



Durham
University

UCL CONFERENCE ON COMPETITION LAW AND POLICY IN A DATA-DRIVEN ECONOMY 2023

EXCLUSIONARY AND EXPLOITATIVE ABUSE OF CONSUMER DATA

Dr Anca Daniela Chirita, Durham University, Law School

<https://www.durham.ac.uk/staff/a-d-chirita/>



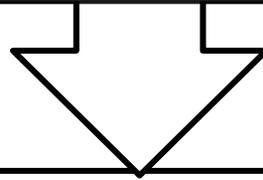
1. ABUSE OF CONSUMER DATA

Hybrid consumer data abuse

Algorithmic (price) discrimination

Consumer data combinations

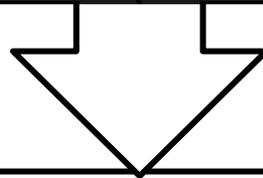
Digital tying



Negative exclusionary and exploitative welfare effects

Difficult to predict due to legal loopholes
A dense categorisation of abuse without repeated judicial experience

zero-priced freemiums, predictive algorithms, and marketing strategies.

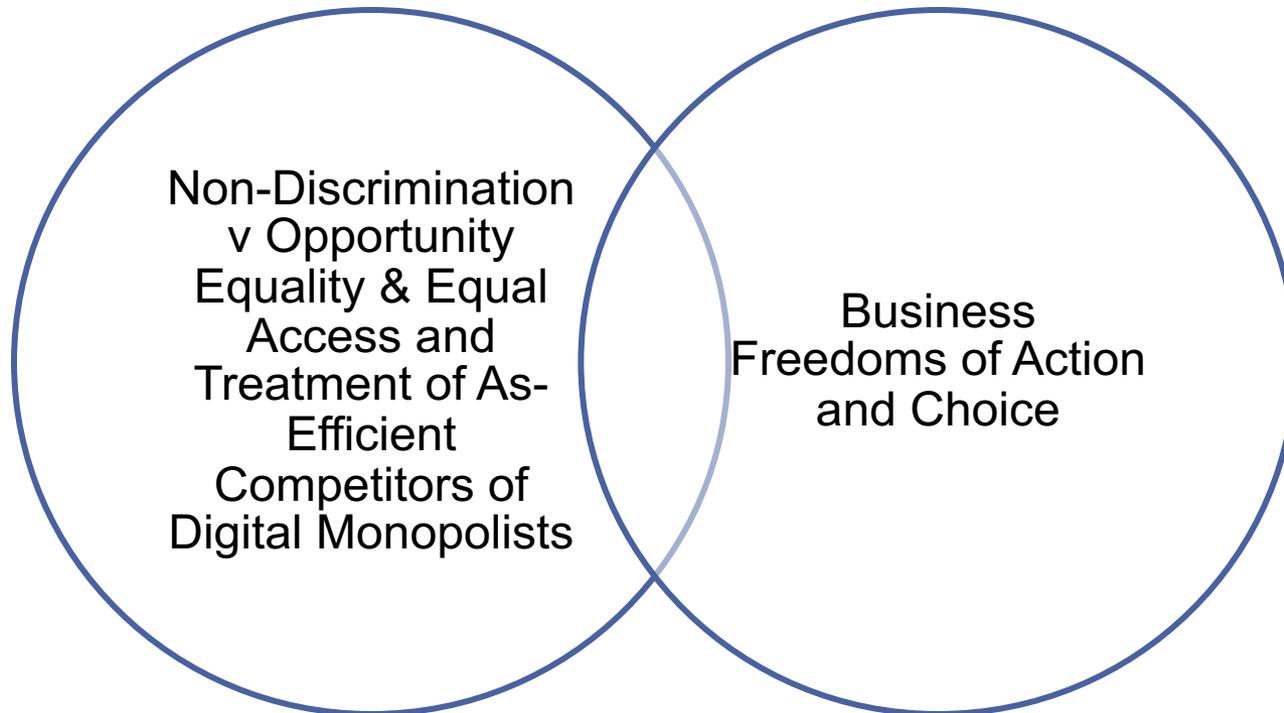


A more detailed drafting of Art. 102 as opposed to traditional law-making and judicial interpretation by the EU Courts of the concept of abuse?

