


**Zeitschriftenartikel:**

Begutachtet

**Redaktion und Begutachtung:**Patricia Blume 

Universität Leipzig

Kai Matuszkiewicz Philipps-Universität Marburg / Institut für  
MedienwissenschaftMarcel Wrzesinski Alexander von Humboldt Institut für In-  
ternet und Gesellschaft**Erhalten:** 31. Dezember 2024**Akzeptiert:** 08. Dezember 2025**Publiziert:** 02. März 2026**Lizenz:**

© Yuliya Fadeeva


Dieses Werk steht unter der Lizenz Crea-  
tive Commons Namensnennung 4.0 Inter-  
national (CC-BY 4.0)**Datenverfügbarkeit:**Alle relevanten Daten befinden sich in-  
nerhalb der Veröffentlichung.**Finanzierung:**Diese Arbeit entstand während der Be-  
schäftigung als Postdoc am Institut für  
Kommunikationswissenschaft, Fakultät  
für Geisteswissenschaften, Universität  
Duisburg-Essen.**Interessenskonfliktstatement:**

Es liegen keine Interessenkonflikte vor.

**Empfohlene Zitierung:**Fadeeva, Y. (2026). *Science Tracking über  
Transformationsverträge und Wissen-  
schaftsplattformen. Vom Beifang zum  
Hauptziel.* kommunikation@gesellschaft,  
26(1), doi: 10.15460/komm-  
ges.2025.26.1.1643

# Science Tracking über Transformationsverträge und Wissenschaftsplattformen

## Vom Beifang zum Hauptziel

Yuliya Fadeeva<sup>a\*</sup> <sup>a</sup>Universität Duisburg-Essen\*Korrespondenz: [yuliya.fadeeva@uni-due.de](mailto:yuliya.fadeeva@uni-due.de)

## Abstract

Der Text untersucht einige Aspekte von Science Tracking, verstanden als die systematische und großflächige digitale Überwachung von Wissenschaft und Wissenschaftler:innen durch ehemalige Großverlage, die als Oligopol den Publikationsmarkt dominieren. Im Rahmen der Digitalisierung und der Open-Access-Transformation entwickelten sie sich zu Datenanalyse-Konzernen mit Geschäftsmodellen, die auf kontinuierlicher Datenabschöpfung in ihren Plattformen und Anwendungen basieren. Damit bringen sie einerseits Tracking-Praktiken in die Wissenschaft – im Gewand der „Verbesserung ihrer Produkte“ und „legitimer Interessen“, mit unbenannten Geschäftspartner:innen und einseitigen Text-and-Data-Mining-Regeln in Open-Access-Transformationsverträgen. Diese Praktiken bergen neben direkten Gefahren der Wissenschaftsspionage und konkreten Bedrohungen für Wissenschaftler:innen auch subtilere Probleme für wissenschaftliche Integrität. Hier geht es um die Relevanz von Privatheit für wissenschaftliche Arbeit. Andererseits erreicht dadurch die Kommodifizierung der Wissenschaft eine neue Ebene, indem die Mechanismen der Webökonomie Einzug in wissenschaftliche Institutionen und Prozesse halten und die Voraussetzungen für unabhängige Wissenschaft erodieren. Gleichzeitig wächst mit der Implementierung weiterer Anwendungen der marktdominierenden Konzerne auch ihr Einfluss auf Institutionen. Durch ihre Präsenz im Forschungszyklus, Wissenschaftsmanagement und mit jedem Big Deal im Publikationssektor bestimmen sie die Entwicklung von Open Access und Open Science hin zu einem Lock-In der Wissenschaft. Nach einer Einbettung der Tracking-Praktiken in die AdTech-Wirtschaft bespreche ich das spezifische Tracking im Wissenschaftsbereich als eine inhärente Funktion der Produkte und Plattformen, das auch die aktuelle Open-Access-Implementierung in Form von Transformationsverträgen durchzieht. Eine analytische Trennung zwischen Science Tracking und Open Access braucht die Unterscheidung zwischen kommerziellen und nicht-kommerziellen Trägerorganisationen mit den durch sie bestimmten Infrastrukturen.

