# Governance of IoT Data:
# Why the EU Data Act will not Fulfill Its Objectives

**Prof. Dr. Wolfgang Kerber**
(University of Marburg)

(Paper available on SSRN: https://dx.doi.org/10.2139/ssrn.4080436;
forthcoming in: GRUR International)

EALE conference, Lisbon
16 September 2022

# 1. Introduction (1)

Philipps Universität Marburg

**Policy background: Data governance of IoT devices**

- Communication: “Building a European Data Economy“ (2017)
  + data policy for more reuse and sharing of data
  + “data producer right”: exclusive rights on IoT data for owner of IoT device
  + doubts about exclusive rights => start of data access / sharing discussion
- connected cars: since 2016 controversial open policy discussion about “access to in-vehicle data and resources” (car manufacturers ⇔ independent service providers) with option of reform of sectoral “type approval regulation for motor vehicles”
  + generally: competition / consumer choice in aftermarket services (repair etc.)
- parallel discussion about access to agricultural data („smart agriculture“)
- new discussion about data access / sharing in B2B IoT contexts

=> EU data policy has focused primarily on voluntary solutions
  + Data Governance Act: data intermediaries
  + Digital Markets Act: only very few and specific data access / sharing obligations

=> Data Act: intended as project for defining new data access / sharing rights

# 1. Introduction (2)

**The Data Act proposal: Overview** (published: February 23, 2022)

Three main data governance issues:

(1) **Governance of the data generated by IoT devices:** (Ch. II)

+ new rights of users of IoT devices to use and share the generated data
+ in B2C and B2B contexts

(2) Business to Government: data access obligations in a public emergency (Ch.V)

(3) Switching between data processing services, solving lock-in problems (Ch. VI)

Additionally:

- **General rules if legal obligations for making data available, e.g. on fair, reasonable and non-discriminatory terms** (w. reasonable compensation) (Ch.III)
- Fairness of contractual terms in data-sharing („imbalances in negotiation power“) for micro, small- and medium-sized enterprises (Ch. IV)

My research question: Can it be expected that the Data Act achieves its objectives regarding IoT data?

# 2. Problems of IoT data governance / objectives of Data Act (1)

**Problems regarding data in IoT contexts:**

- Legal situation: Many generated IoT data are
  - + personal data: EU data protection law remains fully applicable (consent)
  - + non-personal data, for which no „de jure“ rights exist, but data holders can have **exclusive de facto control** over the data

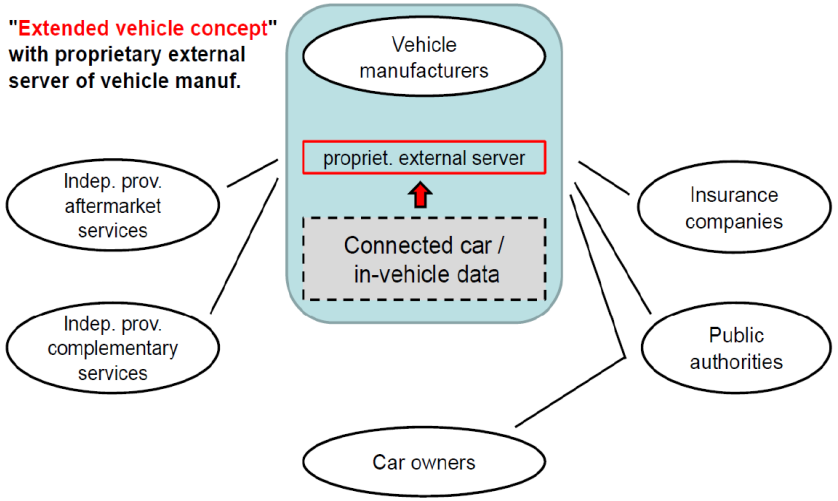
- **Main problem: (**both in B2C and B2B contexts)
  - + Manufacturers of smart devices can **get through their own technical design exclusive de facto control** over all data generated by device
  - + **access problems for**:
    - > users who (co-)generate the data by using their device
    - > firms for providing services but also for data-driven innovation

=> Problems:
- **competition problems, e.g. on secondary markets**
- **negative effects on choice of users for services etc.**
- **negative effects on innovation / under-utilization of data**
- **no fair sharing of the value of data**