Exploitation of the predictive analytics tools of business partners through aggregated data sharing or selling.
Exploitative consumer data abuse includes intermediate consumers.

If the consumers are marginalised to the point of exclusion through an excessive loss of privacy, then an exclusionary abuse does not target only the as-efficient competitors of digital monopolists.

2. EXCLUSIONARY CONSUMER DATA ABUSE



2.1. EXCLUSIONARY CONSUMER DATA ABUSE

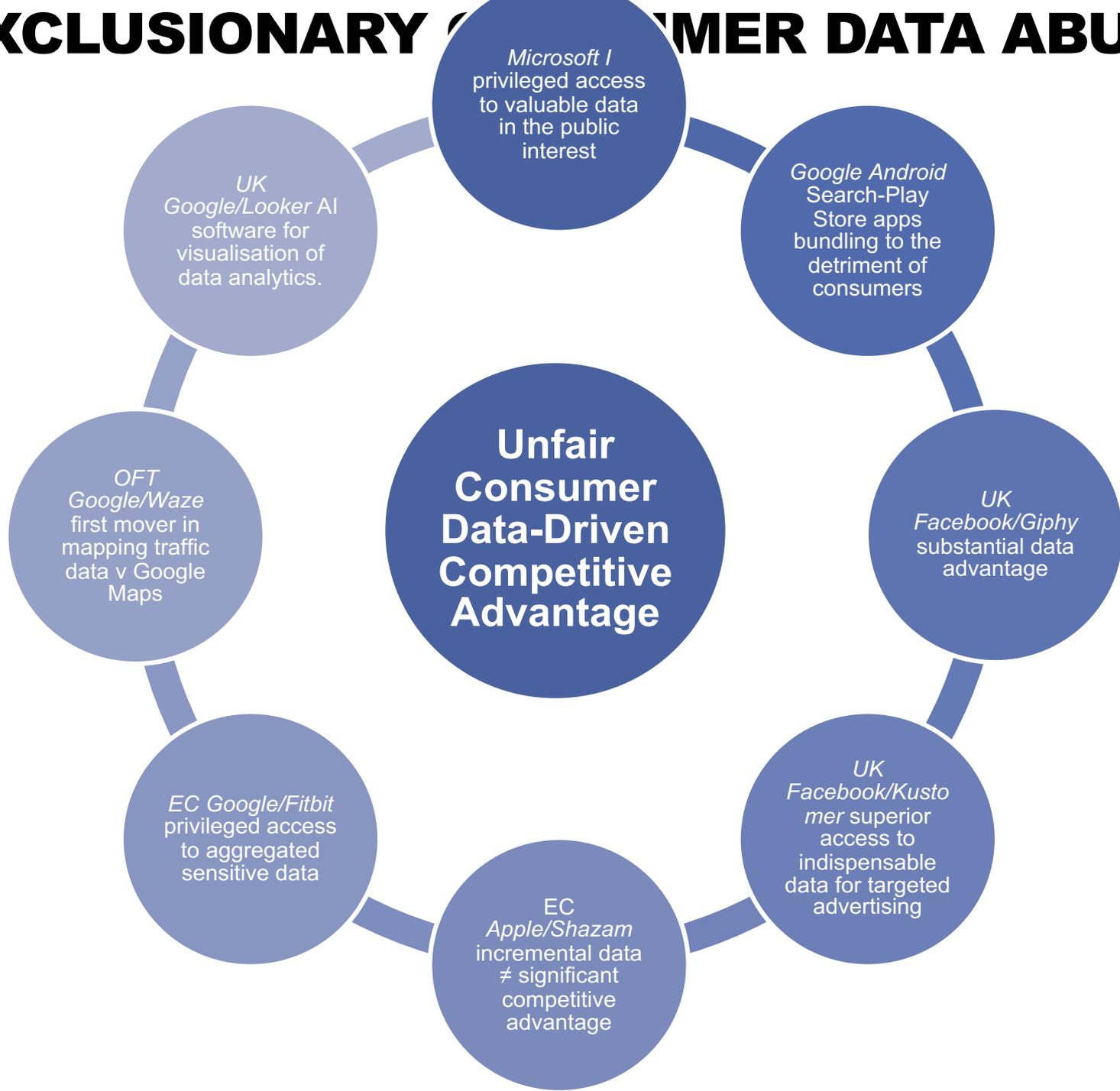


A dynamic interpretation of the consumer data abuse for the transactional value of consumer data

Effect on as-efficient competitors: unequal access to valuable consumer data

Unfair Consumer Data-Driven Competitive Advantage

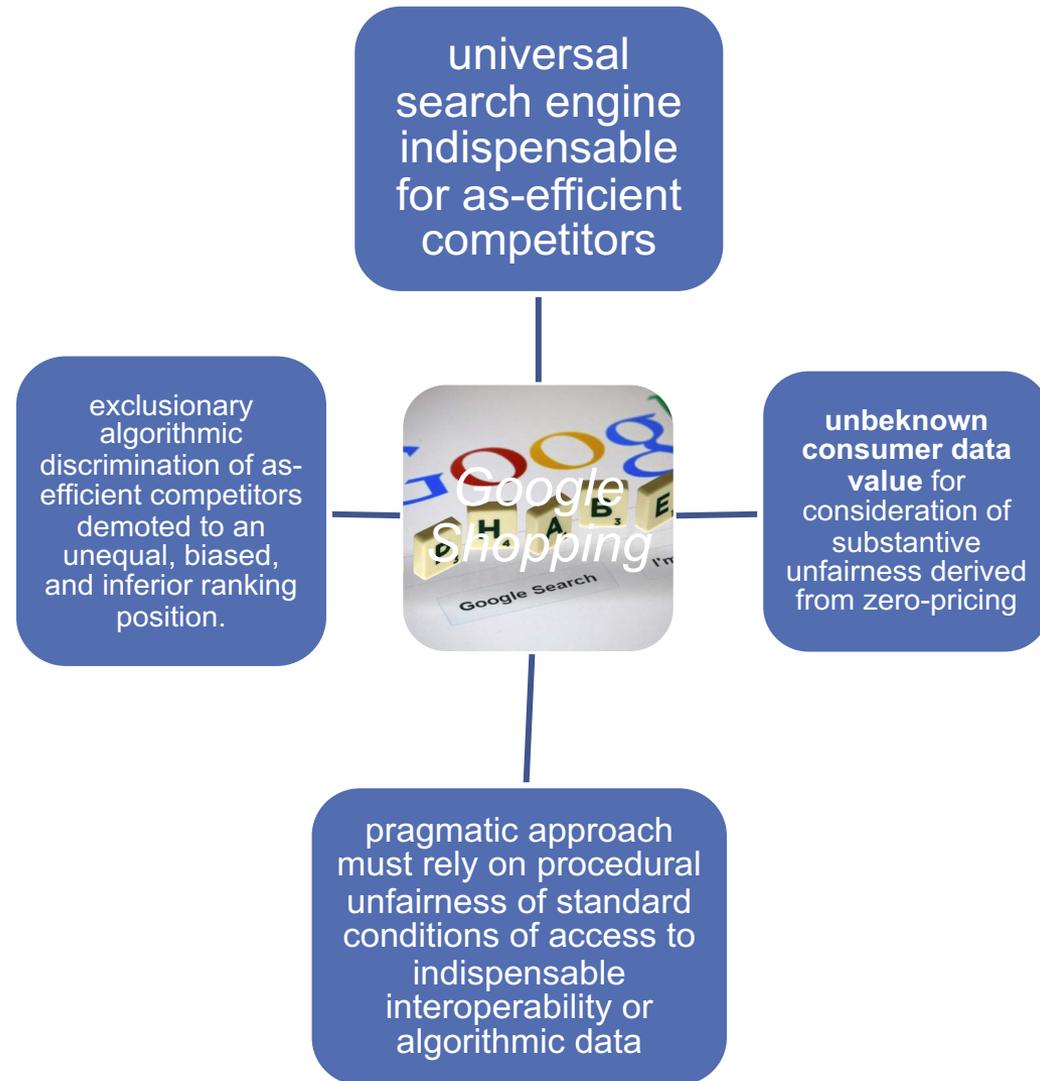
2.2. EXCLUSIONARY (UNFAIR) CONSUMER DATA ABUSE