**Schlagnworte:** Science tracking, open-access-transformation, big five, data analytics, DEAL

## 1 Einleitung<sup>1</sup>

Die Transformation zu globalem Open Access ist ein komplexer, vielschichtiger Prozess, der heterogene Folgen zeigt sowie auch künftig erwarten lässt. In diesem Beitrag geht es um eine Entwicklung der Open-Access-Transformation im Kontext etablierter Großverlage und der *Big Deals*, spezifisch der aktuell in Deutschland laufenden DEAL-Transformationsverträge mit den größten Playern Elsevier (1. Vertrag 2023–2028), Springer Nature (2. Vertrag, 2024–2028) und Wiley (2. Vertrag 2024–2028).

Die thematisierten Entwicklungen sind keine Folge der Idee von Open Access und Open Science oder der vielseitigen Bewegung als solcher, sondern zeigen eine Aporie des Maxwell-Garfield'schen-Modells (Lauer, 2022) des wissenschaftlichen Publizierens auf. Dieses Modell entstand nach dem Zweiten Weltkrieg in Großbritannien und während des Kalten Kriegs in den USA, unter sehr spezifischen ökonomischen und politischen Bedingungen. In einer Situation erhöhter Förderung der Wissenschaftssparte wurde es widerstandslos möglich, dass ein Individuum mit einer findigen Geschäftsidee wie Robert Maxwell die wissenschaftliche Publikationsökonomie völlig veränderte. Dabei etablierten sich sehr ungleiche Bedingungen, die alle finanziellen Erträge, Macht und Urheberrechte bei den Publikationsorganen akkumulierten und Kosten, Arbeitsleistung und Abhängigkeit bei den Wissenschaftsinstitutionen und Wissenschaftler:innen.

Eugene Garfields Science Citation Index wissenschaftlicher Zeitschriftenartikel, primär als eine Methode gedacht, Bibliotheken bei der Auswahl relevanter Zeitschriften für die Subskription zu unterstützen, veränderte sich bald, als Web of Science mit dem darin erstellten Journal Impact Factor zum zentralen Instrument der Quantifizierung wissenschaftlicher Relevanz wurde: „Die Analyse von Daten über die Wissenschaft ist für deren Selbststeuerung immer wichtiger geworden. Aus einem Bibliotheksindex ist eine Wissenschaftsmetrik geworden.“ (Lauer, 2022, S. 3). Sowohl die Bestimmung wissenschaftlicher Relevanz in Form bibliometrischer Faktoren als auch wissenschaftliche Publikationsstrukturen mit den eng daran gebundenen Reputationsmechanismen sind historisch kontingent in proprietärer Hand, werden aber nach wie vor öffentlich finanziert.

Im Verlagsfeld fand in den letzten Jahrzehnten eine immer größere Konzentration statt, sodass mittlerweile die sogenannten Big Five – Elsevier, Springer Nature, Wiley, Taylor & Francis und Sage – das Feld beherrschen: „Overall, the market has significantly consolidated since 2000 – when the top 5 publishers held 39% of the market of articles to 2022 where they control 61% of it“ (Crotty, 2023). Aktuell besitzen Springer Nature über 3.000<sup>2</sup>, Elsevier knapp 3.000<sup>3</sup> und Wiley über 2.000 Zeitschriften<sup>4</sup>. Das sind innerhalb der Big Five die drei dominierenden Player mit außergewöhnlichen Gewinnmargen: „Five for-profit publishing companies [...] dominate the market, generating more than 50 percent of revenues (over \$7 billion in 2022) with profit margins up to 38 percent – higher than big tech companies“ (Drake et al., o. J.). Trotzdem – auch als Reaktion

1 Teile der in diesem Text besprochenen Argumente erscheinen in längerer Form in Fadeeva (2026).

2 <https://www.springernature.com/gp/products/journals>. [zuletzt abgerufen am 07.11.2025]

3 <https://shop.elsevier.com/journals>. [zuletzt abgerufen am 07.11.2025]