# 2. Problems of IoT data governance / objectives of Data Act (2)

**Example: Data in ecosystem of connected cars** (Kerber 2018, 2019)

"Extended vehicle": current data governance concept of vehicle manufacturers (VM)




- all data are directly transmitted to a proprietary server of the VM
- VM has exclusive control over
  1) **access to the data** and
  2) **technical access to the car** (closed system / no interoperability)

  => Gatekeeper position

- **VMs can get control over all secondary markets in this ecosystem** and can foreclose independent service providers and leverage market power

  => **negative effects on competition, innovation, and consumer choice**
- Independent service providers and consumer associations demand a regulatory solution for these problems (policy discussion in the EU since 2016)

=> EU Commission has acknowledged the problem but so far no solution

# 2. Problems of IoT data governance / objectives of „Data Act“ (3)

Data Act acknowledges this main problem and wants to solve it

**Objectives of the Data Act:**

(1) more user (consumer) empowerment and better additional services / competition on secondary markets

(2) „unlocking data“ to make more data available to firms for innovation

(3) fairness in the allocation of value from data among actors in data economy

(4) preserving incentives to invest in generating value through data

Key instrument: **new rights for users** to access IoT data and share them with third parties

# 3. Data access and sharing rights of users: Analysis (1)

Philipps Universität Marburg

## Overview and basic architecture

Starting-point: manufacturers can get exclusive de facto control over IoT data through their own technical design of the IoT devices

(1) Art. 3: Obligation to make data generated by the use of products or related services accessible

(2) Art. 4: The right of users to access and use data generated by the use of products or related services

(3) Art. 5: The right of users to share data with third parties

(4) „Initial contract“ between user and manufacturer / DH: data use of data holder based upon a contract betw. data holder and user (Art. 3, Art. 4(6))

(5) Data sharing with third party requires a „licensing contract“ between DH and TP with FRAND conditions (includ. „reasonable compensation“

Scope of data: raw data through the generation of IoT data (and related services), but not derived or inferred data (scope not so clear)

# 3. Data access and sharing rights of users: Analysis (2)

Philipps Universität Marburg

## Art. 3: Obligation to make IoT data accessible

> Products shall be designed and manufactured, and related services shall be provided, in such a manner that data generated by their use are, by default, easily, securely and, where relevant and appropriate, directly accessible to the user.

- far-reaching provision about the (technical) design of IoT devices
  - \+ plus transparency about generated data, whether continuously or in real-time, and the identity of the data holder who has to make data available etc.

## Art. 4: Right of users to access and use data generated by IoT device (1)

- Looks like a far-reaching right:
  - \+ on a simple request of the user, data holder has to make the data available (w/o need for any further information, e.g., about how it will be used)
  - \+ user seems to be free how to use the data, except
    - > not to compete with data-generating device itself
    - > has to protect trade secrets (technical measures), data protection rights
- But: „data access“ / „make data available“ need not imply right to a data transfer
  - \+ might be only an „in-situ data access right“ (data holder can keep control)

# 3. Data access and sharing rights of users: Analysis (3)

Philipps Universität Marburg

## Art. 5: Right to share data with third parties

> Upon request by a user, or by a party acting on behalf of a user, the data holder shall make available the data generated by the use of a product or related service to a third party, without undue delay, free of charge to the user, of the same quality as is available to the data holder and, where applicable, continuously and in real-time.

- basic idea: for additional services (e.g. repair), for new services (innovation)

## Art. 6: Obligations of third parties receiving data at the request of the user

> A third party shall process the data made available to it pursuant to Article 5 only for the purposes and under the conditions agreed with the user, and subject to the rights of the data subject insofar as personal data are concerned, and shall delete the data when they are no longer necessary for the agreed purpose.

