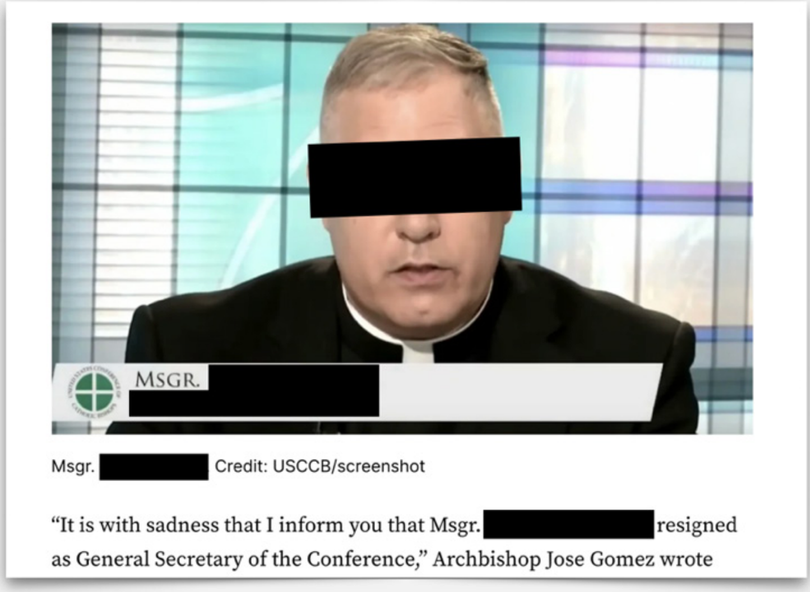
- Doc 1 includes further compromising data about individuals' mental health, psychology, politics, sexuality, and finances. For example, several segments categorise likely **survivors of sexual abuse** (provided by comScore,[98] Grapeshot,[99] Integral Ad Science,[100] and DoubleVerify).[101]

- Segments about people in **France** include whether a person is homosexual,[102] menopausal,[103] and even what brand of underwear they wear.[104]

- Doc 1 also includes **Cambridge Analytica style psychological profiling of German people** (provided by AZ Direct).[105] Among other things, the data indicate the degree to which a target individual is "materialistic" or "dutiful", potentially revealing how open to bribes they are.

Catholic priest outed by sensitive RTB data

RTB data over 52 weeks revealed a Catholic priest's use of gay apps and his visits to private homes and to a gay bathhouse.[106] The individual left the priesthood when the data were made public. It was later revealed that a conservative group had invested millions of dollars on sex app RTB data to monitor whether Catholic priests are celibate.[107] Beyond the severe intrusion into privacy, the **example shows how a similar operation can be conducted to blackmail or manipulate European personnel and leaders**.



Msgr. [redacted] Credit: USCCB/screenshot

"It is with sadness that I inform you that Msgr. [redacted] resigned as General Secretary of the Conference," Archbishop Jose Gomez wrote

- IAB Audience Taxonomy codes identify compromising insights about **target individuals' financial problems**, such as "payday and emergency loans" (code 1395), income, savings, debt, family life, seniority at work, and so on.[108] IAB Context taxonomy code IAB-65 denotes "**bankruptcy**", and IAB-405 denotes "personal debt", etc.[109]

- Commercially available segments in Doc 3 provide insight about targeted individuals' financial circumstances: whether they are **gamblers**,[110] and **gambling high spenders**;[111] their **income**, level of **debt** level, etc. Doc 1 provides insight on whether, for example, a Danish person has only a small pension.[112] . This is valuable information for any foreign state that seeks a means of recruiting a potential European intelligence "asset".

- Doc 3 also includes segments about people's **ideology** and **political views**. For example, whether an Italian is a moderate;[113] a German is a rural conservative;[114] a Dane is traditional and community orientated;[115] or Briton has "family values".[116]

- IAB codes and segment codes can be sent with ID codes to identify the specific person concerned and tie every new piece of data to them.[117] In any case, other data are broadcast that aid identification where there is no ID code.[118] Thus, **foreign states and non-state actors can build detailed dossiers about target individuals daily lives and vulnerabilities.**

Insight

Dissemination of RTB data creates a serious security risk for Europe. RTB data can be combined by foreign states and non-state actors to build highly compromising dossiers about Europe's sensitive personnel and leaders.