4 <https://onlinelibrary.wiley.com/>. [zuletzt abgerufen am 07.11.2025]

auf die Open-Access-Bewegung – haben diese Konzerne ihr Geschäftsmodell seit geraumer Zeit von der Publikations- und Verlagstätigkeit wegbewegt. Sie präsentieren sich als „*global provider of information-based analytics*“<sup>5</sup> (RELX, der Mutterkonzern von Elsevier), als Anbieter von „*technology-enabled products, platforms and services*“<sup>6</sup> für Wissenschaftler:innen (Springer Nature) oder als „*a global company that provides digital education, learning, assessment and certification solutions for various sectors and subjects*“<sup>7</sup> (Wiley). Clarivate, ehemals Thompson Reuters, versteht sich als „*a leading global provider of transformative intelligence for academia, IP and healthcare*“<sup>8</sup> bzw. als Anbieter von „*analytics*“, ein Sammelbegriff für eine ganze Reihe von Tätigkeiten, die im weiteren Verlauf beschrieben werden. Clarivate besitzt selbst keine Zeitschriften, hat aber mit Web of Science die Kontrolle über den einflussreichen Journal Impact Factor und damit eine zentrale Rolle in der Wissenschaftsevaluation. Über den Ausbau ihrer Präsenz in der Wissenschaftsevaluation, dem Wissenschaftsmanagement und mit dem Aufkauf von Anwendungen im Wissenschaftszyklus (Chan, 2019) haben diese Big Player, allen voran Elsevier, ihren Einfluss in den letzten Jahren nochmals beträchtlich ausgedehnt.

Auf übergeordneter Ebene ist die Problematik um die Open-Access-Transformation und Science Tracking die Folge der Kommodifizierung der Wissenschaft mit neuen Technologien sowie ihrer Einbettung in das, was Eisenegger den dritten, digitalen Strukturwandel der Öffentlichkeit nennt (Eisenegger, 2021). Dabei geht es nicht (nur) um Digitalisierung, sondern um eine Plattformisierung, unter der Eisenegger einen „*gesellschaftliche[n] Bedeutungsaufstieg digitaler Tech-Plattformen (u. a. Google, Apple, Facebook) seit den 2010er Jahren*“ versteht sowie einen „*damit verbundene[n] Prozess des fortschreitenden Eindringens infrastruktureller und regelsetzender Plattform-Elemente in die Internet-Ökosysteme, was nicht nur die Medienöffentlichkeiten einem fundamentalen Transformationsprozess aussetzt, sondern die Gesellschaft insgesamt.*“ (Eisenegger, 2021, S. 17). Diese Diagnose lässt sich mühelos auf den Wissenschaftssektor übertragen – auch hier dominieren regelsetzende infrastrukturelle Elemente wie die obligatorische Nutzung der Plattformen für den Zugang zu Open-Access-Material oder das verpflichtende Anlegen persönlicher Accounts auf diesen Plattformen für die Publikationsabwicklung. Auch in der Wissenschaft erfolgt Tracking als Teil der Plattform- bzw. Anwendungsstrukturen und ist ein zentrales Element der Internet-Ökonomie, aus der die Wissenschaft eigentlich ausgeschlossen sein sollte.

## 2 Tracking als Teil der Webökonomie

Das massive und systematische Sammeln von Daten und Metadaten über Individuen oder Gruppen (mass surveillance) wird unter dem Begriff „Data-veillance“ (Clarke, 1988) zunehmend beforscht (Andrejevic & Gates, 2014; Bolin & Jerslev, 2018; Tau, 2024; Van Dijck, 2014), insbesondere hinsichtlich kommerzieller („surveillance capitalism“, „corporate dataveillance“, vgl. Fuchs, 2012; Zuboff, 2019) und staatlicher (Giroux, 2015; Lyon, 2015) Akteur:innen.

5 <https://www.relx.com>. [zuletzt abgerufen am 07.11.2025]

6 <https://www.springernature.com/gp/advancing-discovery>. [zuletzt abgerufen am 07.11.2025]

7 <https://www.wiley.com/en-us/?page=1>. [zuletzt abgerufen am 07.11.2025]

8 <https://ir.clarivate.com/>. [zuletzt abgerufen am 07.11.2025]

Im Folgenden möchte ich Prozesse, Methoden und Interessen aus diesem Bereich herausgreifen, die sich speziell auf Science Tracking beziehen. Das Phänomen Science Tracking und dessen Verbindung zur institutionellen Open-Access-Transformation lässt sich nur sinnvoll beschreiben, wenn zugleich weitere Zusammenhänge seiner wirtschaftlichen Einbettung in die AdTech-Industrie berücksichtigt werden. Dabei gelingt es nur teilweise, die Methoden der *Datensammlung* und die Formen der *Datenverwendung* zu unterscheiden, insbesondere weil diese Prozesse praktisch ineinander greifen. Zunächst zum zweiten Bestandteil des Terminus, also „tracking“ – einem Phänomen, das seit einigen Jahren in Bezug auf die Logiken des Webmarketing und die Praktiken der GAFAM<sup>9</sup>-Konzerne bekannt wurde. Binns (2022) definiert Tracking als „*the collection of data about an individual’s activity across multiple distinct contexts and the retention, use, or sharing of data derived from that activity outside the context in which it occurred.*“ Demnach beinhaltet Tracking folgende Merkmale:

