COMPASS LEXECON

CCP Machine Learning and AI as Business Tools

Privacy, targeted advertising and competition (policy)

6 June 2019

Gregor Langus

GREGOR'S TIMELINE IN GOOGLE SINCE 2017

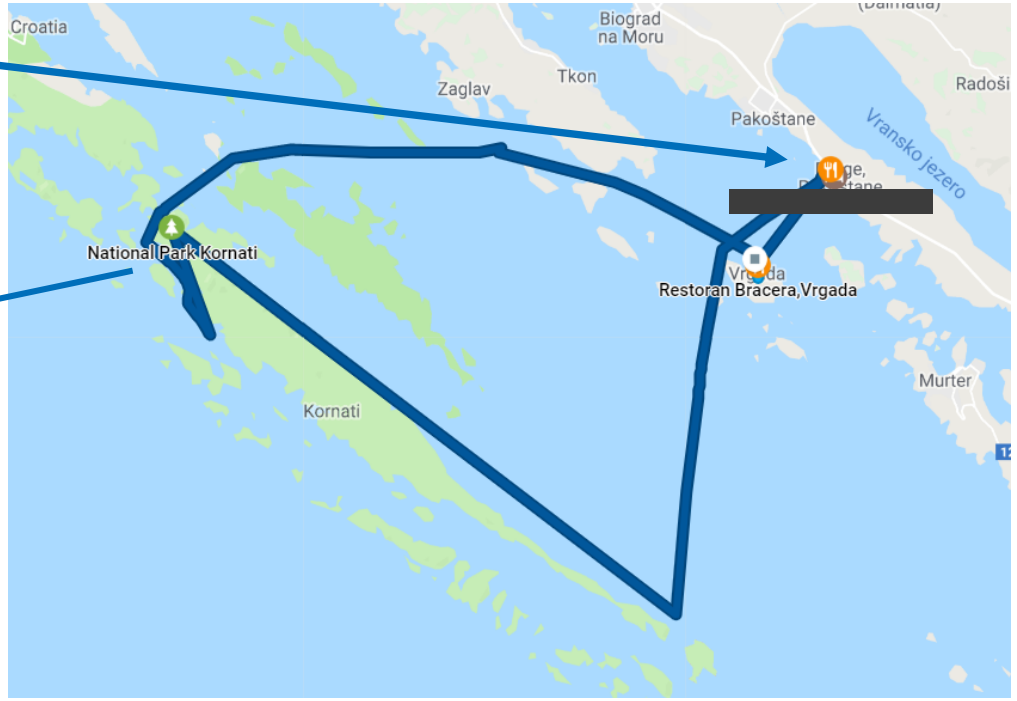
https://www.google.com/maps/timeline?pb

76,4 km
2h 18m

2,4 km
1h 2m

7,0 km
25m

Wednesday, 9 August 2017

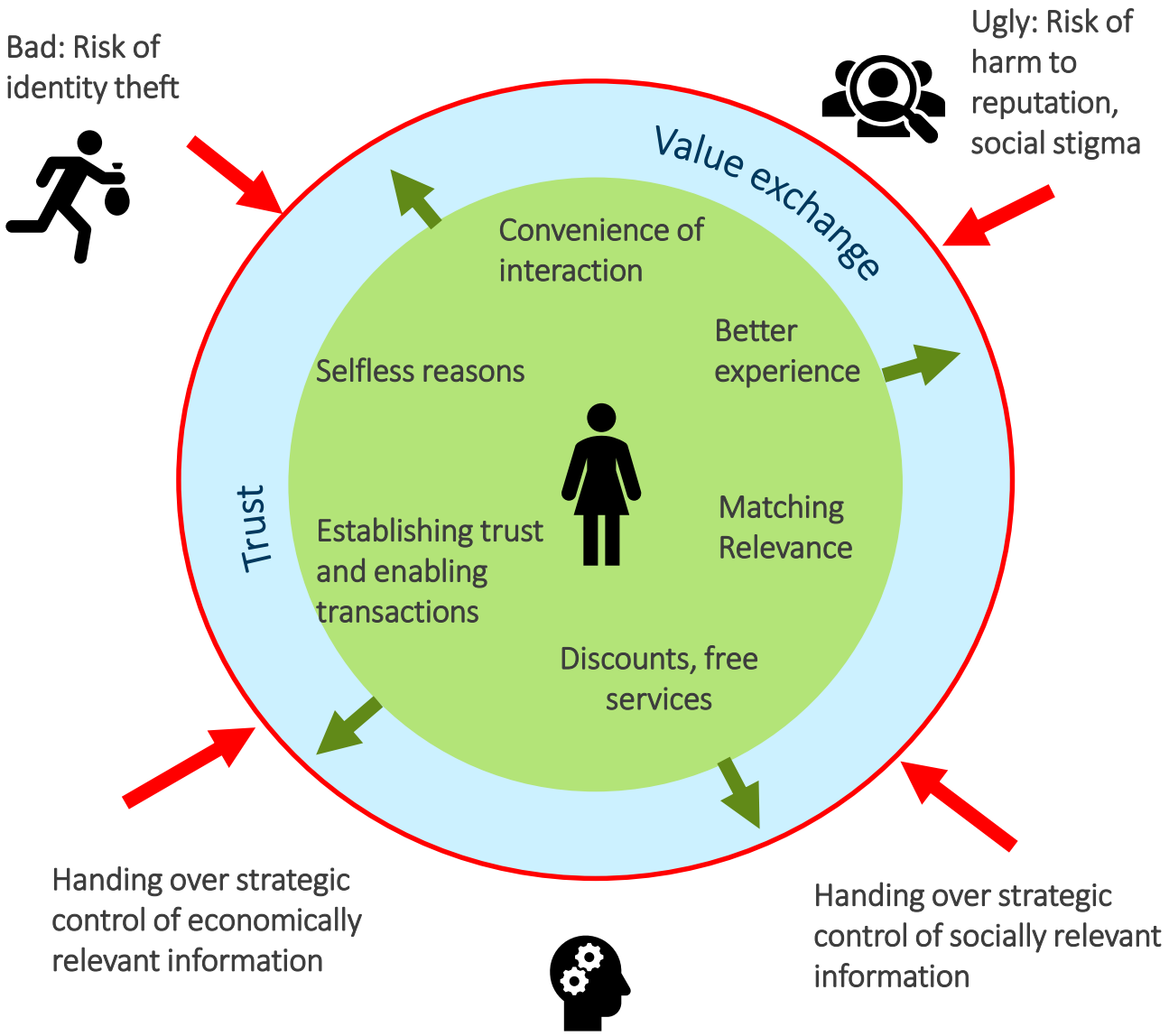


DIFFERENT FACES OF PRIVACY AND MY CLAIMS

Four claims:

- Consumers value privacy (but are willing to give up control of personal data in exchange for value)
- Competition may discourage platforms from invading privacy (but in general has ambiguous effect on the incentive to collect and process personal information)
- Privacy can (and should) be considered a relevant competitive variable (not unlike price or quality)
- But, the fact that consumers value privacy does not mean that more privacy is necessarily better for consumer welfare – there are externalities outside the relationship between individual consumer, platform and brands that make the planner's privacy calculus much more difficult than for an individual data subject.

PRIVACY TRADEOFFS FOR CONSUMERS: THE BAD, THE UGLY AND THE … TRICKY



Do consumers care about privacy?

Personal information private → individual can release personal information or withhold it, depending on situation where interaction takes place.

A self-interested individual should want to preserve control over its personal information.

Yes, rational consumers do care about privacy.

But the calculation is tricky for individual and even more for social planner!

- Identifying and communicating relevant private information in every new interaction is costly
- Uncertainty and reversal of info asymmetry
- Asymmetry in information may negatively affect the welfare of the other party to trade or interaction (company or another consumer).
- On top of that: positive and negative externalities from more privacy protection – beyond the individual-to-individual or individual-to-company interaction.

CONSUMERS CARE ABOUT PRIVACY, BUT ARE STILL WILLING TO HAND OVER PERSONAL DATA IN EXCHANGE FOR VALUE

pwc

2000 US consumers
2017, August and September

- 69% believe companies are vulnerable to cyber attacks
- 25% believe that their personal data is handled responsibly
- 82% agree that governments should regulate more
- 15% believe that companies will use their data to improve their lives

sas THE POWER TO KNOW.

