

---

# Freiheit und Verantwortung



Das Netz zwischen Anonymous und der NSA

---

Hochschule der Medien Stuttgart  
3. Digital Rights Day 2014



Brauchen wir eine staatliche Regulierung des Netzes?

# FREIHEIT UND VERANTWORTUNG

# Agenda



⇒ Brauchen wir staatliche Regulierung des Netzes?

- ▶ Freiheit und Verantwortung
- ▶ Ziele staatlicher Regelungen
- ▶ Anforderungen an diese Regelungen

⇒ Bestehende Regelungen und Problemfelder

⇒ Ideen und Lösungsansätze



# Freiheit

⇒ Freiheit darf nicht grenzenlos sein.

*„Die Freiheit des Einzelnen endet dort,  
wo die Freiheit des Anderen beginnt.“*

– Immanuel Kant zugeschrieben



# Freiheit und Verantwortung

- ⇒ Freiheit bedeutet Macht.
- ⇒ Macht bedeutet Verantwortung.

*„With great power  
comes great responsibility.“*

– Uncle Ben  
in "Spider-Man", 2002



# Freiheit und Verantwortung

- ⇒ Freiheit bedeutet ~~Macht~~ **Verantwortung**.
- ⇒ Macht bedeutet Verantwortung.

*liberty*  
*„With great ~~power~~*  
*comes great responsibility.“*

# Freiheit und Verantwortung



⇒ Freiheit bedeutet Verantwortung.

*„Liberty means responsibility.  
That is why most men dread it.“*

– George Bernard Shaw, 1903  
in: Man and Superman,  
“The Revolutionist’s Handbook”

# Freiheit und Verantwortung



- ⇒ Freiheit bedeutet Verantwortung.
- ⇒ Freiheit bedeutet zunächst Eigenverantwortung.
- ⇒ Der Mensch neigt im allgemeinen eher nicht dazu, sich dem Unangenehmen zu stellen.
- ⇒ Verantwortung ist meistens nicht angenehm.
- ⇒ Eigenverantwortung trägt nicht immer.





# Freiheit und Grenzen

- ⇒ Freiheit darf nicht grenzenlos sein.
- ⇒ Freiheit benötigt Grenzen.
- ⇒ Grenzen werden regelmäßig nur eingehalten, wenn Grenzüberschreitungen Konsequenzen nach sich ziehen.
- ⇒ Wenn die Eigenverantwortung versagt, muss es auch möglich sein, zur Verantwortung gezogen zu werden.



# Freiheit $\Leftrightarrow$ Sicherheit

- ⇒ Absolute Freiheit schließt Sicherheit aus.
- ⇒ Absolute Sicherheit schließt Freiheit aus.
- ⇒ Freiheit ist auch die Freiheit von Angst.
  - ▶ Angst vor anderen Staaten (und Fremden)
  - ▶ Angst vor den eigenen Mitbürgern
  - ▶ Angst vor dem eigenen Staat



# Freiheit von Angst

*„In the twenty-first century,  
all States and their collective institutions  
must advance the cause of larger freedom —  
by ensuring freedom from want,  
**freedom from fear** and  
freedom to live in dignity.”*

- Kofi Annan, 21.05.2005  
in: United Nations, Report of the  
Secretary-General: “In larger  
freedom: towards development,  
security and human rights for all”



# Freiheit $\Leftrightarrow$ Sicherheit

*„They who can give up essential liberty  
to obtain a little temporary safety,  
deserve neither liberty nor safety.”*

- Benjamin Franklin, 1775  
in: Remarks on the Propositions  
(A Plan which it is believed would produce a  
permanent union between Great Britain and  
her Colonies)



# Freiheit $\Leftrightarrow$ Sicherheit

*„Ohne Sicherheit vermag der Mensch weder seine Kräfte auszubilden noch die Früchte derselben zu genießen; denn ohne Sicherheit ist keine Freiheit.“*

- Wilhelm von Humboldt, 1851  
in: Ideen zu einem Versuch, die Grenzen der Wirksamkeit des Staats zu bestimmen



# Freiheit $\Leftrightarrow$ Sicherheit

⇒ Zur Freiheit gehört als notwendige Ergänzung die Sicherheit,

- ▶ dass jeder für sein Tun Verantwortung übernehmen muss

und

- ▶ dass jeder für sein Tun auch zur Verantwortung gezogen werden kann.