- a) Datensammlung über die Aktivitäten einer Person (unabhängig davon, ob es sich um ausschließlich digitale Aktivitäten handelt),
- b) über mehrere, voneinander getrennte Kontexte hinweg,
- c) Handlungen mit diesen Daten in Form von Zurückbehalten, Gebrauch oder Teilen außerhalb des Kontextes der Datenentstehung.

Dieser Beschreibung möchte ich als d) ein weiteres Merkmal hinzufügen, nämlich die grundsätzliche Asymmetrie zwischen der aktiven trackenden Seite und der passiven getrackten Seite:

- d) die genannten Handlungen sind asymmetrisch, weil sie • für Personen im digitalen Raum einseitig *unausweichlich*<sup>10</sup>; • in ihrem Ausmaß, Zusammenhang und in Bezug auf aktuelle wie künftige Konsequenzen für Personen *nicht überblickbar* sind, insbesondere in Bezug auf die Machtposition der trackenden Seite gegenüber Personen als getrackter Seite.

Die technische Seite des Tracking umfasst unterschiedliche Ansätze, die hier nur sehr ausschnitthaft aufgegriffen werden. Die Tabelle 1 enthält in der Spalte „Trackingmethode“ die im Kontext dieses Beitrags besonders wichtigen, aber bei Weitem nicht die einzigen Methoden: IP-Targeting und Geofencing, Cookies in allen Varianten, Fingerprinting, Tracking-Pixel etc. Wichtiger als die Detailanalyse der sich schnell wandelnden Technologien des Tracking (dazu s. Acar et al., 2014; Binns, 2022; Christl & Toner, 2024; Hoofnagle et al., 2012; Lisker, 2023; Schneider et al., 2014) ist mir die Kontextualisierung innerhalb der global dominierenden Webökonomie. Die Verwendung von Tracking-Daten ist dabei längst über reine Werbezwecke hinaus gewachsen und umfasst Fragen der Sicherheit und digitalen Souveränität (Siems, 2024).

Das für die meisten mit Tracking assoziierte Instrument ist das Cookie, das durch die Umsetzung der europäischen Datenschutzrichtlinien als Cookie-Banner eher als störend wahrgenommen wird. Dabei handelt es sich, grob vereinfacht, um Wiedererkennung von Personen an ihren Geräten durch Code,

9 Ein Akronym für die führenden globalen Unternehmen Google, Amazon, Facebook (nun Meta), Apple und Microsoft.

10 Binns (2022); Fraunhofer-Institut für Sichere, 2020; Hoofnagle et al. (2012); Lamdan (2022); Lisker (2023); Schneider et al. (2014); Valentino-DeVries et al. (2018).

der beim Besuch von Websites auf diesen Geräten gespeichert wird. Alternativ bzw. komplettierend können andere Technologien die Funktion der Wiedererkennbarkeit erfüllen. Dazu gehört z.B. Fingerprinting, das nutzerseitige Anonymisierungsmaßnahmen umgeht. Dabei ist die Wiedererkennung der erste Schritt zu einer lückenlosen Verfolgung von Personen über verschiedene Websites und Endgeräte hinweg, während eine wachsende Datenmenge über ihr Verhalten, ihre Eigenschaften und Lebensumstände in umfangreichen Profilen gesammelt und in großen Datenbanken global gehandelt werden. Datenaggregierende Audience Tools stammen z.B. von Adobe, AddThis, Neustar, Oracle BlueKai. Zwar sind solche Profile im Regelfall pseudonymisiert und enthalten keine Klarnamen, sondern eine ID. Jedoch kann die tatsächliche Identität von Personen mit der ID verbunden werden. Diese Verknüpfung kann selbst Teil des Produkts auf dem Datenmarkt sein. Dies ist dadurch vereinfacht, dass Unternehmen wie LiveRamp nicht nur digitale Spuren (Nutzung von Social Media, Smart-TV und anderen Internet-of-Things-Anwendungen, Anwendungen aus dem Gesundheitssektor, unterschiedliche Ortungsdaten, Verfahren für bargeldlose Zahlungen) verarbeiten, sondern in einer ID auch über Jahre gesammelte analoge Informationen verbinden. Dabei sind Datenflüsse nicht einseitig, so dass die einzelnen Anwendungen und Plattformen nicht nur Daten an die Verknüpfungsdienstleister geben, sondern zugleich ihre eigenen Profildatenbestände ergänzen.

