



BHO  
LEGAL

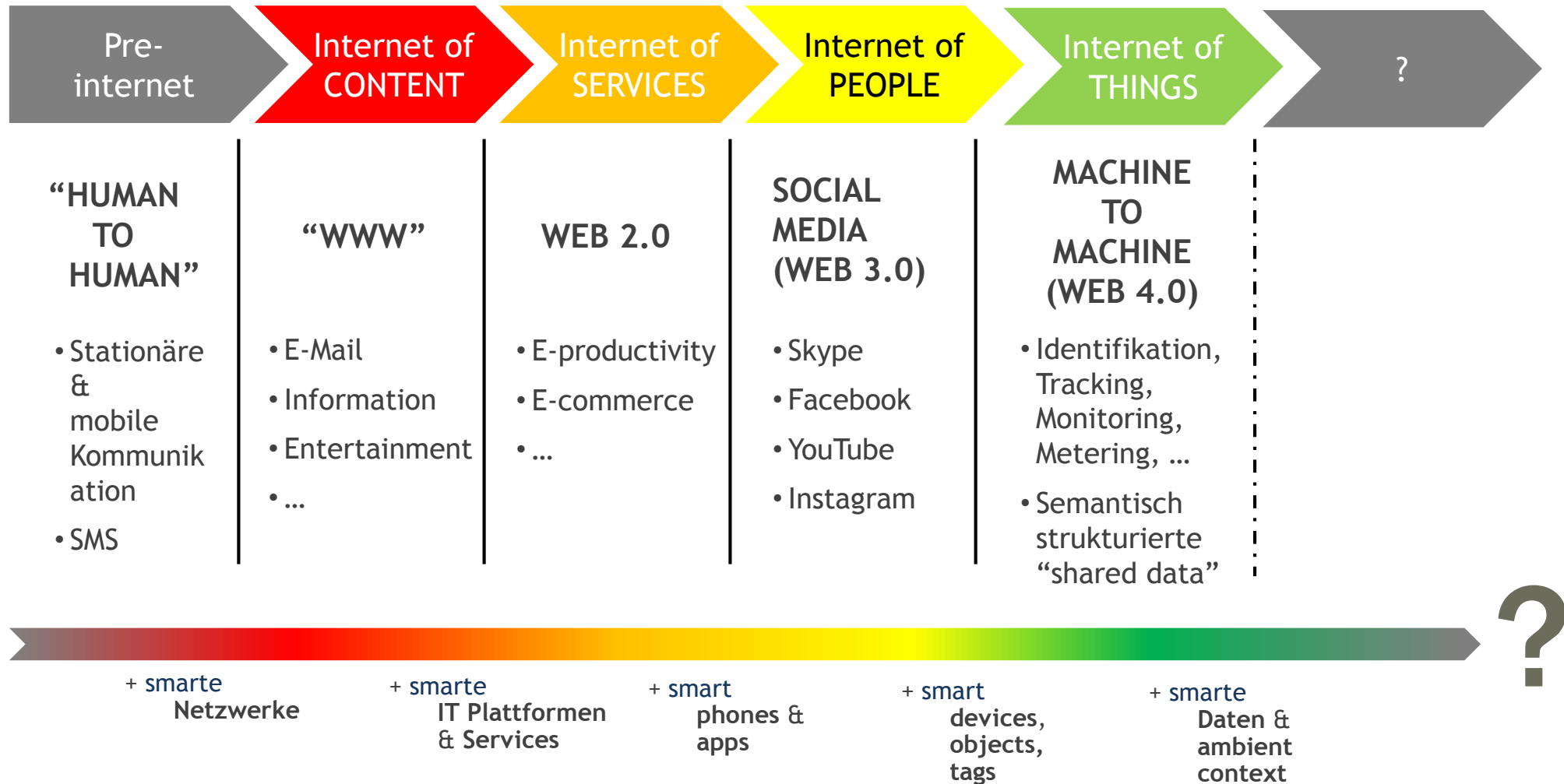
***IoT, M2M***  
***– Wem gehören Maschinendaten?***

Symposium Technologierecht 26. September 2019

*Dr. Philip Lüghausen*

---

# Was ist IoT und M2M?



# Übersicht

## Buzzword-BINGO:

- **Industrie 4.0 und Digitalisierung** entwickeln sich derzeit vom **Hype zum Dogma** für Wettbewerbsfähigkeit und Strategie für die nächsten zehn bis zwanzig Jahre
- „**Things**“ (= Maschinen) im **IoT** sind notwendiges Vehikel der **Digitalisierung**
- Maschinen kommunizieren im IoT miteinander (**M2M**)
- Daten und Metadaten werden ständig und exponentiell steigend produziert und erhoben!
- Das weckt **Begehrlichkeiten** bei allen beteiligten Akteuren
- Auf EU-Ebene und in den Mitgliedsstaaten wird im Rahmen der **Digital Single Market Strategy** über **Data Ownership** nachgedacht
- Wem „gehören“ also Maschinendaten im IoT de lege lata?

