ETHICAL DATA ARE THE ANSWER. AT LONG LAST.

Dr Johnny Ryan @johnnyryan
Problem Set 1:
The “Facebook and Cambridge Analytica Problem”

How to enforce control over personal data that 3rd parties access from your websites?
Control Problem

No data protection of personal data accessed by 3rd party widgets and assets.
Control Problem

No data protection of personal data accessed by 3rd party widgets and assets.

AddThis processes the cross-web actions and content engagement behaviors from consumers across nearly every country in the world.

15M WEBSITES WORLDWIDE
1.9B+ UNIQUE USERS MONTHLY

Your websites Your audience
How RTB/programmatic works
“Behavioural” ad targeting & “programmatic” trading.

(This jargon means: automatic auctions for the right people’s attention)
Visitor
Site
SSP
Ad Exchange
DSP
DMP
Brand

“Supply side”

“Demand side”
The Daily Bugle

Exchange

DSP
DMP
Any one of the hundreds or thousands of parties receiving personal data via ad exchanges can profile and/or trade with unauthorized parties.

JavaScript ad creatives can summon unauthorized trackers.

Plus, other data leakage via SDKs on mobile, 3rd parties on page, logging on load of 3rd party assets, etc.
Risk

DATA LEAKAGE IN ONLINE ADVERTISING

This is the current process of real-time bidding that is used in online behavioural advertising.

Legend
- Channel of data leakage
- Money
- Personal data

Step 1. User requests webpage
Step 2. Ad server selects an SSP
Step 3. SSP selects an exchange
Step 4. Exchange sends bid requests to hundreds of partners
Step 5. Exchange lets some DMPs/DSPs to refresh cookie sync
Step 6. Exchange serves winning bid
Step 7. DSP serves agency creative
Step 8. Assets load from CDN
Step 9. Agency ad server loads verification vendor

Winning DSP
CDN
Agency ad server
Verification vendor

This is the current process of real-time bidding that is used in online behavioural advertising.
Problem Set 2: Consent for ad tracking

97%\(^1\) - 80%\(^2\) would reject 3rd party ad tracking (single dialogue)

1. "Research result: what percentage will consent to tracking for advertising?", PageFair, September 2017 (URL: https://pagefair.com/blog/2017/new-research-how-many-consent-to-tracking/)
A non-compliant GDPR consent screen (single screen)

[Site] and our partners set cookies and collect information from your [browser] [device] to provide you with [website] content, deliver relevant advertising and understand [web] audiences. [View partner info]

We use technology such as cookies on our site to collect and use personal data to personalize content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our partners who also use technologies such as cookies to collect and use personal data to personalize content and ads, to provide social media features and to analyse our traffic on our site and across the internet. View info on our partners and their use of this data. You can always change your mind and revisit your choices.

Manage use of your data  OK

No mention of the duration for which data are stored.
Breach of the GDPR, Article 13, paragraph 2, a

No precise description of a purpose of processing, and no notification of profiling.
Breach of the GDPR, Article 4, paragraph 11, and Article 13, paragraph 1, c, and paragraph 2, f, and Recital 60.

Appears to be hard to not give consent
Breach of the GDPR, Article 4, paragraph 11, and Recital 42, and Recital 32.

Conflation of multiple purposes
Breach of the GDPR, Article 5, paragraph 1, b, Recital 32, and Recital 43.
Do you believe that users will opt-in to tracking for the purposes of advertising?

- **No**
- **Yes, if denied access to the site otherwise**
- **Yes**

**Article 7(2) prohibits conditionality.**

1st party tracking on a website

- 13%
- 64%
- 23%

**Cannot deny access**

---

**PageFair**
Do you believe that users will opt-in to tracking for the purposes of advertising?

- No
- Yes, if denied access to the site otherwise
- Yes

1st party tracking on a website:
- 13%
- 64%
- 23%

3rd party tracking on a website:
- 46%
- 51%
- 3%

Tracking by any party, anywhere on the web:
- 65%
- 32%
- 3%
But the GDPR requires separate legal basis (consent in this case) for each processing purpose.
Examples of the many purposes of data processing in online behavioral advertising.

Each purpose requires its own opt-in.