Dank der raschen Weiterentwicklung von Technologien für die Verarbeitung großer Datenmengen und Verfahren maschinellen Lernens können solche Datenbanken auch für extrem große Menschenmengen<sup>11</sup> betrieben, in beliebig viele Kategorien sortiert und für prädiktive Analytik genutzt werden (Reuter, 2024). LiveRamp z.B. verkauft Daten von 700 Millionen Verbraucher:innen, die das Unternehmen selbst erfasst sowie von rund 150 Lieferanten bezieht: „LiveRamp operates a massive identity surveillance system that assigns every person a proprietary identifier, which is tied to identifying attributes such as names, postal addresses, email addresses, phone numbers and digital IDs referring to browsers, smartphones and other devices.“ (Christl & Toner, 2024) Diese Prozesse sind natürlich nicht mit einer einmaligen Datensammlung abgeschlossen, sondern werden beständig mit aktuellen Daten gefüttert.

Bei prädiktiver Analytik werden mit statistischen Verfahren aus vorhandenen, also bereits gesammelten (personenbezogenen und nicht-personenbezogenen) Daten umfangreiche Schlüsse gezogen, und zwar in Bezug auf noch unbekannte und wirtschaftlich interessante, darunter höchst sensible Eigenschaften und Merkmale von Personen. Ein bekannt gewordenes Beispiel war die (versehentliche) Veröffentlichung eines Datensatzes des Data Broker Xandr. Keegan & Eastwood (2023) schlüsseln die nicht leicht lesbaren Angaben des Datensatzes auf, den Xandr zwar schnell wieder von der Website entfernte, der aber auf GitHub verfügbar ist. Darin finden sich weit mehr als nur Angaben zu Geschlecht, Altersgruppe oder Wohnort, sondern weitere sehr spezifische Kategorien, „audience segments“ (ebd.) genannt. Dazu gehören ethnische Zugehörigkeit, Krankheiten, Einkommen, geschützte Berufe und weitere

11 „AbiliTec and RampID systems maintain and constantly update comprehensive identity records about whole populations: the address where they live, the devices they use, and people they share a household with.“ (Christl & Toner, 2024)

vulnerable Gruppen unter „audience segments“ wie „Abortion“, „LGBTQ“, „Jewish“ oder „Addict“. Keegan und Eastwood sprechen von „650,000 Ways Advertisers Label You“, also von einer feingranulierten Sortierung nach sehr spezifischen Interessen des Datenhandelmarktes: „Political (Ex: US Politics > Issues & Advocacy > Allow Transgender Bathroom - Oppose‘)“; „Health (Ex: Healthcare > Medications > Depression Medications‘)“ (ebd.). Der Datensatz enthält z.B. die Kategorie „Law and Government“, die sich in so sensible Unterkategorien aufteilt wie „Courts & Judiciary“, „Embassies & Consulates“, „Executive Branch“ und „Intelligence & Counterterrorism“.<sup>12</sup>

Diese Weiterverwendung ist besonders asymmetrisch im obigen Verständnis: Die betroffenen Personen haben keine Möglichkeit, ihre Rolle in diesem Handel zu bestimmen, seine Ausmaße einzuschätzen oder Einfluss zu nehmen. In weiteren Schritten können weitere Data Broker und Verknüpfungsdienstleister ins Spiel kommen, deren Geschäftsmodell darin besteht, weltweit mit solchen Daten zu handeln. Eines der bekannteren Unternehmen ist das gerade erwähnte LiveRamp, ehemals Axciom, das schon lange im Datensammelbereich aktiv ist und ältere analoge Bestände mit digitalen Daten zu riesigen Mengen von RampIDs, Identitätsprofilen, verknüpft: *„LiveRamp’s identity graph systems can be considered private population registers, and their identity databases and proprietary identifiers facilitate the exchange of personal data across databases and companies. Many businesses in the digital marketing industry utilize LiveRamp’s identity surveillance technology to recognize, track, follow, profile and target people across the digital world and trade profile information about them. As of 2023, LiveRamp operates in many countries across the planet including the UK, France, Germany, Belgium, Spain, Italy, Poland and Romania.“* (Christl & Toner, 2024, Summary) LiveRamp arbeitet, wie auch andere, nach einer gegenseitigen Komplettierungsstrategie für Daten und beliefert andere Broker mit Daten, während deren Bestände für die Vervollständigung der eigenen Datenbank genutzt werden. Dieses Prinzip zeigt sich auf verschiedenen Ebenen, z.B. durch die Synchronisierung von Cookies, damit sich mehrere interessierte Drittanbieter austauschen können, oder durch die Ergänzung mehrerer Trackingmethoden innerhalb eines Unternehmens.