2.3. EXCLUSIONARY CONSUMER DATA ABUSE

FRAND Terms of Access to Consumer Data – Paradox: the exclusionary theory of harm to residual competition comes at the expense of exploitative harm to the consumers.

- *GC Google Android:* access to consumer data and behaviour as key parameters of digital competition.
- *EC Google/Fitbit:* due to the vagueness of shared access to sensitive consumer data with third parties consumers are unaware of negative consequences of their bargaining power in the health insurance markets.
- *CMA Microsoft/Nuance* exploiting healthcare-specific speech data and access to Microsoft's speech recognition engine.



2.4. EXCLUSIONARY CONSUMER DATA ABUSE



Microsoft I&I (Windows Media Player and Internet Explorer) and Google Android applied the freedom of choice to behavioural consumer bias, following a pre-installed complimentary software, e.g., Play Store tied the Search app and Chrome browser, Apple pre-installed apps on iPhones.

Business
Freedoms of
Action and
Choice

Pre-installation bias made it difficult for as-efficient competitors to attract consumer data needed to improve their services.

Alternative developers had no real prospect of entering a zero-priced market.

Consumer empowerment added price, e.g., Microsoft Office, One Drive; paradox of having no evidence of consumer exploitation, i.e. price of consumer experience data



3. EXPLOITATIVE CONSUMER DATA ABUSE

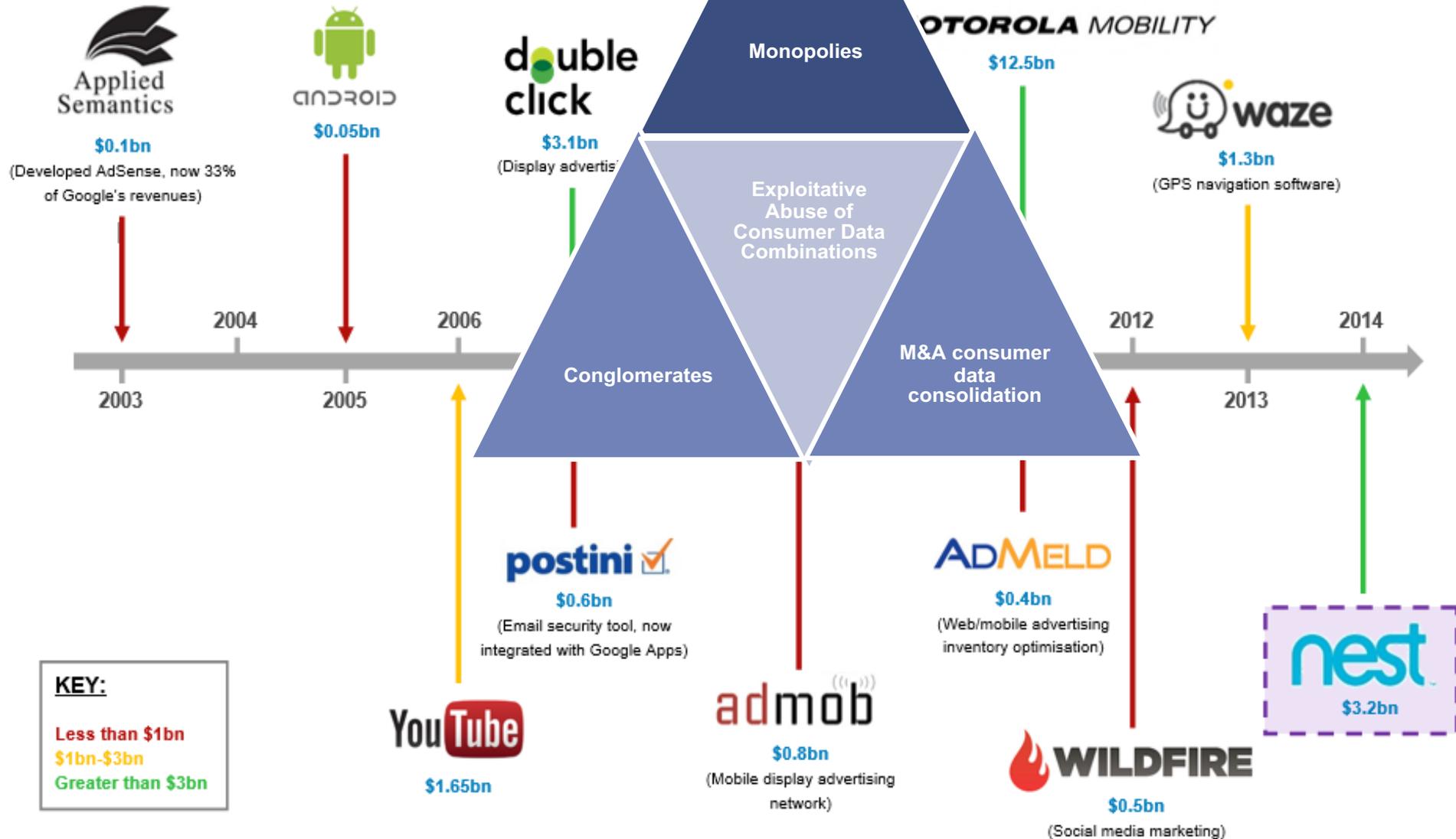
Google Shopping: consumer data were monetary consideration

Google Android: the combination of consumer data from multiple apps: Chrome for search data, Maps for location data, YouTube for experience data and Gmail for location

GC: Android gathered valuable consumer data: location or Google Play usage data from advertising

CMA Privacy Sandbox: consumer privacy: non-disclosure of consumer data from Chrome browsing history, analytics, third-party cookies, software codes, algorithms and business secrets, non-tracking and non-discrimination.