Neutralising RTB's security threat

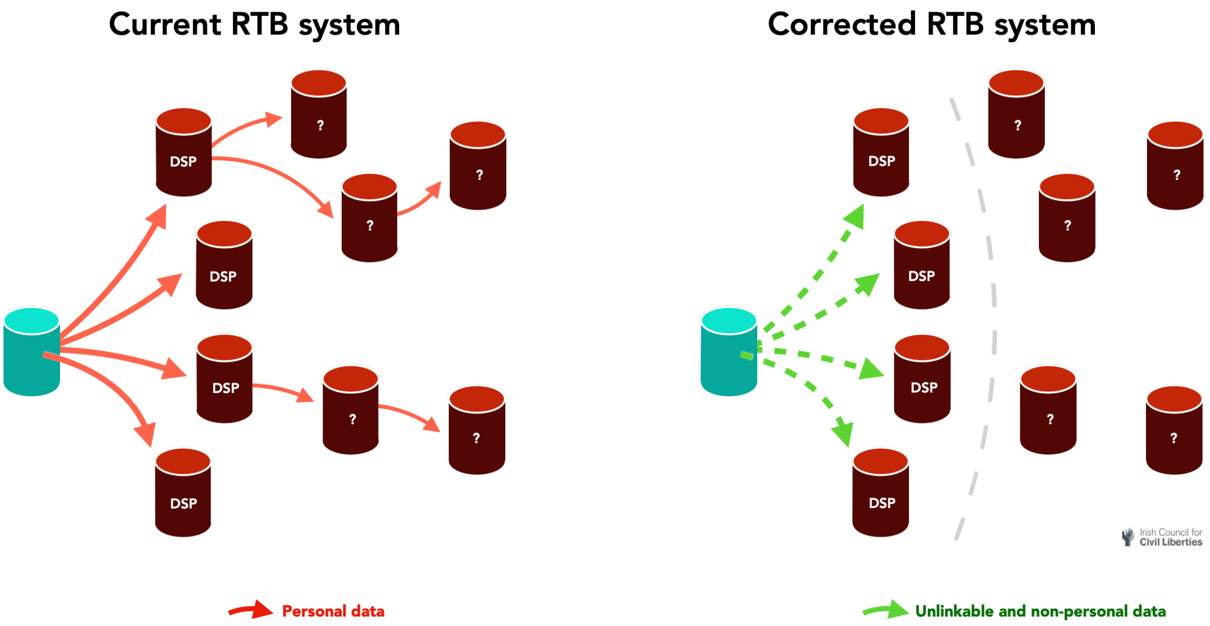
Fixing RTB will resolve Europe's security threat.

- Two entities set the rules for what data are permitted in RTB broadcasts:
  1. **IAB TechLab**: IAB TechLab is the tracking industry's standards body. Its "OpenRTB protocol"[119] sets the rules for 79% of RTB data broadcasts in Europe.[120]
  2. **Google**: Google's "Authorized Buyers protocol"[121] governs the remaining 21% of RTB broadcasts in Europe.

- Currently, IAB TechLab and Google permit RTB broadcasts to include personal data. These personal data can identify a targeted individual, and can be linked to subsequent RTB broadcasts about the same person to build up a long-term dossier about them.

- Google and IAB TechLab should amend their protocols so that no personal data are permitted in future RTB broadcasts. All identifying and linkable data must be removed. This includes high resolution timestamps, data extensions, unique identifiers, etc. This will foil foreign and non-state actors who operate their own DSPs, or who indirectly obtain RTB data from other entities that receive RTB broadcasts. This can be enforced and monitored at SSPs and ad exchanges.

- Google and IAB TechLab are responsible as "data controllers" under the GDPR, and can be ordered to prevent personal data from being broadcast.[122]


Current RTB system

Corrected RTB system

DSP
DSP
DSP
DSP
?
?
?
?
?
DSP
DSP
DSP
DSP
?
?
?
?
?
Irish Council for Civil Liberties
Personal data
Unlinkable and non-personal data

Insight

RTB industry data standards create an unacceptable risk to EU and Member State security. Despite the large number of companies in the RTB industry, the RTB security threat can be easily neutralised by enforcing data protection law on the responsible standards setters.