Eine lückenlose Verfolgung des (digitalen) Verhaltens, Targeting durch die Erstellung feingranulierter Profile, großflächiger Datenhandel und prädiktive Analytik gehören zu den Verwendungsformen des Tracking, die bereits Einzug in den geschützten Bereich der Wissenschaft gehalten haben. In diesem Zusammenhang muss auch das Real-Time Bidding (RTB) genannt werden, eine extrem lukrative Industrie mit mehr als 117 Milliarden US Dollar in den USA und Europa im Jahr 2021 (Ryan, 2022). Die Untersuchung von Ryan & Christl (o. J.) zeigt, in welchem Maße und welcher Breite der Prozess des Datenhandels automatisiert wurde. RTB ist *„active on almost all websites and apps“* (Ryan & Christl, o. J., S. 4) und findet permanent statt: *„RTB data about the average person are broadcast to many entities, hundreds of times a day. There is no way to limit or know what happens to RTB data after they are broadcast.“* (Ryan & Christl, o. J., S. 7).

<sup>12</sup> [https://raw.githubusercontent.com/the-markup/xandr-audience-segments/main/data\\_marketplace\\_public\\_segments\\_pricing\\_05212021.csv](https://raw.githubusercontent.com/the-markup/xandr-audience-segments/main/data_marketplace_public_segments_pricing_05212021.csv), [zuletzt abgerufen am 07.11.2025]

Der Mechanismus dahinter ist eine Echtzeit-Versteigerung von Werbeflächen auf Websites bzw. in Apps, die eine Person bei digitalen Aktivitäten öffnet bzw. nutzt. Die Abbildung 1 zeigt die Weitergabe der Daten während des Vorgangs: Ruft die Person eine Website auf, werden ihre Profildaten an eine „Supply Side Platform“ (SSP) gesendet (Step 1-2 in Abb. 1). Die SSP schickt diese Profildaten an (einen oder mehrere) „Ad Exchange“-Betreiber (Step 2) wie z.B. Google, Pubmatic, Magnitude, BidSwitch oder Microsoft (Xandr) (vgl. Bericht Ryan, 2022). Ein Ad Exchange schickt die Profildaten dann an eine unüberblickbar große Menge von „Demand Side Platforms“ (DSP). Microsoft Xandr spricht von mehr als 1600<sup>13</sup> Firmen und Google<sup>14</sup> von über 1000 Firmen in Europa<sup>15</sup> und über 4500 in den USA<sup>16</sup>, in Abbildung 1 durch die vielen kleinen DSP-Kästchen rechts und unten dargestellt. Diese DSP-Firmen bieten gegeneinander auf den freien Anzeigenplatz (Step 3). Obwohl nur eine DSP die Auktion gewinnt, erhalten alle die Profildaten. DSP sind üblicherweise Werbefirmen, jedoch weisen Christl und Ryan darauf hin, dass die Registrierung als DSP einfach ist und die Beteiligung von diversen Akteur:innen mit politischen Interessen als DSP zum Zweck der Datensammlung und Spionage naheliegt. Damit verbundene Gefahren sind nicht rein theoretisch, wie Ryan und Christl in ihren Ergebnissen betonen:

„Our investigation highlights a widespread trade in data about sensitive European personnel and leaders that exposes them to blackmail, hacking and compromise, and undermines the security of their organisations and institutions. [...] Foreign states and non-state actors can use RTB to spy on target individuals’ financial problems, mental state, and compromising intimate secrets. Even if target individuals use secure devices, data about them will still flow via RTB from personal devices, their friends, family, and compromising personal contacts. [...] Our examination of RTB data reveals Cambridge Analytica style psychological profiling of target individuals’ movements, financial problems, mental health problems and vulnerabilities, including if they are likely survivors of sexual abuse.“ (Ryan & Christl, o. J., S. 4).