# Grenzüberschreitungen



- ⇒ Der individuellen Freiheit müssen Grenzen gezogen werden um der Freiheiten aller willen.
- ⇒ Die Überschreitung dieser Grenzen muss auch Konsequenzen haben (können).
- ⇒ Grenzüberschreitungen verletzen (potentiell) Rechte anderer.
- ⇒ Grenzüberschreitungen sind (potentielle) Rechtsverletzungen.

# Grenzüberschreitungen



- ⇒ Der individuellen Freiheit müssen Grenzen gezogen werden um der Freiheiten aller willen.
- ⇒ Die Überschreitung dieser Grenzen muss auch Konsequenzen haben (können).
  - ▶ strafrechtlich
  - ▶ zivilrechtlich
  - ▶ im Rahmen der institutionellen Selbstkontrolle



# Ziele gesetzlicher Regelungen



Welche Ziele sollte die Regulierung des Netzes verfolgen?

⇒ **Verhinderung** von Rechtsverletzungen

▶ durch Abschreckung

⇒ **Beseitigung** von Rechtsverletzungen

▶ soweit möglich

⇒ Verhinderung von  
**wiederholten Rechtsverletzungen**

# Anforderungen



Gesetzliche Regelungen zur Regulierung des Netzes sollten ...

- ⇒ ihre Ziele möglichst sicher erreichen
- ⇒ möglichst wenig „Nebenwirkungen“ haben
  - ▶ legale Tätigkeiten möglichst wenig beeinträchtigen
  - ▶ persönliche Freiheiten möglichst wenig einschränken
- ⇒ handhab- und umsetzbar sein
  - ▶ für den Staat (Strafverfolgungsbehörden, Gerichte)
  - ▶ für den Bürger
- ⇒ möglichst geringe Vollzugsdefizite aufweisen



Wie steht es derzeit um den Rechtsrahmen im Netz?

# STATUS QUO

# Agenda



⇒ Brauchen wir staatliche Regulierung des Netzes?

⇒ Bestehende Regelungen und Problemfelder

- ▶ Regelungsziele und Regelungsbeispiele
- ▶ Probleme bestehender Regelungen
- ▶ Impressum, „Forenhaftung“, Urheberrecht und Datenschutz

⇒ Ideen und Lösungsansätze



# Impressumsregelungen

⇒ Ziel: Verantwortlicher für Webangebote soll identifizierbar und erreichbar sein.

- ▶ Erkennbarkeit
- ▶ ladungsfähige Anschrift

⇒ Regelungen:

- ▶ § 5 Telemediengesetz (TMG) für „*geschäftsmäßige, in der Regel gegen Entgelt angebotene Telemedien*“
- ▶ § 55 Rundfunkstaatsvertrag (RStV) für „*Telemedien, die nicht ausschließlich persönlichen oder familiären Zwecken dienen*“, insbesondere für „*Telemedien mit journalistisch-redaktionell gestalteten Angeboten*“



# Impressumsregelungen II

- ⇒ Die Regelung ist grundsätzlich durchdacht und für gewerbliche Anbieter und Medienunternehmen auch geeignet.
- ⇒ Problempunkte:
- ▶ Identifizierung von Privatpersonen (Privatanschrift!)
  - ▶ massives Umsetzungsdefizit
  - ▶ im Gegensatz dazu:  
regelmäßige (Massen-)Abmahnungen

# „Forenhaftung“



## ⇒ Ziele:

- ▶ Rechtsverletzungen in Onlinemedien sollen unterbunden werden können.
- ▶ An Provider (Hoster) sollen keine unerfüllbaren Ansprüche gestellt werden.
- ▶ Nutzer sollen dem Hoster gegenüber anonym oder pseudonym auftreten können (§ 13 Abs. 6 TMG).

⇒ Bereits die Ziele sind erkennbar widersprüchlich.

