Consent without Choice:
Market Power, Data Protection, and Competition law

Wolfgang Kerber
(Universität Marburg)

Weizenbaum Lecture
Weizenbaum Institute, Berlin
3 March 2020

1. "Consent without choice": Introduction

Philipps Universität Marburg

To what extent is "informational self-determination" possible in digitized world, and can privacy be protected with individual decisions about use of personal data?

- GDPR grants a strong bundle of rights to individuals regarding their personal data with the principle of "consent" (private autonomy)
  - \+ but also relies on a contractual approach for allowing others to use personal data, leading to a de facto market approach (data as counterperformance)

  => myriads of "consents" to complex contracts about use and sharing of our data
- Crucial question: Do these markets work well or serious market failures?
- One well-known market failure discussion: Problems of intransparency, informational / behavioral problems and too high transaction costs for users

My question: Might we have also second market failure problem that increasingly situations where we have (de facto) no choice any more / are "forced" to consent

(1) Competition problems: dominant firms (or cartels) (BKartA: Facebook case)

(2) Future complex systems (esp. IoT context) with no option to opt-out any more

Structure of my lecture

1. Introduction
2. Mapping the landscape of problems in digital economy
3. The Facebook case and its controversial discussion
4. Relationship between competition and data protection law from an economic policy perspective
5. "Consent without choice" in the future world of IoT
6. Implications for consent and contract-based approaches to data protection and privacy

2. Mapping the landscape of problems in digital economy (1): Privacy, data protection law, and economic policy

- analysis of privacy is difficult from an economics perspective
  + economics of privacy is under-developed (despite Acquisti et al 2016 etc.)
  + models of perfect competition: assumption of perfect information
    => privacy looks more like a problem because it is about hiding information
  + but it can be argued about privacy risks and privacy preferences
- GDPR / privacy / data protection law from an economic perspective:
  + property rights perspective: bundle of rights of a person regarding his/her personal data: can exclude others from using them (consent)
    > but: limited bundle of rights, e.g. legal exceptions (as Art. 6(1)f GDPR)
  + market failure perspective: do markets for allowing use of data work?
    > information / behavioral problems: => similar to consumer law
    > competition problems: => competition law
- analyzing privacy from competition, consumer and data protection law perspective and all three might be important (Kerber 2016a)

2. Mapping the landscape of problems in digital economy (2): Data ownership, data access/sharing, data governance

Philipps Universität Marburg

- from the discussion about new IP-like exclusive right on (non-personal) data …
  + non-rivalry plus excludability of data => no new exclusive right! (Kerber 2016b)
- … to the discussion about more data access/sharing
  (EU Comm. "Building a European data economy", 2017: "data producer right";
  most recent: EU Comm "A European strategy for data", 19 Feb 2020)
- important: deep conflict between privacy protection and the data economy
  + analysis of discussion about ePrivacy-Regulation (in Specht/Kerber 2018)
  + example: smart retailing: opt-in or opt-out for consent of retailers to log into smartphones of customers and tracking them
- new problem of data governance in IoT contexts:
  + problem of exclusive control of data through manufacturer and access problems of users and other stakeholders to the data and the IoT ecosystem
  + data access and interoperability problems in IoT ecosystems from a competition law perspective, esp. also about data in connected cars (Kerber 2018, 2019)

2. Mapping the landscape of problems in digital economy (3): Market power of digital platforms and competition law

Philipps Universität Marburg

Recent discussion on challenges of digital economy for competition law (reports):

- Schweitzer/Haucap/Kerber/Welker (2018): Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen [input for current proposal of amending German comp. law]
- Crémer/de Montjoye/Schweitzer (2019): Competition policy for the digital era (EU report)
- Furman et al (2019): Unlocking digital competition (UK report)
- ACCC (2019): Digital platforms. Final report (Australian report)

Broad consensus: large digital platforms have "entrenched" positions of market power that cannot be challenged and threaten competition and innovation

important: > platform economics (direct/indirect network effects etc.)

> huge amount of accumulated data / control of data as competitive advantage of large digital platforms and entry barrier

Current policy question: What to do about market power of large digital platforms?