Recommendations

RTB is a security threat. Foreign states and non-state actors have access to compromising information about Europe's sensitive personnel and leaders through RTB. The hazard to European security is acute and must be addressed.

1. The European Commission should request that the European Data Protection Board examine the RTB security crisis.[123] Data protection supervisory authorities should enforce the GDPR "security principle" (GDPR Article 5(1)f) by ordering the two relevant data controllers, IAB TechLab and Google, to fix their RTB standards as described on page 18 to prevent SSPs and advertising exchanges from disclosing any potential personal data to any other entities.

2. In parallel, the EU Agency for Cybersecurity (ENISA) should issue an alert to Member States and Union institutions, bodies, offices and agencies. In 2021, the U.S. Cybersecurity and Infrastructure Security Agency recommended that all federal agencies block ads to reduce the "risk of data collection by third parties".[124] However, this on its own will not be sufficient. Even if institutions take steps to mitigate RTB security risks, people will be exposed in their personal and family lives.

3. The European External Action Service (EEAS), the NIS Cooperation Group and ENISA should be directed to urgently conduct a joint assessment of RTB as a security threat to the European Union.

4. If necessary, the European Commission should consider whether there is a divergent approach to this common security issue, and whether it should propose measures to introduce legal certainty and harmonisation.

Notes

Note: links may be removed over time. If a link is inoperable then please refer to the Wayback Machine of the Internet Archive for an archived version of the source.

[1] RTB is the dominant technology of online advertising. RTB "Programmatic" including display and video ads accounted for an estimated $99bn in 2021, more even than search advertising ($78.3bn), according to "PwC IAB Internet Advertising Revenue Report 2021", April 2022 (URL: https://www.iab.com/insights/internet-advertising-revenue-report-full-year-2021/), pp 17, 21.

[2] The word "thousands" is used in "pubvendors.json v1.0", IAB Europe, 25 April 2018 (URL: https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/pubvendors.json%20v1.0%20Draft%20for%20Public%20Comment.md#liability).

[3] "Ad technology providers", Google (URL: https://support.google.com/admanager/answer/9012903?hl=en#).

[4] "Service Policies" , Xandr (No longer public, archived URL: https://www.iccl.ie/wp-content/uploads/2022/01/K13-24032021-service_policies_3-24-2021.pdf).

[5] The industry relies on good faith and contractual stipulations.

[6] "pubvendors.json v1.0", IAB Europe, 25 April 2018 (URL: https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/pubvendors.json%20v1.0%20Draft%20for%20Public%20Comment.md#liability).

[7] This was confirmed by a decision of 28 European data protection authorities. See paragraph 429, 'Decision on the merits 21/2022 of 2 February 2022", European Data Protection Board (URL: https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-21-2022-english.pdf).

[8] The UK Information Commissioner's Office (ICO) reported that *"once data is out of the hands of one party, essentially that party has no way to guarantee that the data will remain subject to appropriate protection and controls"* in "Update report into adtech and real time bidding", 20 June 2019 (URL: https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf), pp. 20-1.

[9] See "lat" and "long" in "Object: Geo" in "AdCom v1, IAB TechLab", March 2022 (URL: https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20v1.0%20FINAL.md#object_geo); and see "HyperlocalSet" in "Authorized Buyers Proto v253", Google (URL: https://developers.google.com/authorized-buyers/rtb/realtime-bidding-guide#hyperlocalset-object).

[10] See "lat" and "long" in "Object: Geo" in "AdCom v1, IAB TechLab", March 2022 (URL: https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20v1.0%20FINAL.md#object_geo); and see "HyperlocalSet" in "Authorized Buyers Proto v253", Google (URL: https://developers.google.com/authorized-buyers/rtb/realtime-bidding-guide#hyperlocalset-object).

[11] For detail on the scale of RTB see "The Biggest Data Breach ICCL report on the scale of Real-Time Bidding data broadcasts in the U.S. and Europe", ICCL, May 2022 (URL: https://www.iccl.ie/digital-data/iccl-report-on-the-scale-of-real-time-bidding-data-broadcasts-in-the-u-s-and-europe/).