- Data holder and third party conclude a („licensing“) contract about data access,
  - \+ in which the user has the right to define through its contract with the third-party the purpose for what the data should be used,
  - \+ requires a negotiation between the data holder and the TP (FRAND with „reasonable compensation“ for making data available, protection of trade secrets etc.) (with dispute settlement mechanism) (Ch. III: Art. 8-10)
- In my view: **not** really a data portability right, only a right to let others use the data

# 3. Data access and sharing rights of users: Analysis (4)

Additional rules:

- (consumer) protection of users against TP: no coercion, deception, and manipulating of user (dark patterns) or profiling the users (Art. 6 (2) a, b) etc.
- (but also protection of TP against being monitored by data holder)
- **Protection of data and trade secrets of data holders** (technical measures) plus additional far-reaching protections of economic interests of data holders
  + see Art. 11 (para.2: remedies from the IP toolbox)

**Key question: For what can the data be used? (for more liquid data markets?)**

- data can be used for „all legal purposes“ (rec. 28)
- not for competition with IoT device itself but possible for aftermarket services etc., even if the data holders offer these services
- **Who can be TP?** Firms, non-profit organizations, intermediation service provider
  + **but not:** Firms that are **„gatekeepers“** (as designated in Digital Markets Act)
- **Unclear:**
  + Can access to the data be sold to TP?
  + Can this data be aggregated and then access to the aggregated data sold to innovators?
  + additional supply for data intermediaries and data markets?

# 4. Effectiveness of data sharing mechanism in practice? (1)

Key idea: data access to firms through **user-initiated** data-sharing mechanism

- Experience of ineffectiveness with data portability right (Art. 20 GDPR)
  + so far DPRs did only work if heavily regulated: e.g., PSD2
- Will this mechanism work better than Art. 20?
- positive: continuous real-time access possible

However: many problems that make this mechanism weak and ineffective

- Problem group I:
  + bilateral negotiation process between data holder and TP
  + experience with negotiated FRAND solutions show difficulties. What is „reasonable compensation“? (new dispute settlement mechanism)
  + Disputes about protection of „trade secrets“ and data protection
  + TP might get only „in-situ access“ to the data: Does this limit the use and value of the data? Costs of using „in-situ access“?
  + what about effectiveness of enforcement?

# 4. Effectiveness of data sharing mechanism in practice? (2)

Problem group II: To what extent does this data access help?

- Problem 1: it is unclear whether the scope of data that is made available is sufficient for providing additional services or for new innovation
  - + only raw data, and only from individual user: enough for repair service, for predictive maintenance services, for innovation?
  - + also processed / derived data might be needed, or data from many users, and possibility to combine data from different sources
  - + often very important that the data can be aggregated/combined, and be traded on data markets
- Problem 2: lacking technical interoperability
  - + for many aftermarket and other services it is necessary to have technical access to the IoT device (requires access to tools and software)
  - + Data Act does not address this at all (only data interoperability)
  - + often necessary: FRAND access to IoT device / software etc.

=> very unclear how useful these rights are for the users and innovating firms

# 4. Effectiveness of data sharing mechanism in practice? (3)

Philipps Universität Marburg

**Example connected cars**

- „Extended vehicle“ concept: ensures exclusive control of car manufacturers over
  - \+ access to the generated data
  - \+ technical access to the car (closed system / no interoperability)
- Data Act would give a data sharing right to the users
  - \+ problem 1: raw data are not sufficient for repair service providers etc.
  - \+ problem 2: no technical interoperability
  - => User sharing right of Art. 5 does not solve these problems
- additional sectoral regulation is necessary (March 2022: Commission started policy initiative for revision of sectoral type approval regulation)
  - \+ esp. need for FRAND access to functions and resources of connected cars
  - \+ (also discussion about alternative solution to „extended vehicle“ w/o exclusive control of car manufacturers: prevention of gatekeeper position)

**Question:** Is this so different for repair services etc. for other IoT devices?

- Problem: protecting competition / supporting innovation on secondary markets often requires a targeted approach, which Data Act does not offer

# 4. Effectiveness of data sharing mechanism in practice? (4)

Philipps Universität Marburg

**Conclusions:**

- very skeptical whether this leads to an effective data sharing mechanism
- unclear to what extent these rights lead to more, better, and cheaper services for users (more competition, innovation and consumer choice)
- low incentives for consumers to use these rights
  + perhaps better in B2B contexts
- Danger that only few data are made available to innovators with this mechanism (too difficult, too slow, too costly for most firms, esp. SMEs, and easy to obstruct)
- Data sharing mechanism would work better, if
  + clearly regulated regarding scope of data, standardised contracts / processes, where TP can initiate data sharing, effective enforcement by a regulator
  + this user data could be traded and offered on data markets