525 US consumers
2018, July

- 73% said they were more concerned about their data privacy now than a few years ago
- 83% would like the right to tell data holder not to share or sell their personal information
- 64% would like the right to have their data deleted

SAILTHRU

2000 US consumers
2018, May

- 60% in favor of more government intervention
- About 50% are unaware or uncertain that social login creates opportunity for data to bass between social platforms and brands.
- 60% think companies should not sell their data

Acxiom, Foresight Factory and DMA
1047 UK customers, 2017, November

- 78% of UK customers believe businesses benefit most from personal data exchange.
- 75% of UK consumers say are very concerned about online privacy.
- 50% of customers will share data under the right circumstances.

MEF MOBILE ECOSYSTEM FORUM

Mobile Ecosystem Forum, Assurant, onDevice, 2018

- 66% have experienced data-related harm themselves or seen it happen to someone close.
- 36% taking actions to protect their privacy

IBM Institute for Business Value

I1000 US consumers, 2018

- 89% tech companies need to be more transparent
- 45% updated privacy setting
- 16% stopped doing business with an entity due to data misuse

THERE ARE UNINTENDED CONSEQUENCES BEYOND CONTROL OF DATA SUBJECT – E.G. IDENTITY THEFT (IN FIGURES – US)

Identity Theft Resource Center and CyberScout 2018 report:

1,244 data breaches

More than 400 million PII records exposed

Hacking most common cause of data breach

Number of breaches in 2018 was 23% down from 2017

Number of exposed consumer PII records was up 126% from 2017

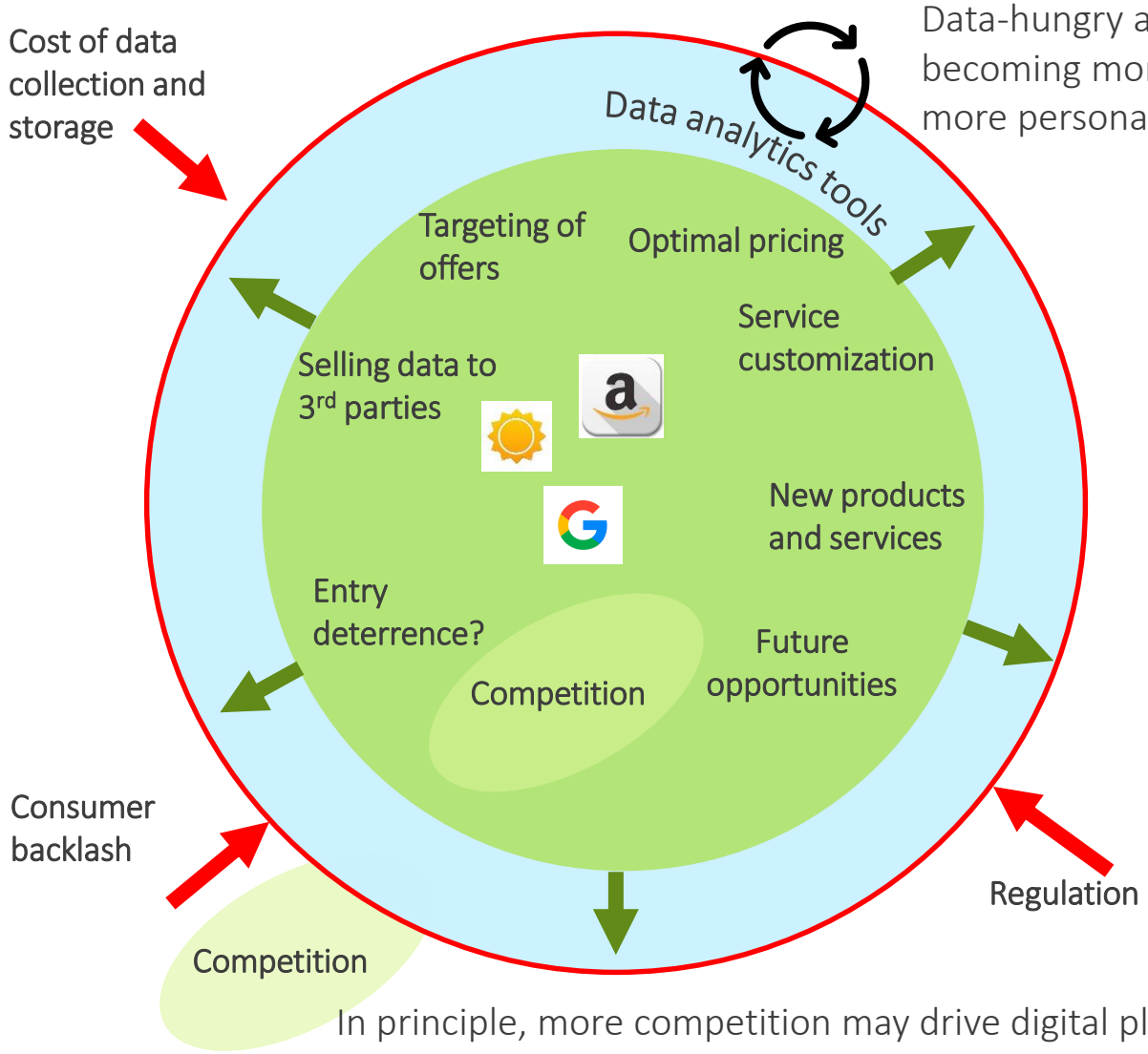
Health care field had the second largest amount of breaches (after Business sector) in 2018 and the highest rate of exposure per breach.