[12] Data obtained by ICCL. See "The Biggest Data Breach ICCL report on the scale of Real-Time Bidding data broadcasts in the U.S. and Europe", ICCL, May 2022 (URL: https://www.iccl.ie/digital-data/iccl-report-on-the-scale-of-real-time-bidding-data-broadcasts-in-the-u-s-and-europe/).

[13] The number of broadcasts per minute in Germany is calculated by dividing the 6.4 billion RTB broadcasts every day by the average number of minutes that Germans spend online per day (326). This average time spent is from a Global Web Index survey of Germans aged 16-64 conducted in Q3 of 2020, published by HooteSuite and We Are Social (URL: https://wearesocial-cn.s3.cn-north-1.amazonaws.com.cn/common/ digital2021/digital-2021-global.pdf).

[14] For detail on the scale of RTB see "The Biggest Data Breach ICCL report on the scale of Real-Time Bidding data broadcasts in the U.S. and Europe", ICCL, May 2022 (URL: https://www.iccl.ie/digital-data/iccl-report-on-the-scale-of-real-time-bidding-data-broadcasts-in-the-u-s-and-europe/).

[15] "The Biggest Data Breach ICCL report on the scale of Real-Time Bidding data broadcasts in the U.S. and Europe", ICCL, May 2022 (URL: https://www.iccl.ie/digital-data/iccl-report-on-the-scale-of-real-time-bidding-data-broadcasts-in-the-u-s-and-europe/), p. 6.
The UK Competition & Markets Authority also found that Google has market power in RTB, in "Online platforms and digital advertising Market study final report", UK Competition & Markets Authority, 1 June 2020 (URL: https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf), p. 20.

[16] According to BuiltWith, checked on 21 July 2023 (URL: https://trends.builtwith.com/ads/DoubleClick.Net).

[17] AppFigures reports 1.5 million Android apps and 127,000 iOS apps. Checked 21 July 2023.

[18] "Authorized Buyers Proto v253", Google (URL: https://developers.google.com/authorized-buyers/rtb/realtime-bidding-guide#hyperlocalset-object).

[19] "The Biggest Data Breach ICCL report on the scale of Real-Time Bidding data broadcasts in the U.S. and Europe", ICCL, May 2022 (URL: https://www.iccl.ie/digital-data/iccl-report-on-the-scale-of-real-time-bidding-data-broadcasts-in-the-u-s-and-europe/), p. 6.
The UK Competition & Markets Authority also found that Google has market power in RTB, in "Online platforms and digital advertising Market study final report", UK Competition & Markets Authority, 1 June 2020 (URL: https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf), p. 20.

[20] Paul Vines et al, 2017, "Exploring ADINT: Using Ad Targeting for Surveillance on a Budget — or — How Alice Can Buy Ads to Track Bob" https://adint.cs.washington.edu/ADINT.pdf

[21] Google sends EU RTB data to
Pangle DSP (TikTok),
北京泛为信息科技有限公司 (Fancy Digital),
世纪富轩科技发展（北京）有限公司 (DHgate Group),
顶新 (www.360.cn),
Umeng Plus Beijing Technology Ltd.,
Xiaomi DSP, and
LnData (Beijing Mega Engine Network Technology Co., Ltd.,
according to Google in "Ad technology providers", Google (URL: https://support.google.com/admanager/answer/9012903?hl=en#).

[22] For China, see Article 35 and 48 of the Data Security Law of the People's Republic of China, adopted 10 June 2021 (URL: www.npc.gov.cn/englishnpc/c2759/c23934/202112/t20211209_385109.html).

[23] Google sends EU RTB data to
AiData,
Yandex,
AdSniper,
AiData,
ROMIR (rmh.ru),
Programmatic Ecosystem LLC (mediasniper.ru),
Mail.ru,
Tinkoff.ru,
Adnetic (adnetic.ru),
Adriver (adriver.ru),
MI DSP (whiteboxdigital.ru),
MT-TECHNOLOGIES LLC (wi-fi.ru),
Mobile Innovations (paypersale.ru), Reactive (reactive-agency.ru),
Retail Rocket LLC (retailrocket.ru),
Sape (sape.ru),
Stream (stream.ru), Vital Media (zefirgood1.ru),
OTM Worldwide LLC (otm-r.com).
According to Google in "Ad technology providers", Google (URL: https://support.google.com/admanager/answer/9012903?hl=en#).

