

Dr Johnny Ryan testimony. Understanding the Digital Advertising Ecosystem and the Impact of Data Privacy and Competition Policy.

Thank you Chairman Graham, Senator Feinstein, and distinguished members.

I represent Brave, a privacy-focussed web browser.

Our CEO, Brendan Eich, is the inventor of JavaScript, the most popular programming language in the world. He also co-founded Firefox, and built it into one of the world's most popular browsers.

Brave is headquartered in San Francisco and we have staff in 17 states. The number of people using our browser grew 600 percent last year.

So what I am about to say might surprise you. We view the GDPR as a great leveller. It can establish the conditions to allow young, innovative companies like ours to flourish.¹

Today, big tech companies create cascading monopolies by leveraging users' data from one line of business to dominate other lines of business too.² This hurts nascent competitors, stifles innovation and reduces consumer choice.³

However, two elements in the GDPR can fix this – if they are enforced. First, Article 5(1)(b), is the “purpose limitation” principle,⁴ which ring fences personal data held by companies so they can't use it outside of consumer expectations. They need a legal basis for each data processing purpose.⁵

Second, Article 7 (3) requires that an opt-in must be as easy to undo as it was to give in the first place, and that people can do so without detriment. Once this is enforced, consent messages⁶ will become far less annoying in Europe – because if a company insists on harassing you to opt in, and you finally click OK, it will be required to keep reminding you that you can opt back out again.⁷

These two GDPR tools, the “purpose limitation principle”, plus the ease of withdrawal of consent, enable freedom. Freedom for the market of users to softly “break up” – and “un-break up” – big tech companies by deciding what personal data can be used for.

Senators, the GDPR is risk based. That means Big Tech that creates big risks get big scrutiny and potentially big penalties. Regulators are only starting to enforce the GDPR and it will take years to have full effect. But already, things are looking bleak for our colleagues at Google and Facebook.

Their year-over-year growth declined steadily in Europe since the GDPR⁸ – despite a buoyant advertising market. They face multiple investigations and it is very likely that they will be forced to change how they do business. (Google’s consent has already been ruled invalid.⁹) And things are even bleaker for other tracking companies, that don’t have a search business to fall back on, as Google does.

Whereas -- we hear anecdotally that publishers are doing better than before! Lax privacy law hasn’t helped publishers.

Let me tell you what happens almost every single time you visit a website: data about you is broadcast to tens or hundreds of companies, which lets advertisers compete for the opportunity to show you an ad.¹⁰ Advertising is necessary, and this sounds OK.

But wait until you hear what information about you is in that big broadcast: it can include your - inferred - sexual orientation, political views, whether you are Christian, Jewish, or Muslim, etc., whether you have AIDS, erectile dysfunction, or bi-polar disorder.¹¹ It includes what you are reading, watching, and listening to.¹² It includes your location, sometimes right up to your exact GPS coordinates.¹³ And it includes unique ID codes that are as specific to you as is your social security number, so that all of this data can be tied to you over time.¹⁴ This allows companies you have never heard of to maintain intimate profiles on you, and on everyone you have ever known.¹⁵

This is not necessary for smart advertising. The latest research shows that this profiling nets publishers only zero point zero zero zero zero eight of a dollar extra per ad.¹⁶ That’s only an extra 4% revenue!

Whereas “contextual” ads, which don’t broadcast your intimate details, would save publishers 55 to 70 percent in “adtech tax”,¹⁷ and avoid having their audiences bought cheaper elsewhere. Advertisers would also recover billions per year from “ad bot fraud” – though few realize this.¹⁸ Privacy law will help the digital advertising ecosystem.

Let me conclude by urging you to enact strong privacy rules so that a healthy marketplace can develop. Give consumers freedom to choose the companies and services they want to reward.

The GDPR is based largely on American principles. We urge you to bring them home.

Thank you.

Notes

- ¹ See Brave to National Telecommunications and Information Administration, Docket No. 180821780– 8780–01 (Privacy RFC), 5 November 2018 (URL: <https://brave.com/ntia-federal-privacy-law/>); see also Brave to Federal Trade Commission, Docket FTC-2018-0100, 7 January 2019 (URL: <https://brave.com/brave-ftc-jan-2019/>); and Brendan Eich to Senate Committee on Commerce, Science, and Transportation, 1 October 2018 (URL: <https://brave.com/us-gdpr-senate/>).
- ² The cross-use of data between different lines of business is analogous to the tying of two products. Indeed, tying and cross-use of data can occur at the same time, as Google Chrome’s latest “auto sign in to everything” controversy illustrates.
- ³ Competition authorities in other jurisdictions have addressed this matter. As early as 2010, France’s Autorité de la concurrence highlighted the topic (in Opinion 10-A-13 on the cross-usage of customer databases). In 2015, Belgium’s regulator fined the Belgian National Lottery for reusing personal information acquired through its monopoly for a different, and incompatible, line of business.
- ⁴ As with many of the principles of the GDPR, this is based on the FIPPs of the 1974 US Privacy Act.
- ⁵ Consider for example the act of posting a photo on the Facebook Newsfeed for the first time. The distinct processing purposes involved might be something like the following list. The person posting the photo is only interested only the first four or five of these purposes. If purpose limitation is enforced, Facebook will be very vulnerable:
- To display your posts on your Newsfeed.
 - To display posts on tagged friends’ Newsfeeds.
 - To display friends posts that tag you on your Newsfeed.
 - To identify untagged people in your posts.
 - To record your reaction to posts to refine future content for you, which may include ethnicity, politics, sexuality, etc..., to make our Newsfeed more relevant to you.
 - To record your reaction to posts to refine future content for you, which may include ethnicity, politics, sexuality, etc..., to make ads relevant to you.
 - To record your reaction to posts to refine future content for you, which may include ethnicity, politics, sexuality, etc..., for advertising fraud prevention.
- ⁶ It does not necessarily matter what a person clicks on when shown one of the industry’s “consent notices”, because there is no technical security measure to prevent these companies from sharing the data with their business partners under the table. For this – and other reasons - the consent system that the industry came up with is itself under investigation for infringing the GDPR. See note 15, below, and see “Risks in IAB Europe’s proposed consent mechanism”, PageFair, 20 March 2018 (URL: <https://pagefair.com/blog/2018/iab-europe-consent-problems/>).