Neben den im Wissenschaftsbereich aktiv genutzten Trackingmethoden kommen auch die beschriebenen Formen der Verwertung zum Einsatz, also RTB, Targeting durch Profilerstellung und prädiktive Analytik. Manche dieser Nutzungen sind einfacher nachzuweisen als andere, unter anderem weil die Involvierung der Data Broker intransparent und Tracking im oben genannten Sinne asymmetrisch ist. Ein Hauptproblem von Tracking bleibt, dass seitens der Nutzer:innen und sogar der IT-Forensik häufig nur Vermutungen möglich sind, was mit Daten geschieht, wenn sie einmal gesammelt sind. Was die verschiedenen Akteur:innen – Data Broker, Verknüpfungsdienstleister:innen,

13 [https://www.iccl.ie/wp-content/uploads/2022/01/K13-24032021-service\\_policies\\_3-24-2021.pdf](https://www.iccl.ie/wp-content/uploads/2022/01/K13-24032021-service_policies_3-24-2021.pdf) [zuletzt abgerufen am 07.11.2025]

14 European list is at „Ad technology providers“, Google (<https://support.google.com/admanager/answer/9012903><https://support.google.com/admanager/answer/9012903>)). [zuletzt abgerufen am 07.11.2025]

15 " U.S. list is at „Ad technology providers“, Google (<https://support.google.com/admanager/answer/9012903>). [zuletzt abgerufen am 07.11.2025]

16 "Ad Manager Certified External Vendors“, Google (<https://developers.google.com/third-party-ads/adx-vendors>). [zuletzt abgerufen am 07.11.2025]

## Very wide broadcasting of sensitive information

The sale of a single ad slot often involves an auction of auctions, with several ad exchanges running competing auctions that are coordinated by a Supply Side Platform (SSP). This increases the number of DSPs that receive the broadcasted data.