## Was bedeutet „gehören“?



- Gehören = in jemandes Eigentum stehen
- Eigentum als Prototyp des absoluten Herrschaftsrechts

### § 903 BGB

Der **Eigentümer einer Sache** kann, soweit nicht das Gesetz oder Rechte Dritter entgegenstehen, **mit der Sache nach Belieben verfahren** und andere von jeder **Einwirkung ausschließen**.

- Aber: Daten sind doch keine Sachen!?

### § 90 BGB

Sachen im Sinne des Gesetzes sind nur **körperliche Gegenstände**.

## Was sind Daten

- ISO/IEC 2382:2015

Daten sind Zeichenfolgen, die von Menschen oder Maschinen gelesen oder verarbeitet werden können

- Daten sind eine Unterart von ~~struktureller (=verkörperter)~~, ~~semantischer (=inhaltlicher)~~ syntaktischer Information

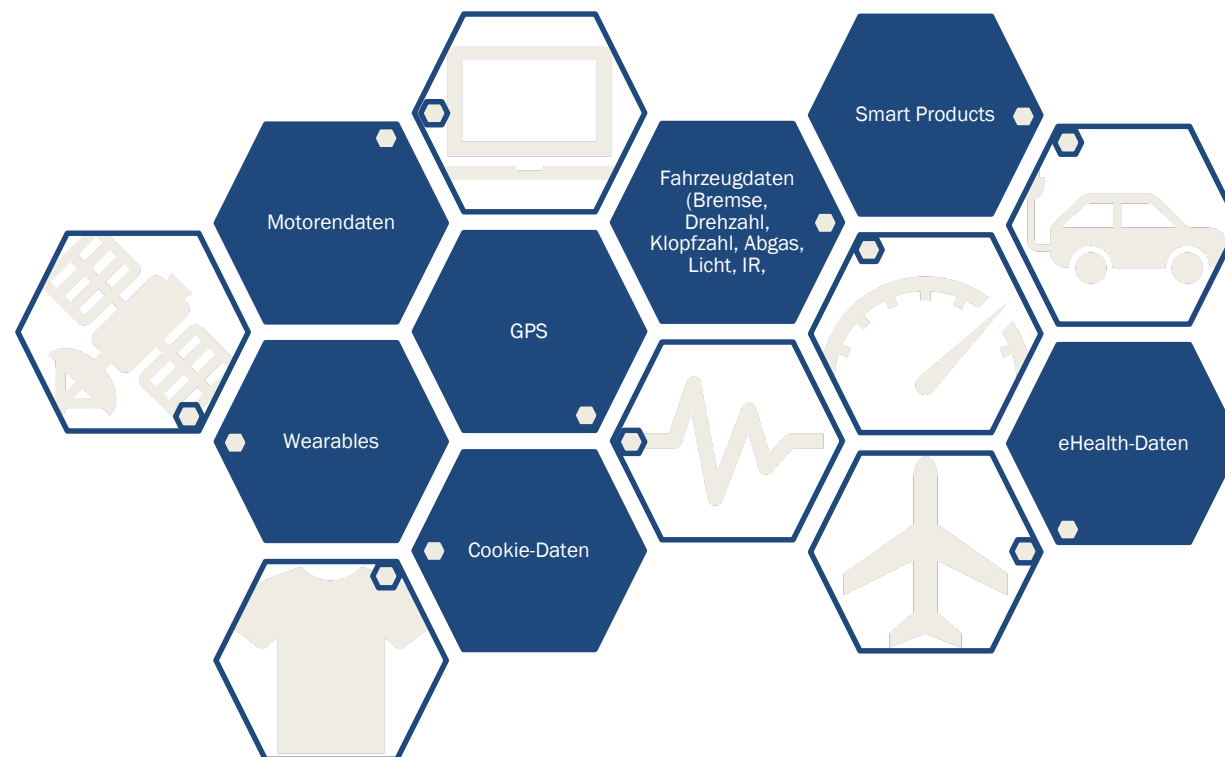
→ Ein Datum ist daher eine **gegebene Zeichenmenge unabhängig vom Informationsgehalt oder Inhalt** und daher lediglich quantitativ definiert