[24] See the various "SORM" (Systema Operativno-Razisknikh Meropriatiy) provisions. For example "On approval of the Requirements for telecommunication networks for carrying out operational investigative activities. Part I. General requirements", Ministry of Information Technology and Communications of the Russian Federation, 16 January 2008 (archived URL: https://web-archive-org.translate.goog/web/20110206080134/http://www.minsvyaz.ru/ministry/documents/1548/3226.shtml?_x_tr_sl=auto&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=wapp).

[25] Dun & Bradsteet's subsidiary Eyeota sells RTB segments on Russians provided by AiData on "Visitors of political opposition sites". See Row 1,921 of **Doc 2**.

[26] Microsoft Xandr sends EU RTB data to Yandex, AdSniper, Xaxis Russia, and Mail.ru, according to Microsoft Xandr in "Supply partners", Xandr (URL - archive from 29 March 2021 because the original has been removed from public view by Xandr - http://www.iccl.ie/wp-content/uploads/2022/01/K33-xandr-incoming-bid-requestssupply_partners_3-29-2021.pdf).

[27] Microsoft Xandr sends EU RTB data to Beijing Supertool Internet Technology Co., Td Best Of The Best Plc, Beijing POP Infotech Ltd, Beijing POP Infotech Ltd, Defy Media, according to Microsoft Xandr in "Supply partners", Xandr (URL - archive from 29 March 2021 because the original has been removed from public view by Xandr - http://www.iccl.ie/wp-content/uploads/2022/01/K33-xandr-incoming-bid-requestssupply_partners_3-29-2021.pdf)

[28] "Ad technology providers", Google (URL: https://support.google.com/admanager/answer/9012903?hl=en#).

[29] Company record of Rayzone Group Ltd., company number 514501899, Israeli company records, dated September 2023.

[30] "Your Ad Data Is Now Powering Government Surveillance", Bloomberg, 11 May 2023 (URL: https://www.bloomberg.com/news/articles/2023-05-11/surveillance-company-turns-ad-data-into-government-tracking-tool).

[31] "Echo – Global Virtual SIGINT System", Rayzone (No longer public. Archived at URL: https://web.archive.org/web/20210724230515/https://rayzone.com/echo-global-virtual-sigint-system/).

[32] OpenX, Smaato, AdColony, according to the WSJ reporter who broke the story, who spoke to ICCL. Near Intelligence's website also confirms that the company uses "Near uses location intelligence from several sources. This data comes from various partners via Real

Time Bidding (RTB), including both Bid requests and SDK data" (URL: https://near.com/uk/platform/).

[33] Called "Engage", according to Near's website (URL: https://near.com/uk/solutions/generate-qualified-traffic/)

[34] https://near.com/uk/expertises/audience-curation/

[35] As recently acknowledged by the US Director of National Intelligence, in "Office of the Director of National Intelligence Senior Advisory Group Panel on Commercially Available Information", U.S. Director of National Intelligence, 27 January 2022 (URL: https://www.odni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf), p. 4.

[36] Google, Twitter ("mopub"), Yahoo!, Pubmatic, Bidswitch, and many other significant RTB companies are cited as source in the graphic on Patternz website, (Version no longer Public. Archived version at URL: https://web.archive.org/web/20210622100652/http://isasecurity.org/patternz (live version at http://isasecurity.org/patternz has removed some references to advertising data)).

[37] Segment name: "Government - Intelligence & Counter terrorism". Dun & Bradstreet ("Eyeota") provides segments on all of these countries. France, Germany, Switzerland, Sweden, Spain, the Netherlands, Poland, Italy, Finland, Denmark, Austria, Czech Republic, Belgium, Ireland, and the UK. **See endnotes 49-63.**

[38] See "segment description" column of row 39,138 of **Doc 3**.

[39] See Content Taxonomy v3.0 (URL: https://iabtechlab.com/standards/content-taxonomy/).

[40] "IAB Audience Taxonomy" v1 and v1.1. (URL: https://iabtechlab.com/standards/audience-taxonomy/).