=> serious doubts about entire approach of relying only on such an user-initiated data sharing right for making data available for innovation and competition

# 5. The unclear initial contract about IoT data with user (1)

Philipps Universität Marburg

**Key role of the contract between manufacturer/seller and user**

- So far not considered: **initial contract** betw. manufacturer and user (sale etc.)
- Art.4(6): „The data holder shall only use any non-personal data generated by the use of a product or related services on the basis of a contractual agreement with the user.“
- this implies: the de facto control position over data alone does not give the data holder the right to use any non-personal data without the consent of the user
  - \+ using the data itself or for others, sharing it with others, extract value from data (data analytics) etc. only possible, if agreed upon in contract with the users (at the time of the sale of the IoT device)

=> theoretically, this looks like a strong position of the users !? Can they use it?

- DA does say nearly nothing about this contract => freedom of contract
- In **B2B contexts** this will be negotiated, and depending on economic conditions (and negotiation power), this can also lead to results that the users will have control over the IoT data (or even become themselves the data holders)

# 5. The unclear initial contract about IoT data with user (2)

Philipps Universität Marburg

**Initial contract in B2C situations (1)**

- existence of serious market failures (esp. information and behavioral problems)
  - + similar to wellknown problems with „consent“ regarding personal data
- It cannot be expected that competition emerges about the conditions of how the data holders can use the generated IoT data
- expected market result: consumers will (have to) accept contracts with very broad consent to the use of all collected data by the data holders for the entire lify-cycle of IoT device („buy-out contracts“)
  - + consumers will be left with „non-waivable“ user rights of Art. 4 and 5 DA
- Any specific protections for consumers?
  - + only precontractual transparency rules but otherwise only freedom of contract
  - + no granular choice options, what data are collected, for what they are used, and which firms they are shared with; and: consumers are „locked in“
  - + many aspects of this contract are unclear (selling of IoT device, change of data holders, termination of contract etc.)

# 5. The unclear initial contract about IoT data with user (3)

Philipps Universität Marburg

**Initial contract in B2C situations (2)**

- DA does not help to solve this market failure / „empower“ consumers for using this contract for „meaningful control“ over IoT data generated w. their own device
- theoretically strong position of consumers through contract will not translate into more consumer empowerment
- also DA does not expect that contract would give consumers more control over how data holders use the IoT data, or a sharing of value of data (data revenues)
  + contract has no function in that respect
- Not surprising that discussion emerges about empowering more the consumers, e.g. through additional consumer protection measures:
  + giving consumers more choice in this contract
  + prohibiting „buy-out contracts“,
  + granting more granular choices, limited duration of this contract etc.

=> these are additional options to introducing „user access and sharing right“ of DA !

**But:** it is also not clear whether more control of consumers over IoT data would have positive effects on data sharing and innovation!

# 6. Data holders: IP-like protection, incentives, and data power (1)

**Does the DA introduce de facto an IP-like position for data holders?**

- The strengthening of the position of data holders:
  - \+ they get from DA a strong protection of their exclusive control over the IoT data
  - \+ it is not an IP-like absolute right but their commercial use of these data is legally acknowledged, and far-reaching measures for protecting their exclusive control (technical protection, „in-situ access rights“ etc.)
  - \+ due to the weak mechanism of user sharing rights this exclusive control will only be limited to a small extent
  - \+ also the „initial contract“ is not a strong limitation of their position (in B2C)
  - => might be **de facto an IP-like protection of the data** generated in IoT devices
- DA justifies this with „preserving incentives to invest in ways to generate value through data“ (DA, p.3)
  - \+ classical IP rationale for exclusive rights on a non-rivalrous intangible good
  - \+ classical solution: balancing need for investment with the benefits of broad use this non-rivalrous good (marginal costs of additional use = zero)