- Es bleibt dabei: **Daten als solche sind mangels Verkörperung keine Sachen!**

- **BGH-Software-Urteil**

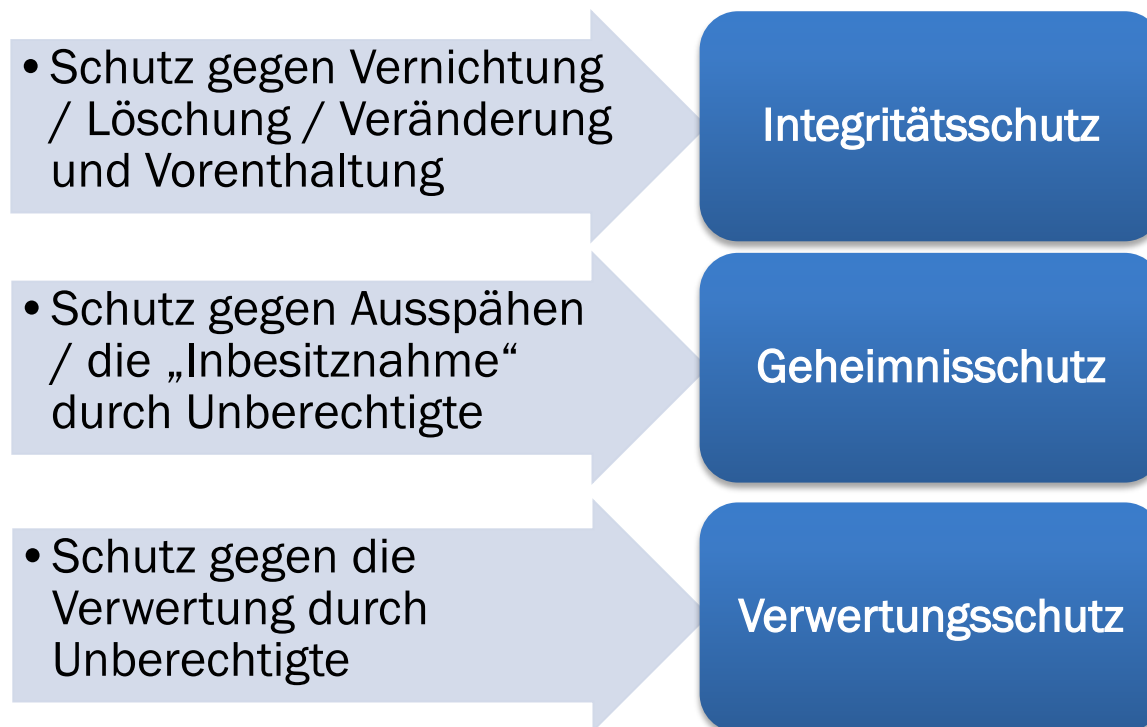
## Welche Arten von Daten gibt es?

- **Breite Definition von Daten** führt dazu dass es unbegrenzt viele Daten gibt
- Daten werden daher nur kategorisiert in (ebenfalls unbegrenzt mögliche) Kategorien und / Unter- / Über- und Querkategorien
- Für uns wichtige Kategorie: **Sensordaten** (Daten, die mit Sensoren (=maschinell) erhoben werden)
- Ebenfalls wichtig: Transportweg der Daten: M2M



## Wogegen müssen Daten Schutz genießen, um zu „gehören“?

### Schutzrichtungen für Daten:



## Woraus können sich Rechte an Daten herleiten?

Um es vorweg zu nehmen:

- Es existiert de lege lata **kein zivilrechtliches grundsätzliches Ausschließlichkeitsrecht** an Maschinendaten
- Begrenzte Ausnahmen **je nach semantischer Qualität der Daten** (UrhG, PatG, DesignG, GebrauchsmusterG, UWG und GeschGehG):
  - Software (§ 69a UrhG)
  - Datenbanken (§§ 87a ff. UrhG)
  - Nachahmungsschutz (§ 4 Abs. 3 UWG) bei wettbewerblicher Eigenart
  - GeschGeh: Geheime Daten, die technischen und/oder organisatorischen Schutzmaßnahmen unterliegen
- **Lediglich akzessorischer Geheimnis- und Verwertungsschutz** über das Sacheigentum (§§ 90, 903, 1004 BGB)
  - Effektiv und praxisrelevant
  - **Aber:** Nicht EU-harmonisiert und setzt Eigentum am Datenträger voraus!



## Woraus können sich Rechte an Daten herleiten?

Aus dem Datenschutzrecht (DSGVO, BDSG)?

