

# **EU Data Act: New data access and sharing rights for IoT data**

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

## **TILT & TILEC Workshop on the Data Act**

Tilburg Institute for Law, technology and Society (TILT) &  
Tilburg Law and Economics Center (TILEC)

3 October 2022

# 1. Introduction

Why is the governance of IoT data so important?

- IoT devices spread very fast, and exponential growth of collected data through IoT devices (and: no indication of an under-investment in IoT devices)
  - IoT devices will be **everywhere** (home, working place, public sphere), and **collect data on all of us all the time** (IoT devices are also „**surveillance instruments**“)
- => Governance of IoT data is and will be a very critical issue in a digital society!
- => What data are collected, who has control over them, who can use them for what, and what are the benefits and risks, and for whom?

What I have done so far:

- Analysis of the expected **effects** of the Data Act on its objectives  
*Kerber: Governance of IoT Data: Why the Data Act will not fulfill its Objectives*  
(forthcoming in: GRUR International; working paper available at: <https://dx.doi.org/10.2139/ssrn.4080436>)

## My presentation:

- three main problems
- suggestions how to amend the DA proposal

## 2. Main problem I: Exclusive de facto control over IoT data

- Manufacturers of IoT devices can **get through their own technical design exclusive de facto control** over all data generated by IoT device
  - => access problems for users and firms for providing services and innovation
- de facto exclusivity grants data holder same economic position like an absolute exclusive right on non-personal data
- Based on an incentive argument for data generation, the DA justifies and strengthens the exclusive de facto position and protects it („as if“ it would be an IPR)
- Key question: **Do we have an incentive problem** regarding generation of IoT data, which justifies such an exclusive de facto position?
- very unclear, because price for IoT device can cover costs for generation of data, i.e. additional monetisation via de facto monopoly position over data is not necessary
- too strong, unjustified „protection“ of IoT data of data holders implying a wrong balancing compared to the potentially large benefits of unlocking more data
- => danger that DA introduces a **de facto IP-like „property“ for non-personal data** by legally recognizing and legitimizing „exclusive control positions“ over data
- => provides problematic incentives to design IoT devices to „capture“ and control monopolistically as much data as possible

### 3. Main problem II: User data sharing mechanism can be expected to be weak and ineffective

- (non-waivable) user rights of Art. 4 and 5 are key instruments:
    - + right of users to require data holder to make data available to third parties for purposes determined by the user (plus „licensing agreement“ betw. DH and TP)
    - + objectives: enabling more IoT-related services and innovation
  - **But: many problems and hurdles** that make this mechanism **weak / ineffective**
    - + insufficient scope of data: only raw data (often derived/inferred data needed)
    - + often access to (proprietary) software and tools needed for repair and maintenance services (=> technical interoperability not addressed in DA)
    - + innovation of new services will need access to aggregated data sets, which are hard to collect by data sharing via individual users
    - + a lot of hurdles for contract between TP and data holders: bilateral negotiation (FRAND conditions / “reasonable compensation”), “in-situ” data access, confidentiality agreements / trade secrets, technical protection, ...
    - + very unclear whether it works for making more data available to data markets
- => **not sufficient for:**
- enabling much more innovative services (aftermarkets)
  - unlocking many data for innovation

## 4. Main problem III: Unclear initial contract of users with data holders about use of IoT data

Art. 4(6): data holders can only use IoT data on basis of contract with user

### **B2C situation:**

- theoretically strong position of consumers but same market failures (information/ behavioral problems, behav. manipulation) as with personal data
  - expected result: consumers will (have to) accept contracts with consent to use of all IoT data by the DH (take-it-or-leave-it / buy-out contracts), leaving consumers with only the (non-waivable) user rights of Art. 4 and 5 DA
  - problem: freedom of contract (with only a few precontractual transparency rules)
    - + no granular choice options, what data are collected, for what they are used, and which firms they are shared with (and: we as consumers are „locked in“)
- => DA does not help to solve this market failure and „empower“ consumers for using this contract for „meaningful control“ over IoT data generated w. their own device
- => no control of extent of surveillance by IoT devices (consent/GDPR does not work)

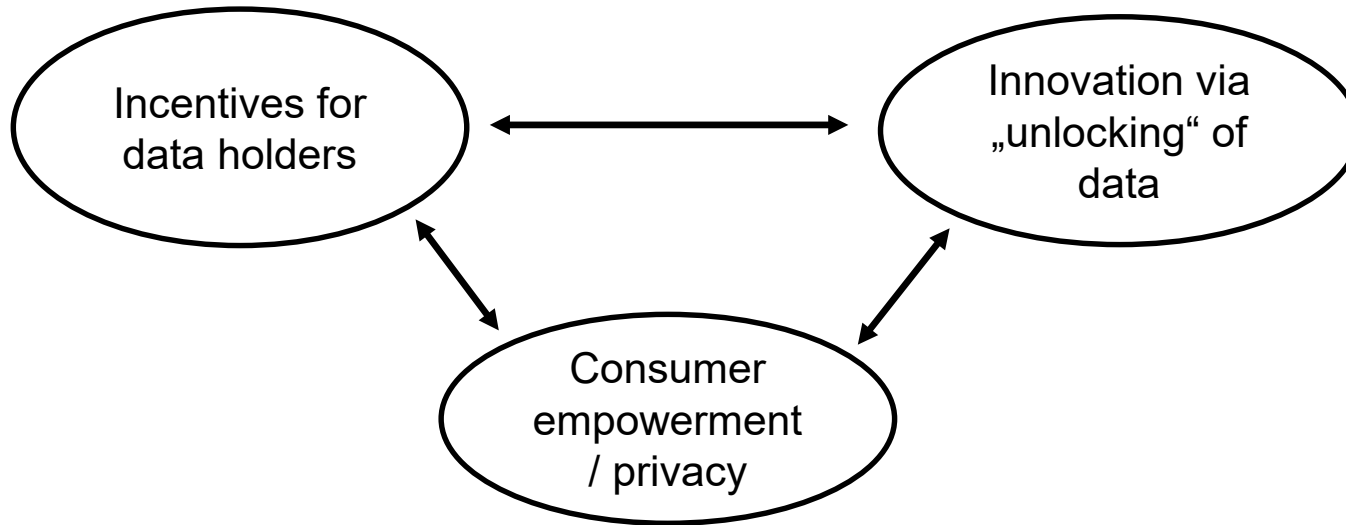
**B2B situations:** this can be very different