# „Forenhaftung“ II



## ⇒ Regelungen:

- ▶ Haftungsabschichtung (§§ 7–9 TMG) zwischen
  - eigenen,
  - bereitgehaltenen fremden und
  - nur durchgeleiteten Informationen
- ▶ **Haftungsfreistellung** für durchgeleitete Informationen, **Haftungsprivilegierung** für bereitgehaltene fremde Informationen (Haftung erst ab Kenntnis)

## ⇒ Modifikation durch Rechtsprechung:

- ▶ Haftungsprivilegierung gilt nur für Schadensersatz-, nicht aber für Unterlassungsansprüche
- ▶ Einzelheiten schwer überschaubar und im Fluss



# „Forenhaftung“ III



- ⇒ Der Versuch, unvereinbar erscheinende Zielvorstellungen miteinander zu verbinden, ist als gescheitert zu betrachten.
- ⇒ Die gesetzliche Regelung kann keinen fairen Interessenausgleich gewährleisten.
- ⇒ Die Rechtsprechung konnte ebenfalls noch keine überzeugende Lösung „aus einem Guss“ liefern.

# Urheber- / Verwertungsrechte



- ⇒ Ziel: Gerechter Interessenausgleich zwischen Urhebern (und – vor allem – Verwertern) auf der einen und Nutzern (Konsumenten) auf der anderen Seite.
- ▶ Neue Probleme durch Netz und digitale Technik:
    - verlustlose Kopien
    - ubiquitäre Kommunikation
  - ▶ Regelungskonzepte aus der analogen Welt greifen nur sehr bedingt:
    - private Vervielfältigungsrechte
    - Ausgleich durch Abgaben auf Medien und Geräte
  - ▶ Bereits „analog“ erkannt:  
eine „Totalüberwachung“ ist unmöglich



# Urheber- / Verwertungsrechte II

⇒ Regelungen (ausschnittsweise):

- ▶ Unzulässigkeit von Privatkopien einer „offensichtlich rechtswidrig hergestellten oder öffentlich zugänglich gemachten Vorlage“
  - Tauschdienste
  - illegale Downloadangebote
  
- ▶ Recht der „öffentlichen Zugänglichmachung“
  - traditionelle Anbindung des Urheberrechts an Vervielfältigungen (Kopien) erfasst Netzangebote nicht

# Urheber- / Verwertungsrechte III



⇒ Probleme (ausschnittsweise):

- ▶ Anbieter im Ausland sind oft nicht greifbar
- ▶ Nutzeridentifizierungen über Auskunftersuchen an Provider (§ 101 UrhG)
  - erfordern eine Datenspeicherung beim Provider
  - werden richterlich aller Voraussicht nach aufgrund der Masse (und der Eilbedürftigkeit) nur cursorisch geprüft
- ▶ Anschlussinhaber sind nicht zwingend auch Verletzer
- ▶ Streitwerte der Abmahnungen führen zu prohibitiven Kosten mit Strafcharakter
- ▶ Abmahnungen erfolgen nicht zum Zweck der Rechtsverteidigung, sondern der Einkommensgenerierung.



# Datenschutz im Netz

- ⇒ Ziel: Schutz des Nutzers vor Ausforschung durch Anbieter und einer umfassenden Verknüpfung der anfallenden Daten („gläserner Nutzer“)
  
- ⇒ Regelungen (ausschnittsweise):
  - ▶ Grundsatz der Datensparsamkeit
  
  - ▶ Anspruch auf anonyme/pseudonyme Nutzung
  
  - ▶ grundsätzliches Verbot der Speicherung von Verkehrs- bzw. Nutzungsdaten mit Einwilligungsvorbehalt



# Datenschutz im Netz II

## ⇒ Tatsächliche Folgen:

- ▶ kaum mehr übersehbare Komplexität der Regelungen
- ▶ Auslegungstreitigkeiten → Rechtsunsicherheit
- ▶ Anwendung gebräuchlicher wie auch neuer Webtechnologien ist datenschutzkonform nicht oder nur mit wirklichkeitsfremden Aufwand möglich:
  - Einbindung sozialer Netzwerke (Facebook-, Twitter-, Google+-Buttons)
  - Webanalyse (Google Analytics, Piwik)
  - Logging (IP-Adressen!)
    - Logfiles von Web-, Mail- usw. -Servern
    - Kommentare, Forenbeiträge
  - Cookies

# Datenschutz im Netz III



## ⇒ Tatsächliche Folgen:

- ▶ Nutzer sind (trotz allem) verfolg- und identifizierbar:
  - (persistent) Cookies, Tracker, Webbugs, Pixel, Beacons
  - Browseridentifizierung
  - Zusammenführung von Informationen aus verschiedensten Quellen durch große Anbieter wie Google oder Facebook („big data“)
- ▶ Eine Vielzahl von Informationen wird durch Benutzer aus Unkenntnis, aufgrund des damit verbundenen Komforts oder schlicht aus Mangel an Alternativen freiwillig den Anbietern überlassen.
- ▶ Das deutsche Datenschutzrecht ist im Ausland zahnlos; Geheimdienste wie die NSA scheren sich ohnehin nicht um Datenschutzregelungen.