3.1. EXPLOITATIVE CONSUMER DATA ABUSE

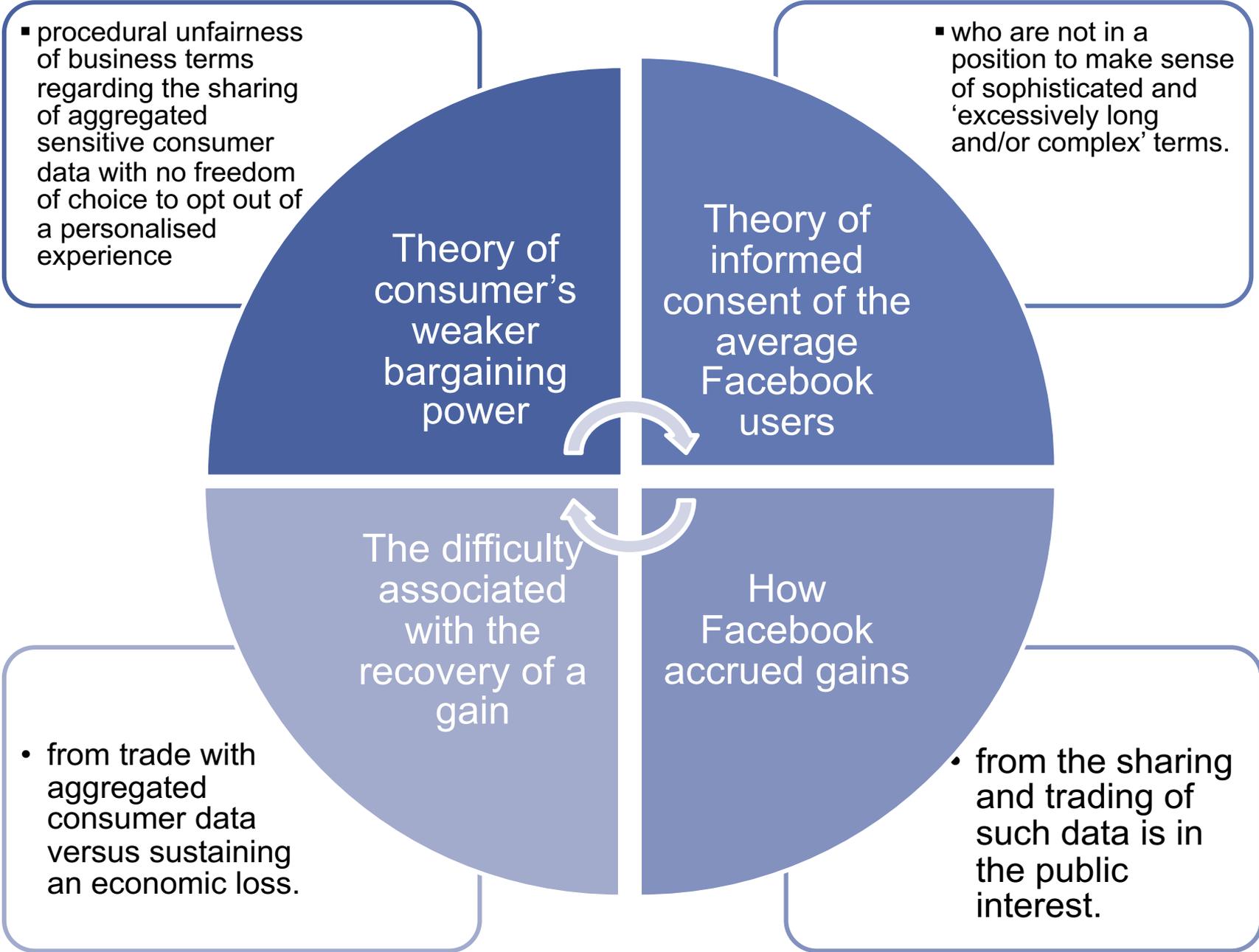


3.2. EXPLOITATIVE CONSUMER DATA ABUSE

Google/Nest Labs	Consumer data combinations especially from Nest smart speakers, thermostats, and surveillance cameras and doorbells
Google/Looker	AI software for aggregated consumer data combinations from advertising, marketing, and cloud storage, jointly with Looker analytics
Google/Double Click	<p>Project Bernanke manipulated AdX bids to consolidate dominance, tweaked algorithm against publishers who used innovative bidding technology and increased data advantage by acquiring access to rival bids to adjust fees.</p> <p>Project Poirot won rival bids by artificially manipulating them below the minimum price agreed upon by the advertisers.</p> <p>Project Bell artificially lowered rival publisher bids.</p>
Google/Fitbit	Due to aggregated sensitive consumer data combinations, the exclusionary foreclosure in healthcare markets.



3.4. EXPLOITATIVE CONSUMER DATA ABUSE



3.5. EXPLOITATIVE CONSUMER DATA ABUSE

Reliance on the *United Brands* test for excessive pricing

rather than a flexible application of substantive unfairness

to freemiums paid with sensitive consumer data.