## 5. Intermediate Results (1)

- Exclusive de facto control of data holders of IoT data remains largely intact, due to
    - + weak and ineffective data sharing mechanism
    - + control of users through initial contract does not work (in B2C)
  - Objectives of DA will not be fulfilled:
    - + will not solve the problem of „unlocking of data“ for innovation
    - + not enough consumer empowerment
    - + (nearly no contribution to fairness of allocation of value from data)
  - Main reason: **over-protection of exclusive position over IoT data** of manufacturers and data holders, who in my view are the main beneficiaries of the DA and not the users and not the third parties (as the Commission claims)
- => **need for a significant rebalancing** of the DA in favour of more „unlocking of data“ and „consumer empowerment“

## 5. Intermediate Results (2)

Trade offs between incentives for DH, innovation, and consumer empowerment



=> **Rebalancing:** Due to lack of serious incentive problems for IoT data, much more emphasis on innovation via „unlocking of data“ and consumer empowerment

**Can this be achieved through amendments to the current DA proposal?**

=> I am not sure, because it has a very complex architecture

=> small amendments will not be sufficient

## 6. What can be done? Some suggestions (1)

### **No introduction of a quasi-IPR on non-personal data through general legal recognition of de facto exclusive control over data by data holders**

- let us be very cautious to not introduce (intentionally or unintentionally) an IP-like de facto „property“ on non-personal data,
  - + which manuf./DH can grant themselves through their own technical design of the IoT device (leading to the design of entire markets and ecosystems; example: „extended vehicle“ concept of car manufacturers)
  - + leads to huge problems for competition and innovation (e.g. data power)
  - + recitals should clarify this in a much more explicit way (the in the DA already existing principle of non-exclusivity should be strengthened!)
- reduce / eliminate the provisions in the DA that lead to additional protections of the exclusive control of the DH over the data: (not strengthen them by amendments!)
  - + limit/eliminate „in-situ“ access, technical protection measures, Art. 11(2) etc. for protecting generated IoT data of DH (cautious protection of „trade secrets“)
- since the data are not „property“ of DH and no general incentive problem exists,
  - + unclear why we need a negotiated „licensing“ contract between DH and TP (with „reasonable compensation“) in the data sharing mechanism



## 6. What can be done? Some suggestions (2)

### **Make the user data sharing mechanism much more effective**

- since user rights are main instrument for limiting exclusive control of DH and for „unlocking“ data for innovation, then this mechanism must be much more effective
  - + through increasing the benefits for users and third parties and
  - + reducing the transaction costs
- DA entails too many barriers and potential issues of disputes:
  - + too complicated, too slow, too expensive, and not attractive enough for many innovators, esp. start-ups and SMEs (too many hurdles for innovation)
  - + we have to find much simpler and effective solutions
- user data sharing mechanism should lead to more „liquid“ data markets:
  - + clarification that the IoT data from the user rights can be an input for data markets (incl. combination with other data, and the possibility of reselling)
  - + provisions in DA necessary that help in that respect and not impede it
- Data Act should strengthen a **data sharing-friendly culture** but the DA proposal does the opposite through its very data holder-friendly design

## 6. What can be done? Some suggestions (3)

### **More empowerment of consumers over the generation, use, and sharing of generated data from their IoT devices**

- Market failure problems regarding the initial contract between data holders and consumers should be addressed with additional provisions
- Prohibition of behavioral manipulation/dark patterns etc. by DH ( $\Leftrightarrow$  consumers)
- minimum standard of choice options for consumers might be necessary with regard to the collection, use, and sharing of their IoT data
  - + this would also help privacy and data protection (surveillance problem)
- for example: Option that IoT device only generates data that necessary for functionality of IoT device (but no additional data for monetisation, e.g. digital advertising)

### **Development of different provisions for B2B and B2C situations**

- problems, market failures, and possible solutions are very different (often these user rights are not needed in B2B)
- manufacturer can also be the weaker party (perhaps data access right also for manufacturer instead of user)
- in B2B bilateral structure (data holder  $\Leftrightarrow$  user) does often not fit

## 6. What can be done? Some suggestions (4)

Need for discussion of other data governance solutions, which are not based any more on such a „property-like“ position of data holders

=> need for changing the basic architecture of the DA

- acknowledgment that **also direct data access rights** might be necessary, e.g. with respect to large anonymised data sets for AI
- giving **broad scope to sectoral solutions** (DA should not be a „straightjacket“)
- using more **data intermediaries** and/or **data trustee** solutions for aggregating IoT data and making them available to innovators
- solutions for **independent parallel use and monetisation of IoT data by DH and users** (and in competition w. each other; breaks up „exclusivity“/„data monopolies“)
  - + limits scope of initial contract (Art. 4(6)): both have independent „rights“
  - + e.g., based upon concept of „cogenerated“ data (no „licensing contract“ needed)
  - + can also consider „legitimate interests“ of other party and limit the scope of independent use, but can also privilege certain purposes (like, e.g. innovation and other public interests)
  - + (very innovation-friendly proposal of German consumer association vzbv)