Unity Point Health data breach exposed 1.4 M patients' protected health information.

2018, March, Cambridge Analytica. Then, in Sept, attackers stole access tokes (full control) for 50 million users

2018, Oct, Google announced it would shut down Google+ after finding a bug that exposed user data from 52 million accounts

TRADEOFFS FOR PLATFORMS IN COLLECTION OF PERSONAL DATA



Data-hungry analytics tools becoming more sophisticated → more personal data collection.

Data is key input for platforms. Successful platforms use data to reduce:

- Search costs – online prices are often lower, easier to find niche products, fill capacity, better matching quality
- Verification cost
- Coordination cost
- Replication (modularity, automatization and standardization)

In principle, more competition may drive digital platforms to either collect more data or to collect less of it. But for competition to deter from personal data collection data we need (1) awareness, and (2) verifiability.

BUSINESS VALUE OF BEHAVIORAL TARGETING – MIXED EVIDENCE

Compare run-of-network advertising to behaviorally targeted advertising.

Advertising rate significantly higher for behaviorally targeted adds. CPM (cost per impression) twice the average CPM for run-of-network. But also more effective in terms of conversion rates. Gives consumers more utility. [Beales, 2010, online]. Also, Farahat and Bailey (2012) estimate that TA generated twice the revenue of non-targeted advertising in 2012.

Enactment of privacy-protection bill in the EU (EU Privacy and El. Comm. Directive, 2002) that limited the ability of advertising companies to track online behavior resulted in significantly less effective advertising. [Goldfarb and Tucker, 2011, Man.Sc.]

However, Mayer and Mitchell (2012), Lambrecht and Tucker (2013, JMR), Blake et al. (2015, Econometrica) – returns on TA are very modest. White et al (2008, ML) find that consumers may negatively react to highly personalized messages when the fit with personal characteristics is not explicitly justified

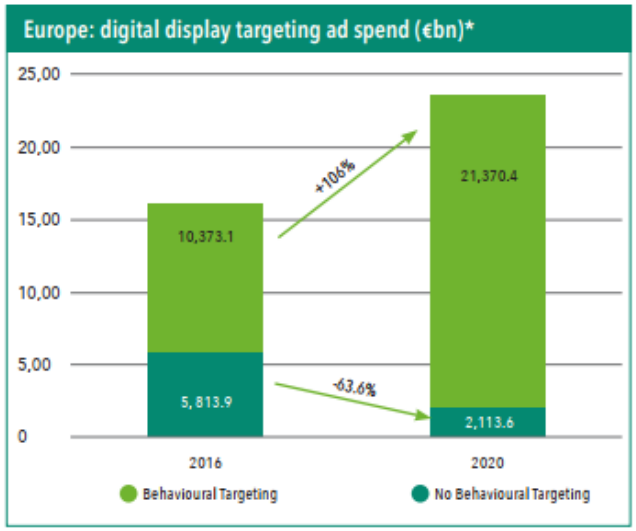
There is little evidence that targeting leads to systematic price discrimination.
Valentino-Devries et al (2012, WSJ) suggest that some online retailers may discriminate based on the physical distance to offline store; Mikians et al (2013) suggest price difference of 10% to 30% for identical products based on the location and browser (search history) configurations. Vissers at al. (2014) do not find any experimental evidence of PD in online airline tickets