- Vermittelt dem Datensubjekt (im Datenschutzrecht: „Betroffener“) ein annähernd absolut wirkendes Abwehrrecht auf semantischer Ebene ((eingeschränkte) Mitteilungshoheit des Datensubjekts)
- Eröffnet aber keine uneingeschränkte Datenherrschaft am **eigenen personenbezogenen (!) Datum**
  - So schon das BVerfG am 15. Dezember 1983
- **Mitteilungshoheit des Datensubjekts und Zweckbindungsgrundsatz** verhindert grundsätzliche die Marketability **personenbezogener Maschinendaten**



## Woraus können sich Rechte an Daten herleiten?

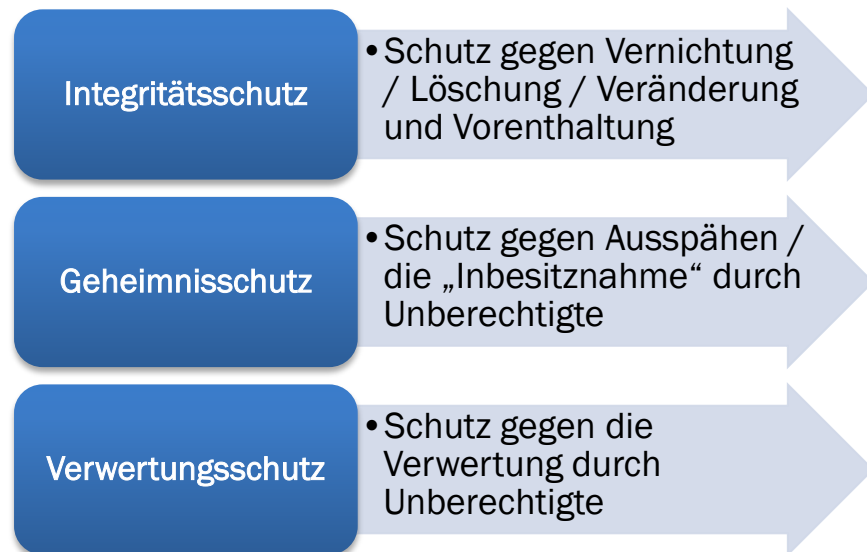
### Derzeit vorrangige (vorläufige) Lösung:

- Vertragsrecht über Nutzungs- und Zugriffsrechte / Herausgabe- und Lösungsansprüche
- Vorteile:
  - Daten können als Leistungssubstrat z.B. über das Kaufrecht oder das Miet/Pachtrecht in Bezug genommen werden.
  - **Flexibel** und international anpassbar
  - Nicht abhängig von (aber möglicherweise beeinträchtigt durch) Schutzrechte Dritter
- Nachteile:
  - Wirkung nur **inter partes**: Schwacher Schutz ggü. Dritten
  - Mangelhafte **Insolvenz- und ZV-Festigkeit**

## Ausblick

- In der Regel erfüllen auf EU-Ebene die von Maschinen erzeugten Rohdaten für sich genommen keine der gesetzliche Schutzanforderungen
- Der Vertragsgestaltung ist daher mittelfristig das besondere Augenmerk zu widmen!
  - **VORSICHT:** Datenschutzrecht
- Auf EU-Ebene (und in den Mitgliedsstaaten) wird weiterhin über die Schaffung eines „Data Ownership“ diskutiert.
- Ein (mitgliedsstaatliches) Ausschließlichkeitsrecht könnte aber in Konflikt mit der Proklamation des „**Grundsatzes des freien Datenverkehrs in der EU**“ stehen, vgl. Verordnung (EU) 2018/1807 „Free Flow of Data Initiative“ (→Abschottungseffekt)
- **Ausbau Cloud-Computing:** Um in Zukunft im IoT in der EU marktfähig zu bleiben, widmet sich die European Cloud Initiative (2 Mrd. EUR aus Horizon 2020) z.B. der European Open Science Cloud (EOSC)
- **Bemerkenswert auf nationaler Ebene:**
  - Unklarheit über zukünftige Geschäftsmodelle und daher auch wer welche Rechte braucht / nicht braucht!
  - Daher: Unsicherheit der Akteure, ob ein Datenrecht nicht mehr Probleme herbeiführt, als es löst

## Ausblick



Solange keine konkreten Geschäftsmodelle anliegen, deren Aufkommen ein Ausschließlichkeitsrecht erfordern, gilt:

**Code is Law**

→ Gut verschlüsselte Daten gewähren Dateninhabern ein Maximum faktischer Datenherrschaft

## Kontakt

BHO Legal

Hohenstaufenring 29-37  
50674 Köln

Tel.: + 49 (0) 221 270 956 0  
Fax: + 49 (0) 221 270 956 222

[cologne@bho-legal.com](mailto:cologne@bho-legal.com)

Dr. Philip Lüghausen

Rechtsanwalt | Partner

Tel.: + 49 (0) 221 270 956 210  
Mobil: + 49 (0) 161 28 31 86 9

[philip.lueghausen@bho-legal.com](mailto:philip.lueghausen@bho-legal.com)