[41] Data firms Bombora, comScore, Grapeshot, and Pier 39 offer the segment "Airbus_All Employees_LP_Dec_2018". For example at row 283436 of **Doc 1**.

[42] comScore offers the segment "Custom Targeting: BAE Systems - Engineers (Brand Safe) (Proximic Agent)" at row 215,643 of **Doc 1**.

[43] Grapehot offers the segment "crunchdmc_babcock_bae_system_job_cuts (Grapeshot)" at row 164,701 of **Doc 1**.

[44] Segment: "GKN Aerospace_All Employees_LP_Jan_2019"at row 289,830 of **Doc 1.**

[45] "GKN aerospace overhauls first F-35 wheels and brakes assemblies for European fleet", GKN, 22 June 2023 (URL: https://www.gknaerospace.com/en/newsroom/news-releases/2023/gkn-aerospace-overhauls-first-f-35-wheels-and-brakes-assemblies-for-european-fleet/).

[46] For example, for Germany see rows 48,128 of **Doc 3**.

[47] Segment: "ShareThis - CA, FR, DE, UK, AU, HK - Law & Government - Government - Courts & Judiciary" at row 127,621 of **Doc 1**.

[48] Segment: "ShareThis - CA, FR, DE, UK, AU, HK - Law & Government - Government - Legislative Branch" at 127,627 of **Doc 1**.

[49] Segment: "ShareThis - CA, FR, DE, UK, AU, HK - Business & Industrial - Energy & Utilities - Nuclear Energy" at row 127,348 of **Doc 1**.

[50] Segment: "ShareThis – CA, FR, DE, UK, AU, HK – Business & Industrial – Aerospace & Defense - Defense Industry" in row 127,312 of **Doc 1**.

[51] Segment: "ShareThis - CA, FR, DE, UK, AU, HK - Business & Industrial - Aerospace & Defense - Space Technology" at row 127,313 of **Doc 1**.

[52] Segments: "ATT_SecurityRiskConference_Hotels (Factual)", "ATT_SecurityRiskConference_Restaurants (Factual)", "ATT_SecurityRiskConference_Venue (Factual)" at rows 268,573-6 of **Doc 1**.

[53] Segment: "MilitaryBases_Geo_6Miles_AdSquare" at row 376,082 of **Doc 1**.

[54] Row 311,174 of **Doc 1**, segment name: "Country-Specific Audiences > Germany > B2B > Firmographic > Industry > Government > Civil Service (BlueKai)"

[55] Row 311,175 of **Doc 1**.

[56] **Doc 2**, row 10,192.

[57] **Doc 2**, row 100,44.

[58] **Doc 2**, row 10,099.

[59] "LiveRamp Acquires Pacific Data Partners to Revolutionize B2B Marketing with People-Based Precision", LiveRamp, 15 February 2018 (URL: https://investors.liveramp.com/news-and-events/press-release-details/2018/LiveRamp-Acquires-Pacific-Data-Partners-to-Revolutionize-B2B-Marketing-with-People-Based-Precision/default.aspx).

[60] **Doc 3**, row 727.

[61] **Doc 3**, row 8,341.

[62] **Doc 3**, row 15,784.

[63] **Doc 3**, row 23,147.

[64] **Doc 3**, row 31,208.

[65] **Doc 3**, row 39,138.

[66] **Doc 3**, row 49,042.

[67] **Doc 3**, row 59,859.

[68] **Doc 3**, row 67,263.

[69] **Doc 3**, row 76,746.

[70] **Doc 3**, row 84,484.

[71] **Doc 3**, row 93,377.

[72] **Doc 3**, row 102,818.

[73] **Doc 3**, row 112,167.

[74] **Doc 3**, rows 120,303.

[75] For example, for Austria see row 1,373 of **Doc 3**. Segment description: "Users who are decision makers

for the Government Industry, specifically National Security and International Affairs".

[76] For example, see row 10,592 in **Doc 3**, segment name: "EMEA Selling Simplified - Job Function - Most Senior Contact - Seniority - Senior Officer, C-Level".

[77] Row 13,779 of **Doc 3**.

[78] For example, for Germany see Row 50,670 of **Doc 3**.