It would be cumbersome, *ad absurdum*, to prove how a price of zero is 'too high'.

For consumer justice, this inquiry should not be about the excessiveness of zero-pricing (*probatio diabolica* for substantive unfairness),

but rather about an excessive disclosure of consumer data (procedural unfairness pragmatism).

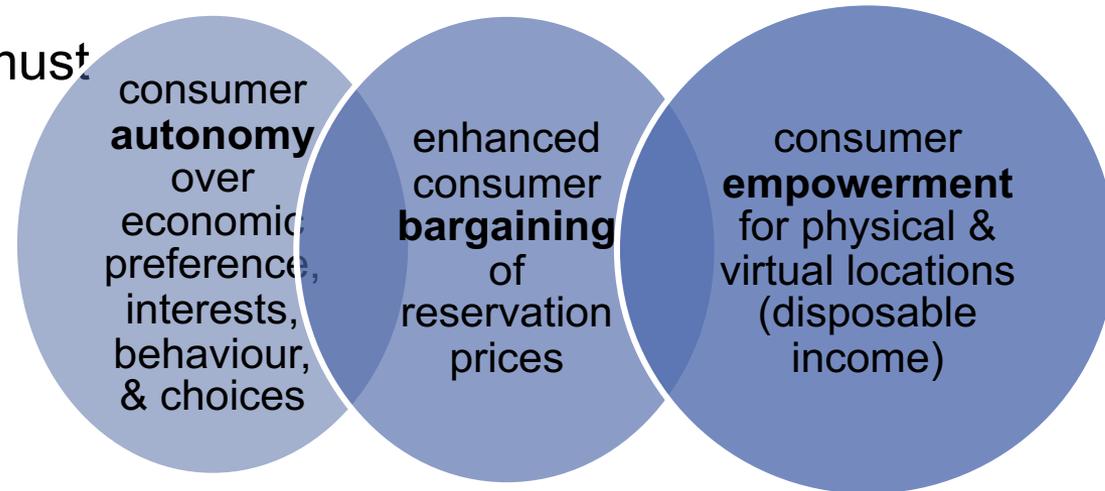
Most untenable for consumer justice: paid subscriptions could only diminish Meta's corporate profits.

UK precedent should recognise

Consumer economic loss of privacy, e.g., location and willingness to pay.

4. HYBRID CONSUMER DATA ABUSE – FOR CONSUMER JUSTICE: GREATER AUTONOMY, ENHANCED BARGAINING, AND CONSUMER EMPOWERMENT

Consumer privacy must be inclusive of



- **Meta**: the economic context of targeted advertising for data combinations focused on consumer data shared for personalisation.
- Consumer data-driven algorithmic discrimination exploits consumer ignorance for unwanted attention.
- The monopoly control of aggregated consumer data could have exclusionary and exploitative effects on rivals and consumers, respectively.

4.1. HYBRID CONSUMER DATA ABUSE

CMA Facebook/Kustomer

- the advertisers were interested, inter alia, in consumer characteristics and location.

CMA Facebook/Giphy

- selling consumer data for higher prices for personalised advertisements.

EC Google/Fitbit

- consumer data about health, wellness, and location could significantly improve targeted advertisements by capturing iPhone users who actively use Fitbit instead of the Google health-tracking app.

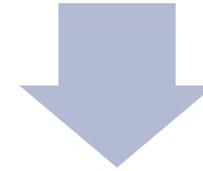
- ❑ Due to the collection of sensitive consumer data, such as heart rate, sleep activity and oxygen saturation level, cookies, and geolocation data; consumer data exploitation for personalised advertisements was a far greater danger for
- ❑ leveraging dominance into healthcare insurance markets through Google Cloud and Project Nightingale. Consumers could only be worse off.