- Is current competition law (with its ex-post control of abusive behavior) capable of dealing with it or do we need also ex-ante regulation of large digital platforms? (see EU Comm, A European strategy for data, 2020, p.14)

2. Mapping the landscape of problems in digital economy (4): Market power of digital platforms and competition law: personal data

Advantages of Facebook and Google with regard to access to personal data (and therefore competitive advantages in advertising markets) (ACCC 2019, 84-89)

Example Facebook:

- direct collection of high quality user data from
  - \+ Facebook platform data, Instagram, WhatsApp, Messenger
  - \+ websites / apps using Facebook analytics and other Facebook business tools as Like/Share buttons
  - \+ websites that allow users to sign-up using Facebook account …
  - \+ in addition: device data and payment data
- additionally third-party trackers (Google and Facebook are leading companies)

=> Google and Facebook have multiple "touch points" for collecting personal data

- this has huge implications for:
  - \+ privacy
  - \+ competition

3. The Facebook case and its controversial discussion (1): The proceedings of the case

Philipps Universität Marburg

Importance of Facebook case of German Bundeskartellamt:

- first competition law case, which explicitly considers privacy issues and rules that Facebook's data collection practices is an abusive behavior of a dominant firm
- background question: Relationship of competition and data protection law?

Proceedings of the Facebook case:

- March 2016: start of the investigation
- December 2017: preliminary assessment claiming that Facebook is abusing its dominant position by making the use of its social network conditional on allowing to collect every kind of data generated by third-party websites and merge it with the user's Facebook account (=> bundling of consent)
- February 2019: decision: prohibiting this behavior as an exploitative abuse and requiring that merging of data is only allowed after an additional consent, i.e. users should be able to use Facebook social media w/o such a bundling
- July 2019: OLG Düsseldorf: granted interim relief to Facebook / rejecting BKart
- further legal proceedings

3. The Facebook case and its controversial discussion (2): The reasonings of the Bundeskartellamt

BKartA has applied German competition law (§ 19 GWB) and not Art. 102 TFEU

Market dominance of Facebook:

- Assessment: Facebook is dominant on the market for social media in Germany

Abusive behavior:

- exploitative abuse with regard to terms and conditions (excessive data collection)
- users face a "take it or leave it" decision, and through Facebook's market power users are de facto forced to accept these terms of services (no voluntary consent)
- decisive: infringement of data protection law (also due to market power of FB, intransparency of Facebook, and information/behavioral problems of users)

  + (data protection agencies support Facebook case!)
- violations also gives FB advantages vis-a-vis competitors => exclusionary beh.

Remedy:

- FB is not allowed to merge third-party data (only with additional consent), i.e. they at least have to keep both data sets separate

3. The Facebook case and its controversial discussion (3): The first court decision and overview on discussion

Philipps Universität Marburg

Decision of OLG Düsseldorf: "serious legal doubts" about the decision of BKartA

- accepted market definition and dominance of Facebook, but:
- no abuse because no anticompetitive conduct [but here exploitative abuse]
- no economic loss of consumers, no loss of control of their data; users knew what they agreed to (FB's terms and conditions), voluntary decision despite dominance
- "strict" instead of "normative" causality betw. market power and GDPR violation [proposal of German comp. law wants to clarify that no strict causality required]

Discussion of the case:

- general: widely discussed case internationally; seen as an innovative, bold step of BKartA; triggered a discussion about privacy considerations in competition law
- broad consensus that the decision has weaknesses:
  + very specific legal reasoning using § 19 GWB plus German court decisions
  + why not more focus on exclusionary effects (this is very brief in decision)
- but also the decision of OLG is broadly criticized as too harsh and simple

3. The Facebook case and its controversial discussion (4): Overview on discussion

Philipps Universität Marburg

Support for BKartA decision:

- privacy harm /excessive data collection should be considered in competition law (also in Art. 102 TFEU; so far EU Commission very reluctant)
- infringement of data protection law (privacy as human right) as a suitable benchmark for exploitative abuse of a dominant firm

Critique of BKartA decision:

- unclear whether these terms and conditions lead to more harm to consumers (debate about privacy risks)
- competition law overstretched by including privacy harms; privacy problems (due to info / behavioral problems) to be solved by data protection / consumer law

What is surprisingly not discussed:

- "bundling of consent" and the remedy of giving the users an additional choice
- what about the relationship between competition law and data protection / consumer law, if we might have - as in the Facebook case - simultaneously two market failures (market dominance and information/behavioral problems)?