# Datenschutz im Netz IV

## ⇒ Konsequenz:

- ▶ Große Anbieter haben Zugriff auf eine Vielzahl von Daten, die sie nicht selten auch personalisieren können.
- ▶ Inwieweit (deutsche und europäische) Datenschutzvorgaben eingehalten werden, ist schwer kontrollierbar, Rechtsverstöße sind kaum verfolgbar.
- ▶ Dennoch werden legale Angebote erheblich behindert.
- ▶ Dennoch beeinträchtigen datenschutzrechtliche Regelungen die Verfolgung privater Rechte wie auch die Strafverfolgung nicht unerheblich.





Anonymität im Netz verträgt sich nicht  
mit der Übernahme von Verantwortung

# VERANTWORTUNG STATT VERANTWORTUNGSLOSIGKEIT

# Agenda



⇒ Brauchen wir staatliche Regulierung des Netzes?

⇒ Bestehende Regelungen und Problemfelder

⇒ Ideen und Lösungsansätze

- ▶ Grundproblem derzeitiger Regelungen: Belohnung von Verantwortungslosigkeit
- ▶ verpflichtende Nutzeridentifizierung
- ▶ indirekte Pflicht zur Nutzeridentifizierung
- ▶ pseudonyme Nutzeridentifizierung

# Thesen



- ⇒ Grundlage der bisherigen Regelungen ist nicht nur eine fehlende Verpflichtung, sondern oft sogar ein weitgehendes Verbot der Nutzeridentifizierung und -kontrolle.
- ⇒ Die Folge ist eine Belohnung von Verantwortungslosigkeit statt der Einforderung von Verantwortung.
- ⇒ Es ist daher geboten, eine Nutzeridentifizierung zumindest zu erlauben, wenn nicht sogar vorzuschreiben, und an den Verzicht darauf weitergehende Haftungsfolgen zu knüpfen.

# Verantwortungslosigkeit



- ⇒ Redaktionelle Kontrolle führt aufgrund der damit verbundenen Kenntnisnahme zur direkten Haftung für Inhalte. Je weniger Kontrolle, desto – rechtlich – günstiger für den Anbieter.
- ⇒ Die Erfassung – und Überprüfung – von personenbezogenen Daten führt nicht nur zu Aufwand, sondern zu Rechtfertigungszwang (Datensparsamkeit, Recht auf anonyme/pseudonyme Nutzung). Je weniger der Anbieter über seine Nutzer weiß, desto günstiger für ihn.

# Verantwortungslosigkeit II



- ⇒ Die Speicherung der Zuordnung von IP-Adressen zu Nutzern ist beim Accessprovider (außer zu Abrechnungszwecken) nur unter hohem Begründungsaufwand möglich. Je weniger der Provider sich Gedanken macht, desto einfacher wird die Lage für ihn.
- ⇒ Je weniger der Anschlussinhaber sein Netz sichert, desto eher kann er sich darauf zurückziehen, dass Rechtsverstöße ihm nicht zuzurechnen sind (Stichwort „offenes WLAN“).



# Nutzeridentifizierung

- ⇒ Unter dem Gesichtspunkt der Übernahme von Verantwortung wäre das Gegenteil logisch:
- ▶ Je stärker ein Anbieter sich bemüht, Rechtsverletzungen seiner Nutzer zu unterbinden, desto günstiger sollte seine rechtliche Stellung sein.
  - ▶ Statt eines – teilweisen – Verbots der Nutzeridentifizierung würde sich umgekehrt eine entsprechende Verpflichtung anbieten (Vorratsdatenspeicherung).
  - ▶ Alternativ ließe sich die Haftung des Anbieters an das Maß der gezeigten Eigenverantwortlichkeit koppeln.