# 6. Data holders: IP-like protection, incentives, and data power (2)

**But do we have an incentive problem regarding IoT data?**

- Making the incentive argument here in the DA so strong is entirely surprising
- So far no concerns or any evidence for an underinvestment in IoT devices or in using too few sensors, cameras, microphones in IoT devices
  + everybody predicts a fast exponential spread of IoT devices and the huge increase of collected data through them
  + incentives for data collection have so far not played no prominent role
- Very unclear whether any incentive problem emerges through these use rights:
  + it is only about the generated data itself, not about inferred/derived data
  + as owners of the IoT devices the users already have paid a price, which solves incentive problem to invest in generating the data that are important for the functionality of the device for the consumers

  => no general incentive problem for data generation in IoT devices !
- But: danger of over-investment in generating IoT data:
  + manufacturers get large incentives for more sensors to collect additional data not necessary for functionality of IoT device => danger to privacy

# 6. Data holders: IP-like protection, incentives, and data power (3)

**Data power, data concentration, and gatekeeper problems**

- Not discussed in DA: possible negative effects through protecting exclusive de facto control of IoT data by data holders
- Many data sets will be unique and therefore allow monopoly prices: leads to under-utilization of data (P > marginal costs of using them)
- Competition problems: gatekeeper problems in IoT ecosystems with negative effects on secondary markets
- Many manufacturers will „sell“ data-holding position to data companies (free data market), who specialize in commercializing them
  - \+ danger of data concentration with few very large data companies
  - \+ might well be GAFA / gatekeeper firms (DMA)
  - \+ can also lead to additional competition problems and market power
  - \+ users are not allowed to make their data available to gatekeeper firms (as TP) but data holders face no restrictions selling the IoT data to these firms

=> Protection of exclusive de facto control of data can lead also to potentially high additional costs through high data prices, data power and market power !

# 7. Expected effects of the Data Act: Results

**Why the objectives will not be fulfilled:**

- **insufficient consumer empowerment**:
  - + weak mechanism for user rights to access and share IoT data (unclear whether more, better and cheaper services)
  - + initial contract does not work as instrument for meaningful control of IoT data
- **insufficient unlocking of IoT data for innovation:**
  - + presumably only very limited amount of data will be made available
  - + will not help much innovation
- **no improvement with respect to fairness regarding sharing of value of data**
  - + fairness only partly addressed B2B with respect to SMEs (negotiation power)
  - + fairness not addressed in B2C situations: very asymmetric distribution of value of IoT data between data holders and consumers
- (**too) large data generating incentives of manufacturers / data holders**
  - + presumably too large incentives through strong protection of exclusive control of DH and weak user rights mechanism

# 8. Conclusions (1)

- DA starts well with diagnosis of exclusive de facto control of manufacturers over data as main problem for not enough access and use of IoT data
- Introducing additional rights is a good approach, but user rights mechanism is too weak and ineffective (need for additional direct access rights)
- Too much strengthening of position of data holders by introducing a de facto „property-like“ protection of non-personal IoT data,
  + which is not limited enough through these weak user rights and
  + makes sharing of IoT data via users hard, expensive, and unattractive
  + large concerns about more data concentration and data power in the future
- far not enough unlocking of data for innovation and competition
- nearly no consumer empowerment regarding meaning ful control over collection/ use of IoT data
- fairness in allocation of value from data not addressed in B2C situations

=> **wrong balancing between objectives of DA: need for rebalancing !**
  + too much emphasis on strengthening data holders
  + not enough on innovation, competition, consumer empowerment, fairness

# 8. Conclusions (2)

Philipps Universität Marburg

Other main problem of DA: **too broad horizontal approach**:

- \+ one data governance solution (property-like „exclusive de facto control“ of manufacturers plus non-waivable user rights) is equally imposed as solution to very different problems and situations (with same data set and same rules)
- \+ this leads both to too large costs and too small effectiveness

Few general recommendations:

(1) Make different solutions for B2C and B2B, because type and extent of market failures are very different

(2) Do not focus on one data set but on problem-oriented data access solutions (scope of data, access to software etc.) for provision of services, innovation, e.g., with more sectoral regulations …

(3) Encourage also other data governance solutions that do not rely on „exclusive de facto control“ of manufacturers, e.g. data trustee solutions, and encourage other ways of solving possible incentive problems (instead data monopolisation)

(4) Be very cautious not to introduce (unintentionally) a de facto exclusive property on non-personal data => dangerous path for innovation and data economy

(5) Legislators should not rush to legislative decisions … very complex problems