GROWTH IN TARGETED ADVERTISING REVENUE SUGGESTS A CLEAR BUSINESS VALUE OF TARGETED ADVERTISING

IHS Markit™

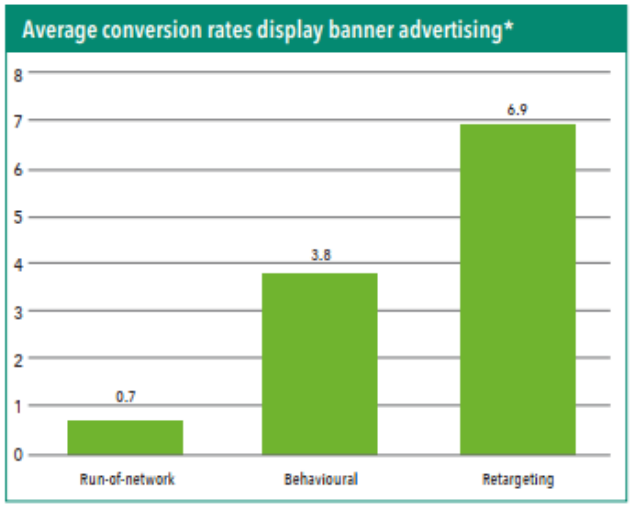
Study: In 2016, in Europe, digital advertising generated annual revenue of approximately 42 billion Euro, growing at more than 12% year on year. 86% of programmatic advertising uses behavioral data

EXHIBIT 1: BEHAVIOURAL TARGETING MARKET SIZE

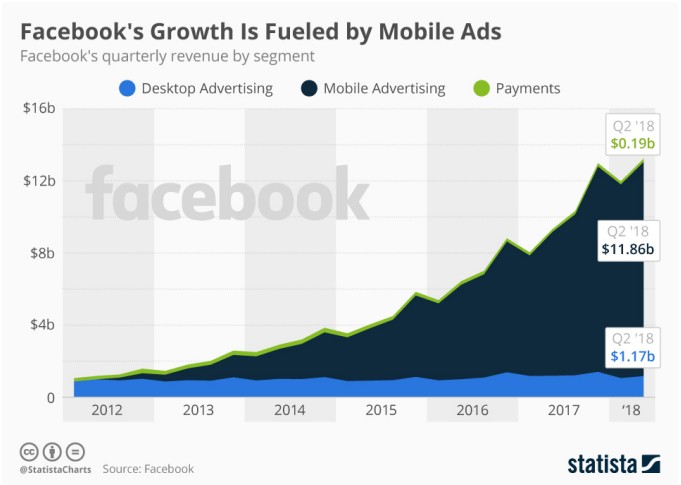


Source: IHS Markit Behavioural Impact Model. 2020 is forecast data assuming average annual growth rates of 10% between 2016 and 2020.

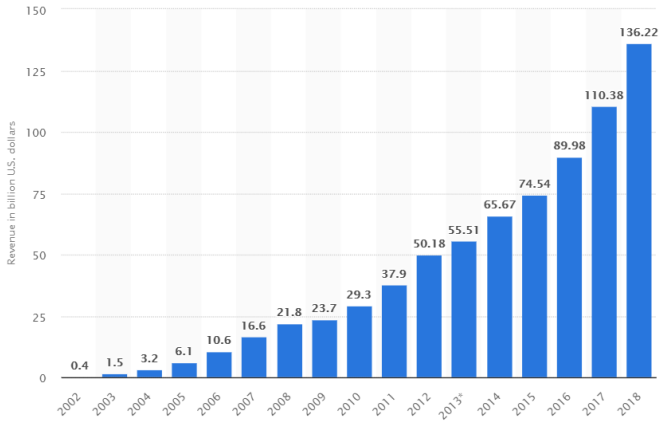
EXHIBIT 2: CONVERSION RATES



Source: IHS Markit industry survey, 2017. Data refers to advertising campaigns in the EU-28.