<table>
<thead>
<tr>
<th>Purpose Description</th>
<th>Website</th>
<th>SSP</th>
<th>Ad Exchange</th>
<th>DSP</th>
<th>DMP</th>
<th>Advertiser</th>
<th>Fraud verification</th>
<th>Ad server</th>
<th>Analytics</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. To inform the agents of prospective advertisers that you are on visiting the web site, so that the website can solicit bids for the opportunity to show an ad to you.</td>
<td>Controller</td>
<td>Processor</td>
<td>Processor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. To combine your browsing habits with data they already have collected about you (and infer further insights about you) so that they can select relevant ads for you.</td>
<td>Controller</td>
<td>Controller</td>
<td>Controller</td>
<td>Controller</td>
<td>Controller</td>
<td>Controller</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. To use your browsing habits to build or improve a profile about you, in order to sell these data to partners for online marketing, credit scoring, insurance companies, background checking services, and law enforcement. This profile may include your income bracket, age and gender, habits, social media influence, ethnicity, sexual orientation, religion, political leaning, etc.</td>
<td>Controller</td>
<td>Controller</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. To identify whether you are the kind of person that its advertising clients want to show ads to.</td>
<td>Processor</td>
<td>Controller</td>
<td>Controller</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. To combine your browsing habits with data they already have collected about you (and infer further insights about you), to personalize the service or product that it offers you. This may include determining whether to offer you discounts. This profile may include your income bracket, age and gender, habits, social media influence, ethnicity, sexual orientation, religion, political leaning, etc.</td>
<td>Controller</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. To monitor your behavior on websites in order to determine if you have viewed or interacted with an ad.</td>
<td>Controller</td>
<td>Controller</td>
<td>Processor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. To determine whether you have purchased one of its products or services following your viewing of or interaction with an ad that it has paid for.</td>
<td>Controller</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. To combine your browsing habits with data they already have collected about you (and infer further insights about you), to verify that you are human rather than a “bot” attempting to defraud advertisers. This profile may include your income bracket, age and gender, habits, social media influence, ethnicity, sexual orientation, religion, political leaning, etc.</td>
<td>Controller</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9. To record the number of times you have viewed each ad, to prevent a single ad being shown to you too frequently.</td>
<td>Controller</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10. To combine your browsing habits with data they already have collected about you (and infer further insights about you), to understand how you and people similar to you browse the web. This profile may include your income bracket, age and gender, habits, social media influence, ethnicity, sexual orientation, religion, political leaning, etc.</td>
<td>Controller</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
An opt-in for **each** processing purpose

Help keep Example.com profitable

Let these companies combine your browsing habits for 6 months with data they already have collected about you to improve their profile of you, including by inferring insights, to show you relevant advertising. (This profile may include your income bracket, age and gender, habits, social media influence, ethnicity, sexual orientation, religion, political leaning, etc.).

**Duration**
Article 13, para 2, a.

**Unambiguous, Specific Affirmative Action. Not Yes by Default.**
Article 4, para 11, and Recital 32.

**Contact Details of the Data Controller, and List of Categories of Processor.**
Article 13, para 1, a, and Recital 42.

**Purpose of Processing, and Notification of Profiling.**
Article 4, paragraph 11, and Article 13, para 1, c, and para 2, f.

**Granular Opt-in for Several Purposes**
Recital 32, and Article 29 Working Party Guidance November 2017

**Details of Rights to Complain to Supervisory Authority, and to Access, Correct, and Transfer Data, Etc.**
Article 13, para 2, b, c, and d.

Learn about your data rights here.
Help keep Example.com profitable

Let these companies combine your browsing habits for 6 months with data they already have collected about you to improve their profile of you, including by inferring insights, to show you relevant advertising. (This profile may include your income bracket, age and gender, habits, social media influence, ethnicity, sexual orientation, religion, political leaning, etc.).

CONFIRM?

Item 1 of 9  Next

Viewing 2 of 251 partners

Acxiom GmbH
Martin Behaim Strasse 12,
63263 Neu-Isenburg,
Germany

Google Ltd.
Gordon House, Barrow St. Dublin 4, Ireland

Learn about your data rights here.

Explicit consent for special categories of personal data

“Explicit consent” (to process special categories of data)
Article 9, paragraph 2, a.

This design requires two tap / click / drag actions to signal consent explicitly.
Help keep Example.com profitable

Let these companies combine your browsing habits for 6 months with data they already have collected about you to improve their profile of you, including by inferring insights, to show you relevant advertising. (This profile may include your income bracket, age and gender, habits, social media influence, ethnicity, sexual orientation, religion, political leaning, etc.).

ON

Item 1 of 9  Next

Viewing 2 of 251 partners

**Acxiom GmbH**
Martin Behaim Strasse 12,
63263 Neu-Isenburg,
Germany

**Google Ltd.**
Gordon House, Barrow
St, Dublin 4, Ireland

Learn about your data rights here.