-
- ⁷ GDPR, Article 7 (3) and (4), and Recital 42. See also “Guidelines on Consent under Regulation 2016/679”, European Data Protection Board, 10 April 2018.
- ⁸ See year-over-year growth figures in Alphabet quarterly filings, Q1 2018 to Q1 2019 (URL: <https://abc.xyz/investor/>), and Facebook quarterly filings, Q1 2018 to Q1 2019 (<https://investor.fb.com>).
- ⁹ “Délibération n°SAN-2019-001 du 21 janvier 2019 Délibération de la formation restreinte n° SAN – 2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société GOOGLE LLC”, Commission Nationale de l'Informatique et des Libertés, 21 January 2019 (URL: <https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000038032552&fastReqId=2103387945&fastPos=1>).
- ¹⁰ “Ryan report on behavioral advertising and personal data”, evidence submitted to the Irish Data Protection Commission, and UK Information Commissioner's Office, 12 September 2018 (URL: <https://brave.com/Behavioural-advertising-and-personal-data.pdf>).
- ¹¹ See Google’s RTB “Publisher Verticals” list, which is referred to in several contexts from the Google Authorized Buyers Proto (URL: <https://developers.google.com/authorized-buyers/rtb/downloads/publisher-verticals>); see also IAB OpenRTB “content taxonomies” list, which is referred to in several contexts in the IAB OpenRTB AdCOM API (https://www.iab.com/wp-content/uploads/2017/11/IAB_Tech_Lab_Content_Taxonomy_V2_Final_2017-11.xlsx).
- ¹² See “Ryan report on behavioral advertising and personal data” and “Examples of data in a bid request from IAB OpenRTB and Google Authorized Buyers’ specification documents” (URL: <http://fixad.tech/wp-content/uploads/2019/02/3-bid-request-examples.pdf>), evidence submitted to the Irish Data Protection Commission, and UK Information Commissioner's Office, 12 September 2018 and 20 February 2019.
- ¹³ See “Object: geo” in AdCOM Specification v1.0, Beta Draft”, IAB TechLab, 24 July 2018 (URL: <https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20v1.0%20FINAL.md>); and “Hyperlocal object”, “Point object”, “HyperlocalSet object” in Authorized Buyers Real-Time Bidding Proto”, Google, 23 April 2019 (URL: <https://developers.google.com/authorized-buyers/rtb/realtime-bidding-guide>).
- ¹⁴ See “Object: user” in AdCOM Specification v1.0, Beta Draft”, IAB TechLab, 24 July 2018 (URL: <https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20v1.0%20FINAL.md>); “hosted_match_data”, “google_user_id”, and “UserList object” in Authorized Buyers Real-Time Bidding Proto”, Google, 23 April 2019 (URL: <https://developers.google.com/authorized-buyers/rtb/realtime-bidding-guide>).
- ¹⁵ There is no technical control over where these data go once they are broadcast, and aside from the thousands of immediate recipients of the data. This is the subject of

a formal GDPR complaint filed in Ireland, the United Kingdom, Poland, Spain, Luxembourg, and the Netherlands. See <http://fixad.tech>.

For an indication of the scale of this problem, Google DoubleClick/Authorized Buyers is the largest “advertising exchange” involved in the “real time bidding” industry that conducts these broadcasts. It is installed on 8.4+ million websites and broadcasts personal data about visitors to these sites to 2,000+ companies. See “DoubleClick.Net usage statistics”, Builtwith.com (URL: <https://trends.builtwith.com/ads/DoubleClick.Net>) and “Ad Exchange Certified External Vendors”, Google Authorized Buyers (URL: <https://developers.google.com/third-party-ads/adx-vendors>), last updated 18 April 2019.

¹⁶ Marotta, Abjishkek, Acquisti, “Online Tracking and Publishers’ Revenues: An Empirical Analysis”, due for publication in June 2019. Professor Acquisti of Heinz College, Carnegie Mellon University, revealed that the results recently at the Chicago Booth School Stigler Centre 2019 Antitrust and Competition Conference.

¹⁷ The 70% figure is from The Guardian’s case against a major adtech company in 2017. To gather evidence, The Guardian masqueraded as an advertiser and bought ads on its own website. For every dollar that The Guardian spent as an advertiser, it received only 30c as a publisher. The publisher got 30%, adtech took 70%. This is known as the ad tech tax. The 55% figure is from “The Programmatic Supply Chain: Deconstructing the Anatomy of a Programmatic CPM”, IAB, March 2016.

¹⁸ For example, at least \$5.8 billion of their spend is stolen by “ad fraud” or “bot fraud” criminals. Other estimates are higher: \$50 billion by 2025. See “Compendium of Ad Fraud Knowledge for Media Investors”, World Federation of Advertisers, 2016 (URL: https://www.wfanet.org/app/uploads/2017/04/WFA_Compndium_Of_Ad_Fraud_Knowledge.pdf); see also “2018-2019 Bot baseline: fraud in digital advertising”, Association of National Advertisers (URL: <https://www.ana.net/getfile/25093>).