4.2. HYBRID CONSUMER DATA ABUSE

In a hypothetical worst-case scenario, most visible consumers who overshare consumer data about their economic interests, preferences, and choices on monopolistic platforms



must subsequently pay up to 15 to 25% higher prices due to having their footprint analysed for an exploitative price increase.



Extracting the valuation difference could be the key to the said price increase. Even a modest increase, within a range of 5 to 15% is exploitative and inflationary.



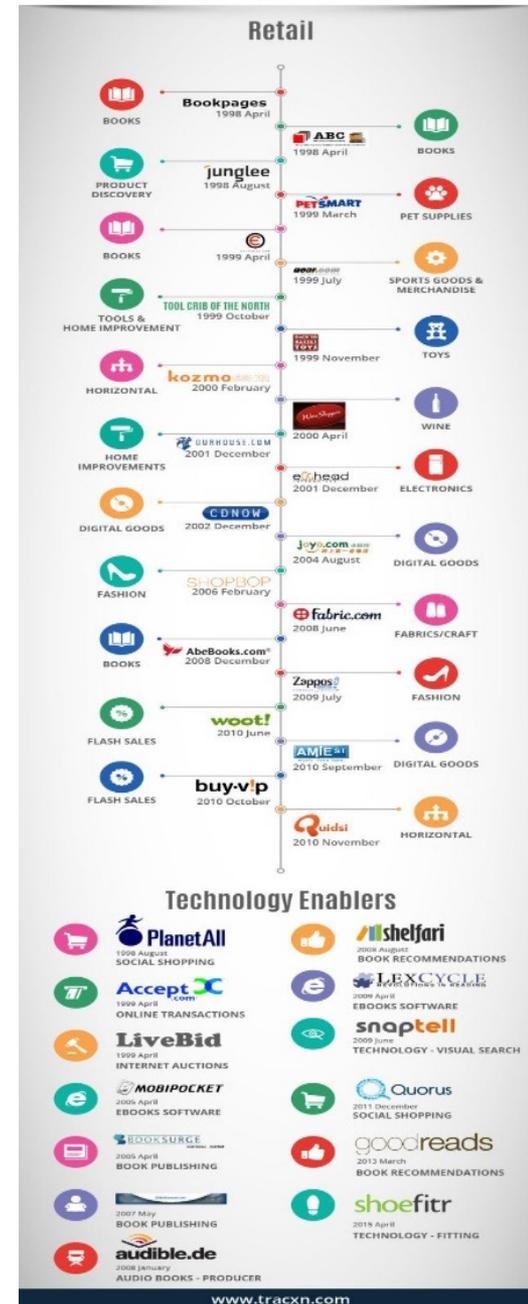
The SSNIP test could examine the average price, which less visible consumers who go for traditional, rather than digital platforms, shopping, incl. leisure, pay for similar offerings.

4.3. HYBRID CONSUMER DATA

CMA Amazon/Deliveroo: the behavioural price discrimination effects on the supply of online food.

□ AI predictive analytics of historical and external consumer data to estimate delivery time to consumers and analytics services to restaurants; e.g., Pizza Hut lacked shared access to aggregated consumer data.

□ Delivery speed is a key competition driver for affluent consumers who prioritise convenience, especially Amazon Prime customers.



5. CONCLUSIONS

- ❖ Legislative gaps:
 - (i) AI software algorithms for predictive analytics of consumer behaviour due to consumer experience, location, medical and financial data and
 - (ii) marketing strategies, such as personalised offers;
- ❖ Legal interpretations to close the gap in the prohibition of abuse when applied in conjunction with the DMA provisions (consumer data combinations, digital tying, and algorithmic discrimination);
- ❖ Digital conglomerate mergers & killer acquisitions sustain an unfair consumer data-driven advantage and consumer data combinations;
- ❖ The conflicts of interest between
 - (i) the under-enforcement of the consumer data abuse and the lenient scrutiny of data-driven mergers;
 - (ii) FRAND terms of access to aggregated sensitive consumer data and consumer economic privacy.