"Explicit consent" (to process special categories of data)
Article 9, paragraph 2, a.
Most people will not click OK to any of this

(So what is the answer?)
CLEAN, SAFE DATA*

*non-personal data
### GDPR scale: FACEBOOK

<table>
<thead>
<tr>
<th>Score</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Needs “opt-in” consent, but is unable to communicate with users</td>
<td></td>
</tr>
</tbody>
</table>
| 4     | Needs “opt-in” consent, but user has little incentive to agree | - Facebook Audience Network  
- WhatsApp advertising (see assumption 1) |
| 3     | Needs “opt-in” consent, and may get it |  |
| 2     | Can show an “opt-out” before using data | - NewsFeed ads (based only on personal data with no “special” personal data (e.g. ethnicity, political opinion, religious or philosophical beliefs, sexual orientation), unless marked “public” or visible to “friends of friends” (see assumptions 1 and 2)  
- Instagram ads (see assumption 1) |
| 1     | Out of scope of the regulation, if business is modified. |  |
| 0     | Already out of scope of the regulation. |  |

**Assumption 1.** That the use of personal data to target advertising will be accepted as a “compatible” purpose with the original purpose for which personal data were shared by users, under GDPR Article 6, paragraph 4. GDPR Recital 61 says that if the further processing is compatible then the company must alert the data subject that it is using their data for this further purpose before it starts processing. GDPR Article 21, paragraph 2 and 3 say that the data subject must be alerted about their right to object to their data being used for direct marketing, and can do so at any time. GDPR Recital 70 says this alert should be presented clearly and separately from any other information. However, the Article 29 Working Party’s opinion on purpose limitation notes that among the various things that the compatibility assessment must consider are “the impact of the further processing on the data subjects”.

**Assumption 2.** GDPR Article 6, paragraph 4, c, indicates a higher bar for “special categories of personal data” that reveal race, ethnicity, political opinion, religious or philosophical beliefs, trade union membership, or related to a data subject’s sex life or sexual orientation. However, this does not apply if the data have been “manifestly made public by the data subject” (GDPR, Article 9, paragraph 2, (e)). This may mean that the publicity settings that a user places on their post will prevent or enable those posts to be mined for advertising.
<table>
<thead>
<tr>
<th>Score</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Needs “opt-in” consent, but is unable to communicate with users</td>
<td>- Most personalized AdWords ads on Google properties including Search, Youtube, Maps, and the Google ads Network (including “remarketing”, “affinity audiences”, “in-market audiences”, “demographic targeting”, “similar audiences”, “Floodlight” cross-device tracking), “customer match”, “remarketing” (see assumption 1)</td>
</tr>
<tr>
<td>4</td>
<td>Needs “opt-in” consent, but user has little incentive to agree</td>
<td>- Gmail ads - Programmatic services (DoubleClick)</td>
</tr>
<tr>
<td>3</td>
<td>Needs “opt-in” consent, and may get it</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Can show an “opt-out” before using data</td>
<td>- Location targeting in Maps (see assumption 2)</td>
</tr>
<tr>
<td>1</td>
<td>Out of scope of the regulation, if business is modified.</td>
<td>- AdWords (if all personalized features are removed) on Google properties including Search, Youtube, Maps</td>
</tr>
<tr>
<td>0</td>
<td>Already out of scope of the regulation.</td>
<td>- “Placement-targeted” ads on Google properties.</td>
</tr>
</tbody>
</table>

**Assumption 1.** That the average user does not “sign in” to Google Search or Chrome. If, however, users did sign in then Google may be able to further process their data for other purposes.

**Assumption 2.** That the use of personal data to target advertising will be accepted as a “compatible” purpose with the original purpose for which personal data were shared by users, under GDPR Article 6, paragraph 4. GDPR Recital 61 says that if the further processing is compatible then the company must alert the data subject that it is using their data for this further purpose before it starts processing. GDPR Article 21, paragraph 2 and 3 say that the data subject must be alerted about their right to object to their data being used for direct marketing, and can do so at any time. GDPR Recital 70 says this alert should be presented clearly and separately from any other information. However, the Article 29 Working Party’s opinion on purpose limitation notes that among the various things that the compatibility assessment must consider are “the impact of the further processing on the data subjects.”
OLD INDUSTRY
Regulatory disincentive

Fossil Fuel

CO₂
N₂O

NEW CLEAN INDUSTRY
Regulatory incentive

Renewable Energy
**OLD INDUSTRY**

- Personal data
- Fossil Fuel
- CO₂
- Regulatory disincentive

**NEW CLEAN INDUSTRY**

- Non-personal data
- Renewable Energy
- Regulatory incentive

**Comparison**

- Ads (Conventional Data) vs. Ads (Ethical Data)
OLD INDUSTRY
Regulatory disincentive

Personal data

Fossil Fuel

NEW CLEAN INDUSTRY
Regulatory incentive

Non-personal data

Renewable Energy

Small, premium market

Personal data (with consent and enforceable protection)
Summary

1. “Consent” for RTB/programmatic is lawsuit bait.

2. Leakage of personal data from widgets & adtech exposes publishers, adtech, agencies, and brands to legal risk.

3. Media owners should ask for regulatory action: when you comply, you are not cheated by competitors.
JohnnyRyan1@Gmail.com

Twitter: @JohnnyRyan