# Haftung für anonyme Nutzer

- ⇒ Alle Bemühungen der Rechtsprechung, Dritte unter dem Gesichtspunkt der Störerhaftung in die Verantwortung zu nehmen, finden ihren Grund darin, dass der Primärstörer nicht greifbar ist.
  - ▶ „Forenhaftung“:  
Forennutzer sind nicht identifizierbar
  - ▶ Haftung des Anschlussinhabers:  
Nutzer ist nicht identifizierbar
- ⇒ Warum dann den Haftungsumfang nicht davon abhängig machen, ob der Dritte / der Anbieter den Primärstörer (Nutzer) benennen kann?



# Direkte Haftung

- ⇒ Denkbar wäre bspw. die Einführung einer unmittelbaren Haftung desjenigen Anbieters, der seine Nutzer nicht identifizieren kann oder nicht zumindest – hilfsweise – ausreichende Anstrengungen in dieser Richtung nachweisen kann.
- ⇒ Wer den Primärstörer benennen kann, ist nur zur Beseitigung ab Kenntnisnahme verpflichtet.
- ⇒ Wer dies nicht kann (oder will), muss selbst eine Wiederholung sicher verhindern (Unterlassungsverpflichtung).





# Indirekte Haftung

- ⇒ Stattdessen – oder ergänzend – wäre eine Erweiterung der Anforderungen an den Provider bezüglich der Unterbindung wiederholter Rechtsverstöße denkbar, die ihn faktisch zur Identifizierung seiner Nutzer zwingt, weil er nur so sicher eine Wiederholung (durch Neuanmeldung nach Accountsperre) unterbinden kann.
- ⇒ Dabei käme auch eine Form der pseudonymen Identifizierung in Betracht.



# Pseudonyme Identifizierung

- ⇒ Zumindest wiederholte Rechtsverletzungen lassen sich auch dann vermeiden, wenn der Provider zwar nicht die reale Identität seines Nutzers kennt, aber ein nicht (ohne großen Aufwand) änderbares Pseudonym.
  - ▶ Zuordnung eines definierten Pseudonyms (Hash?)
  - ▶ Schaffung privater Identifizierungsdienste
  - ▶ Einbau eines pseudonymen Zertifikats als Funktion des neuen Personalausweises
- ⇒ Solche Lösungen würden eine Pseudonymität ggü. dem Provider mit einer Identifizierbarkeit für Strafverfolgungszwecke verbinden.

# Verlust der Anonymität



⇒ Ein Anrecht auf (absolut) anonyme Kommunikation, die auch für Zwecke der Strafverfolgung nicht gebrochen werden kann, besteht nicht.

BVerfG, Beschluss vom 24.01.2012 – 1 BvR 1299/05 –

⇒ Um eine auch nur annähernd sichere Anonymität zu gewährleisten, bedarf es bereits jetzt eines nicht unerheblichen Aufwands.



# Missbrauchsgefahren

- ⇒ Dass verschiedene Netzidentitäten zusammengeführt werden können, kann dadurch verhindert werden, dass das „reale“ Pseudonym durch den Anbieter nicht nach außen kommuniziert werden darf.
- ⇒ Sinnvoller als Datenerhebungsverbote sind Verbote der Verwendung, Verknüpfung und Übermittlung von Daten.
- ⇒ Kontrolldefizite bestehen überall in gleicher Weise.



# Freie Meinungsäußerung

- ⇒ Das Grundrecht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten, garantiert unsere Verfassung.
- ⇒ Zu seiner verantwortungsvollen Wahrnehmung ist starke Anonymität nicht erforderlich.
- ⇒ Der Wunsch nach Anonymität als Form der absoluten Freiheit muss hinter dem Bedürfnis der Allgemeinheit zurückstehen, Rechtsverletzer und Straftäter zur Verantwortung zu ziehen.

# Ausblick



⇒ Mit der Möglichkeit, Nutzer für das, was sie tun, verantwortlich zu machen, sind natürlich noch längst nicht alle Probleme gelöst.

Impressumsregelungen:  
– Privatadresse  
– fehlende Durchsetzbarkeit

betrügerische  
Massenabmahnungen

Streitwerte von  
Abmahnungen

fehlende internationale  
Durchsetzbarkeit

fehlender Datenschutz  
ggü. Unternehmen

⇒ Immerhin wäre es aber ein erster Schritt.

# Danke!



## Danke für Ihre Aufmerksamkeit!

Thomas Hochstein  
<http://thomas-hochstein.de/>