[79] **Doc 3**, rows 740; 8,354; 15,797; 23,160; 31,221; 39,151; 49,055; 59,872; 67,276; 76,759; 84,497; 93,390; 102,831; 112,180; and 120,316.

[80] For example, for Czech Republic see row 15,797 of **Doc 3**. Segment name: "Global ShareThis - Law and Government - Military - Army".

[81] For example, for Finland see row 31,224 of **Doc 3**. See also row 10,037 of **Doc 2**. Segment description: "people who work in the navy".

[82] For example, see row 11,097 in **Doc 3**, segment name: "Global ShareThis - People and Society - Family and Relationships - Military Families".

[83] Patternz marketing material (version no longer public. Archived URL: https://web.archive.org/web/20231003181009/https://sovsys.co/wp-content/uploads/2020/04/PATTERNZ-NATIONAL-SECURITY-PATTERN-DETECTION.pdf).

[84] "billions of ad transactions daily" according to the website about Patternz, Israeli Security Academy company website (URL: http://isasecurity.org/patternz).; "87 SSPs and [ad]exchanges", according to Patternz marketing material (version no longer public. Archived URL: https://web.archive.org/web/20231003181009/https://sovsys.co/wp-content/uploads/2020/04/PATTERNZ-NATIONAL-SECURITY-PATTERN-DETECTION.pdf). Google, Twitter ("mopub"), Yahoo!, Pubmatic, Bidswitch, and many other significant RTB companies are cited as source in the graphic on Patternz website, (Version no longer Public. Archived version at URL: https://web.archive.org/web/20210622100652/http://isasecurity.org/patternz (live version at http://isasecurity.org/patternz has removed some references to advertising data)).

[85] Public version no longer available. Archived version at URL: https://web.archive.org/web/20231003181009/https://sovsys.co/wp-content/uploads/2020/04/PATTERNZ-NATIONAL-SECURITY-PATTERN-DETECTION.pdf.

[86] Patternz, Israeli Secutiy Academy company website (URL: http://isasecurity.org/patternz).

[87] Both CIA and KGB used M.I.C.E. during the Cold War. See for example "An Alternative Framework for Agent Recruitment: From MICE to RASCLS", Studies in Intelligence, v 57, no. 1, March 2013 (URL: "An Alternative Framework for Agent Recruitment: From MICE to RASCLS", Studies in Intelligence, v 57, no. 1, March 2013 ("Money, Ideology, Compromise, and Ego" https://www.cia.gov/static/Alt-Framework-Agent-Recruitment.pdf)". See interview with KGB defector Stanislas Levchenko, 3 June 1985 (CBS Morning News) (URL: https://www.cia.gov/readingroom/docs/CIA-RDP90-00552R000403690002-9.pdf).

[88] See IAB Audience Taxonomy

[89] See IAB Context Taxonomy

[90] Row 124,867 of Doc 1.

[91] Rows 115,959 and 115,959 of **Doc 1**.

[92] Rows 459,351 and 459,354 of **Doc 1**.

[93] Rows 215,311 and 548,275 of **Doc 1**.

[94] Row 626,955 of **Doc 1**.

[95] Row 5,300 of **Doc 2**.

[96] Row 4,973 of **Doc 2**.

[97] Row 5,060 of **Doc 2**.

[98] Row 548,286 of Doc 1, segment name: "Health & Fitness::Incest/Abuse Support - comScore (content relevance)". See also row 548,286 and 621,661.

[99] Row 22,317 of **Doc 1**, segment: "prhlthmd_health_incest_abuse_support (Grapeshot)".

[100] Row 85,536 of Doc 1, segment: "IAB_T2_INCEST (Integral/IAS) Contextual"

[101] Row 35,476 of **Doc 1**, segment name: "DoubleVerify - DV: Contextual>Health & Fitness>Incest/Abuse Support".

[102] Segment name: "amnetfr_communaute_gay (Grapeshot)" at row 202,559 of **Doc 1**.

[103] Segment name: "amnetfr_spf_activite_physique_femmes_menopause (Grapeshot)" at row 140,478 of **Doc 1**.

[104] For example, see row 226,294 of **Doc 1**, Segment: "Fidall > FR > Lingerie buyers > Rougegorge lingerie (adsquare)".