4. Relationship between competition and data protection law from an economic policy perspective (1): Introduction

Philipps Universität Marburg

Economic policy: division of labor between different policies

- different policies for different market failures and/or objectives (not so clear)
- competition policy: solving competition problems / looking at consumer welfare
- consumer law: for solving market failure problems through info/behav. problems
- data protection law: not so clear, because perhaps different market failures lead to privacy risks (specific objective: privacy as a fundamental value)

[An entire other reasoning: one policy helps another policy that does not work well

- one policy has to step in if another policy does not work effectively
- problem of serious underenforcement of GDPR (not enough resources for data supervisory bodies) (see, e.g., Datenethikkommission 2019)
- in law not uncommon that problems can be solved by different fields of law
- example: competition law had to solve defects of IP law (which seem not to be solvable in IP law)]

4. Relationship between competition and data protection law from an economic policy perspective (2): Introduction

Philipps Universität Marburg

Economic implications of simultaneous existence of two market failures:

- usually in law and in economics: analysis of only one market failure and how to remedy it with implicit assumption that no other market failure exists
- What about the aggregate effects of two market failures? Do they (mutually) reinforce each other?
- Can a dominant firm increase/exploit better info/behavioral problems?
  - + Can a dominant firm reduce transparency/collect more data or does the data-collection lead to higher privacy risks (more comprehensive consumer profiles), i.e. more consumer harm than in the case of non-dominant firms
- Can info/behav. problems lead to larger market power/or more abusive behavior?
  - + e.g., due to info/behav. problems competition with privacy policies might not work well leading to more data-collection and increase in market power
  - + German report (Schweitzer et al 2018): information (manipulation) power (biased ratings/rankings) might lead to larger market power (intermediation power)

=> interaction between two market failure effects needs much more research!

4. Relationship between competition and data protection law from an economic policy perspective (3)

Philipps Universität Marburg

Can harm to privacy be taken into account in competition law?

- extent and terms of collecting personal data can be considered (either as part of "quality" or also directly; extent of privacy risks can be a non-price parameter)
- clear: there should also be competition on data collection / privacy policies
- effective competition: => fulfilling (heterogeneous) privacy preferences
  - + with different privacy policies, also offering options that users can choose etc., also options with payment of services w/o collecting data
  - + quality of privacy policy can also include transparency of terms and conditions
- from a competition perspective: Is it sufficient that the GDPR is not infringed?
  - + no, because the GDPR is only offering a minimum standard
  - + test case: horizontal cartel about privacy policies that fulfill GDPR but not more
    => clear violation of Art. 101 (if not exemptible): collusion on data collection
  - + traditional view: infringement of GDPR is directly neither a sufficient nor a necessary condition for a competition law violation
    (=> misleading discussion about CAs enforcing GDPR and other laws)

4. Relationship between competition and data protection law from an economic policy perspective (4)

Philipps Universität Marburg

Can market power be taken into account in data protection / consumer law?

- if a dominant firm collects data => danger of more data/increased risks for privacy
- in principle, data protection/consumer law treat all firms equally, i.e. no distinctions betw. firms with and without market dominance (or small/large firms)
- but: discussion about whether consent is still "voluntary", if a firm is dominant (small reference in Art. 29 WP, Opinion 06/2014); BKartA has used this but it is an unexplored idea in application of data protection law
- but very clear: data protection authoriteries so far cannot make a competition analysis (dominance of a firm or whether there is a privacy-harming cartel?)

=> result: data protection authorities cannot solve competition problems with regard to privacy-harming behavior of firms !

(but: contractual / market approach to data requires protection of competition)

- what about solutions to prohibit privacy-harming behavior through consumer law (Italian Facebook cases)? => danger of overenforcement (also small firms)

4. Relationship between competition and data protection law from an economic policy perspective (5)

Philipps Universität Marburg

Back to competition law: How to consider harm to privacy in competition law?

- exclusionary abuse:
  - + main argument: bundling of all these data leads a further advantage of Facebook with regard to personal data in comparison with other competitors, especially on advertising markets => foreclosure effects
  - + it is a pity that BKartA has not focussed much more on this point
- exploitative abuse:
  - + "bundling" of consent forces consumers to give consent to the entire bundle of data (users are locked-in into Facebook) => larger collection/use of data => more comprehensive consumer profiles / higher privacy risks
  - + exploitative abuse always difficult: analogy to price abuse does not fit well; do we need a counterfactual? (how much data collection under competition?)
  - + BKartA/much of the legal literature: infringement of GDPR as benchmark
  - + perhaps: new different approach necessary for exploitative abuse with regard to privacy (perhaps developing new concepts with data protection scholars/authorities)

4. Relationship between competition and data protection law from an economic policy perspective (6): Conclusions

- competition market failure (dominance / cartels) so far cannot be solved by data protection / consumer law

  => application of competition policy necessary as long as there are effects of dominance / mergers / cartels on extent of data collection/use/privacy risks

  + can we take into account effects through info/beh. problems in competition law? => yes! (as part of effects analysis)

  + [can competition law also consider "privacy as a fundamental value" as an additional objective? => difficult but we can think about that …]

=> both competition & data protection/consumer law are necessary for solving privacy / data collection problems as in the Facebook case

=> much more research about the interplay necessary!