Digital platforms have and will continue to have strong incentives for personal data hoarding.



Source: Statista.com

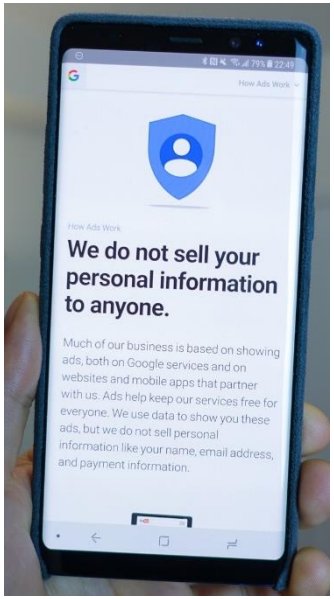
YET, DIGITAL PLATFORMS ARE RESPONDING – PRIVACY SEEMS TO BE BECOMING A FACTOR IN COMPETITION

Facebook CEO Mark Zuckerberg says the 'future is private'

The chief executive of the world's largest social network wants to turn his company around

By Nick Statt | @nickstatt | Apr 30, 2019, 1:22pm EDT

https://www.theverge.com/2019/4/30/18524188/facebook-f8-keynote-mark-zuckerberg-privacy-future-2019



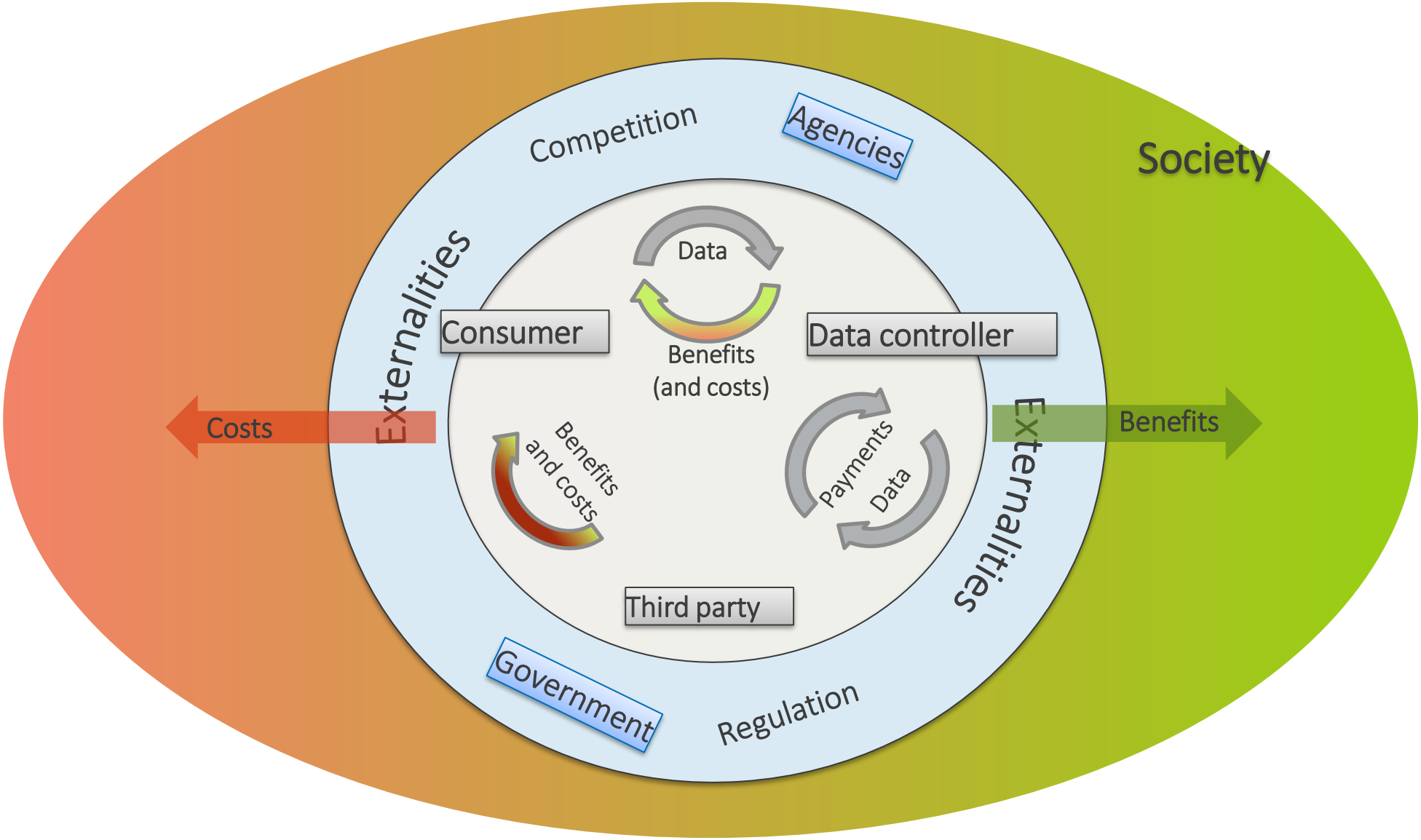
Android Q leak reveals system-wide dark mode and bigger emphasis on privacy