[105] example: degree of affinity to various psychological traits including "dutiful", "combative", "dominant", "dreamy", "materialistic". See rows 191,336 to 191,363; and 223395; 223412; 223413; 223417; 223554; 223567; 223606; 223678; 223682; 223698; 223705; 223794; 223798; and 223804 of **Doc 1** for "psychological values. For example, see row 191,351 of Doc 1, Segment name: "KBM Group - Germany - AZ Direct | Psychological Values | Psychological Values | Dutiful - low affinity".

[106] "Pillar Investigates: USCCB gen sec Burrill resigns after sexual misconduct allegations", 20 July 2021 (URL: https://www.pillarcatholic.com/p/pillar-investigates-usccb-gen-sec).

[107] "Catholic group spent millions on app data that tracked gay priests", Washington Post, 9 March 2023 https://www.washingtonpost.com/dc-md-va/2023/03/09/catholics-gay-priests-grindr-data-bishops/

[108] See IAB Audience Taxonomy

[109] See Content Taxonomy v1-3.0, IAB TechLab (URL: https://github.com/InteractiveAdvertisingBureau/Taxonomies/tree/main/Content%20Taxonomies).

[110] For example, see row 15,362 of **Doc 3**, "Users who Gamble" in the Czech Republic.

[111] For example, see row 30,194 of **Doc 3** , segment name "DK GDR - Online gambling / betting - Betting - High Spender - Tips, Pool, Lottery" in Denmark.

[112] Row 226875 of **Doc 1**.

[113] Row 70,545 of **Doc 3**, segment name: "Audiences that are likely to have moderate political views" in Italy, provided by comScore.

[114] Row 55,131 of **Doc 3**. Provided by Experian.

[115] Row 28,564 of **Doc 3**, Provided by GDR.

[116] Row 129,068 of **Doc 3**, provided by Starcount.

[117] Some or all RTB ad exchanges reject bid requests unless they contain ID codes about the person who will see the ad. For example, Microsoft Xandr says "*Xandr only responds to a bid when we can map your request to a Xandr user ID*" in "Supply partners", Xandr (URL - archive from 29 March 2021 because the original has been removed from public view by Xandr - http://www.iccl.ie/wp-content/uploads/2022/01/K33-xandr-incoming-bid-requestssupply_partners_3-29-2021.pdf). Similarly, Magnite's documentation, which says the identifier is always present (URL: https://www.iccl.ie/wp-content/uploads/2023/08/8-8-2023-Magnite-Streaming-—-OpenRTB-Specification-for-Bidders-_-Magnite-Help-Center.pdf).
Similarly, Meta's RTB system, the Meta Audience Network, requires a unique "mandatory" unique ID code. In "Server-to-server bidding", Meta for Developers (URL: https://developers.facebook.com/docs/audience-network/overview/in-house-mediation/server-to-server). See also a brief overview of the data standard for cross-referencing data at "Data Transparency Standard 1.0", IAB Tech Lab, 27 June 2019 (URL: https://iabtechlab.com/wp-content/uploads/2019/06/Data-Transparency-Standard-1.0-Final-June-2019.pdf).

[118] user agent string, high resolution timestamp, location, URL etc.

[119] OpenRTB v3 (AdCOM) and OpenRTB v2.x. https://iabtechlab.com/standards/openrtb/.

[120] Based on industry data for a 30 day period, see "The Biggest Data Breach ICCL report on the scale of Real-Time Bidding data broadcasts in the U.S. and Europe", ICCL, May 2022 (URL: https://www.iccl.ie/digital-data/iccl-report-on-the-scale-of-real-time-bidding-data-broadcasts-in-the-u-s-and-europe/).

[121] https://developers.google.com/authorized-buyers/rtb/realtime-bidding-guide.

[122] Data protection supervisory authorities can order them to do so in order to comply with the security obligations in the GDPR, Article 5(1)f and Article 32.

[123] under GDPR Article 70(1)(e).

[124] "Capacity enhancement guide: securing web browsers and defending against malvertising for federal agencies", CISA, January 2021 (URL: https://www.cisa.gov/sites/default/files/publications/Capacity_Enhancement_Guide-Securing_Web_Browsers_and_Defending_Against_Malvertising_for_Federal_Agencies.pdf), p. 2.