- Institutional implications:

  + collaboration of competition and data protection authorities to assess and solve problems and find a suitable set of remedies that help to achieve objectives of both policies

  + other institutional solutions

5. "Consent without choice" in the future world of IoT (1)

- Some reflections on freedom of contract, choice and competition:
  - + competition: choice betw. firms that compete with each other
  - + cartel: choice formally possible but de facto limited due to cartel agreements
  - + monopoly: consumers cannot choose betw. firms (monopoly power) but can still choose whether to buy a product
  - + [Franz Böhm (1928): freedom of contract only works well if competition]
  - + important: outside option decisive how "voluntary" consent is
- But: digital transformation leads us increasingly into situations where we have no outside option any more, i.e. we are de facto forced to "consent"
- so far: separation of the online world and real / physical world: we live in offline world, and then we decide to go online, and agree to conditions of online service providers, but we can still log out, and we can decide not using them (???)
- in future digital world with ubiquitous data-collecting IoT devices (sensors, cameras, microphones, etc.) in real physical world, we are always part of digital world, and data about us will collected and processed permanently (w/o outside option)

5. "Consent without choice" in the future world of IoT (2)

Philipps Universität Marburg

Examples of having (nearly) no choice any more:

- surfing in the web, and most of the websites collect our data and "sell" them to others (by sharing them) for other services (as Facebook/Google analytics etc.)
- professional context: e.g., writing a review for a scientific journal, which requires acceptance of privacy policies of an account (with sharing of data with others)
- buying a connected car and having to accept the transfer of all data to car manufacturers and allowing them to "monetize" these data
- visiting a friend / family members and "having to accept" their use of Alexa
- smart retailing: entering a supermarket which is directly logging into your smartphone and tracks you in the supermarket
- smart metering/energy/smart buildings: renting/buying an apartment and have to accept the processing of a huge amount of smart home data
- smart city: collection and processing of a huge amount of personal data from citizens, also in public places, public transport systems etc.

=> Do we still have a normative meaningful "consent" about use/sharing of personal data in these kinds of situations?

6. Implications for consent and contract-based approaches to data protection and privacy (1): Problems

- GDPR: informational self-determination (private autonomy) with consent principle
  + individual decision-making / individual privacy self-management
- Market failure problems:
  + information / behavioral problems with regard to consent, too high info costs
  + ignorance / uncertainty about privacy risks
  + not enough choice (competition problems, systems with no opt-out option)
  + too many sequential decisions leading to suboptimal aggregate outcome
  + externalities: inference risks (can the same info be gotten somewhere else?)
- Very unclear whether individual persons can
  + control the use of their personal data through the instrument of "consent"
  + and self-manage their privacy

6. Implications for consent and contract-based approaches to data protection and privacy (2): What can be done?

Philipps Universität Marburg

Options for solving the problems of individual consent: empowering individuals

- helping to solve information/behavioral problems: more transparency, more salient information, privacy icons, reduce transaction costs (by more aggregate log-ins)
- protecting competition and requiring less bundling / more opt-out options (Facebook decision as contribution to that)
- [regulatory approaches to reduce privacy risks, e.g., through better anonymisation methods, better regulation of hypertargeting consumers ("dark matter")]
- establishing new data trustee solutions (PIMS etc.), which manage decisions about consent and the use of personal data
  - \+ so far this has not worked well
  - \+ but new discussion (Datenethikkommission 2019, Kommission Wettbewerbsrecht 4.0 2019, EU-Commission: A European Strategy for Data, 2020)
  - \+ very interesting but unclear whether this is realistic without heavy regulation

=> But to what extent can this help sufficiently?

6. Implications for consent and contract-based approaches to data protection and privacy (3): What is the future of consent?

Philipps Universität Marburg

If individual-decision making about consent for processing personal data does not work, what are other options?

- reducing the scope of individual consent (and private autonomy) and decide at a collective level (in a regulatory manner)
  - \+ that certain (sets of) personal data are not allowed to be collected or used for certain purposes, leading to a more direct substantive minimum protection of privacy, which cannot be circumvented through consenting to contracts
    - > (already existing: e.g., right on deleting personal data / data portability)

  and/or (vice versa, for helping the data economy)

  - \+ whether, to what extent, and for what purposes personal data can be used by others (whom?) without consent of individuals (limiting their bundles of rights)
    - > (already existing: e.g., Art. 6 (1)f GDPR (legitimate interests), use of anonymised data sets)

  => both variants would reduce scope of consent, markets and private autonomy

- but also other options possible …