Expect to hear more about Android Q in the spring

By Chris Welch | @chriswelch | Jan 16, 2019, 4:43pm EST

https://www.theverge.com/2019/1/16/18185763/android-q-leak-dark-mode-new-privacy-settings

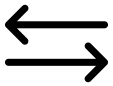
PRIVACY CALCULUS: DATA SUBJECT, DATA CONTROLLER AND SOCIAL PLANNER



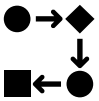
TARGETED ADVERTISING BEYOND AN INDIVIDUAL DATA SUBJECT OR FIRM – SOCIAL WELFARE: ECONOMIC THEORY

But, a per click fee is regarded as a marginal cost → passed through also suboptimal quality of sponsored links.[De Corniere 2016, AEJ].

Targeted advertising on search: reduce search costs, improve matches and intensify competition (targeting reduces the perceived costs of additional search).



Exchange of information regarding customers between two companies can reduce information distortions and enhance social welfare. Think of insurance markets. [e.g. Calzolari and Pavan, 2006, JET].



An intermediary with superior information about consumer preferences may have an incentive to direct consumers to a less preferred alternative and only then to the optimal one in order to increase traffic or product exposure. [Hagiu and Jullien, 2011, RAND]

High demand consumers tend to prefer privacy and low-demand consumers tend to prefer no privacy. More generally, whether dynamic pricing is beneficial to consumers, platforms, or sellers (or not) is highly context dependent. [Taylor and Wagman, 2014, SSRN]

A comprehensive survey on the economics of privacy by Acquisti, Taylor and Wagman (2016, JEL).

Targeted advertising can improve matching, but prices increase as well. This is because the advertiser expects to reach consumers who have a low price-elasticity of demand.
Informational rent is passed on to sellers and disclosing information may be too costly for the platform [De Corniere and Nijs, 2014, SSRN; also Ganuza and Penalva, 2010, Econometrica]

CONCLUSIONS

Consumers are concerned with privacy:

- Increasing awareness;
- Actions to protect privacy, want control, transparency;
- Generally averse to targeted advertising, but do seem able to recognize benefits;
- Will trade personal data when they trust the platform and when they see a value exchanged.

→ Privacy increasingly a variable that is relevant to competition, similar to price and quality

→ Individual data subjects generally have an interest in high level of privacy (control over the release of their personal information)

However, this does not necessarily mean that more privacy will necessarily increase consumer and especially social welfare.

Platforms are taking actions:

- 2019 is all about privacy
- Starting to use privacy as an instrument of competition: giving more transparency, more control to users

Nevertheless:

- Privacy will only become a relevant competitive variable if it is verifiable.
- Platforms will continue to be hungry for personal data.
- We are likely to continue to see data hording, data breaches.