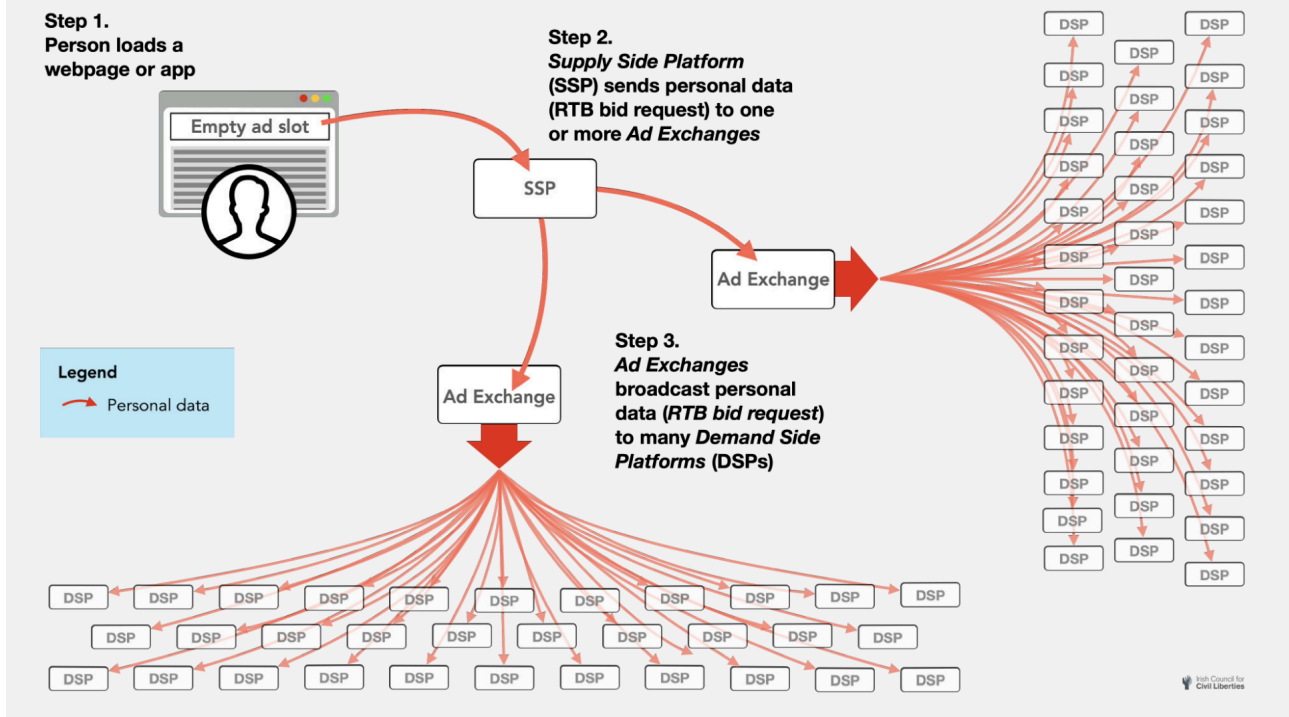


Abbildung 1: Broadcasting personenbezogener Daten durch RTB (Ryan & Christl, o. J., S. 5)

DNS, große Konzerne, die diese Rollen kombinieren und prädiktive Analytik betreiben – mit den Daten machen, ist nur ihnen bekannt. Über künftige Verwendungen können nicht einmal sie selbst Auskunft geben, das hängt von weiteren Entwicklungen im Bereich Big Data, den Bedarfen auf dem Datenhandelmarkt und nicht zuletzt vom Merging- und Aufkaufverhalten der Unternehmen ab.

Es ist wichtig festzuhalten, dass Tracking in weit größerem Maße stattfindet als allein mit dem Akzeptieren oder Ablehnen von Cookies. Zahlreiche weitere invasive Technologien werden komplettierend eingesetzt, sowohl innerhalb eines trackenden Unternehmens als auch durch Austausch zwischen solchen Unternehmen. Selbst für Personen, die großen Wert auf Anonymisierung legen, sind bestimmte Formen des Datenabflusses unausweichlich.

### 3 Von Tracking zu Science Tracking

Während das bisher skizzierte generelle Tracking als Methode der Datengewinnung sowie der Datenverwertung eine komplexe Verbindung zwischen Einzelpersonen und einer trackenden Seite beschreibt, werden die beiden Gruppen beim Science Tracking präzisiert. Unter „Science Tracking“ wird hier

die systematische und großflächige digitale Überwachung von Wissenschaft und Wissenschaftler:innen – getrackte Seite – durch im Wissenschaftsumfeld agierende Datenanalyse-Konzerne und mit ihnen assoziierte weitere Unternehmen – trackende Seite – verstanden. Eine manchmal anzutreffende Verwendung des Terminus als bibliometrische Erfassung und Analyse bzw. Auswertung von Wissenschaftsergebnissen mit digitalen Technologien zu (mehr oder weniger) wissenschaftsinternen Zwecken ist hier nicht gemeint. Eine Reihe in der Webökonomie genutzter Trackingverfahren wurde längst in den Wissenschafts- und Universitätsbetrieb implementiert. Im Fall von Elsevier/RELX kommt erschwerend hinzu, dass RELX mit der „risk“-Unternehmenssparte LexisNexis ein globales Schwergewicht in der Sicherheits- und Risikoindustrie ist. LexisNexis wendet extrem umfangreiche und weitreichende Identifikations- und Analyseverfahren mit quasi-nachrichtendienstlicher Funktion für Leistungen wie Risikomanagement, Betrugsprävention und -entdeckung an<sup>17</sup>. Die Existenz und das Ausmaß der Trackingverfahren werden von der trackenden Seite entweder explizit bestritten oder in verharmlosende Rhetorik<sup>18</sup> gekleidet, mit vagen Bezügen auf Produktverbesserung, Analytics<sup>19</sup>, ihre „legitimen Interessen“ oder die Interessen ihrer unbenannt bleibenden Partner:innenunternehmen sowie notwendige Maßnahmen zum Schutz vor Betrug<sup>20</sup>.

Diese Problematik ist zunächst durch Clifford Lynch, Cody Hanson, SPARC für den angelsächsischen Raum und anschließend im deutschsprachigen

17 Die Informationsbestände von LexisNexis umfassen nach eigenen Angaben Identitätsdatenbanken mit digitalen Identifiern in Milliardenhöhe, die nicht nur „nearly 100% of the U.S.“ abdecken, sondern auch ein “[c]lear understanding of identities across systems, agencies, and states” (LexisNexis, 2023, S. 6) ermöglichen. LexisNexis kooperiert mit US-Behörden im Sicherheitsbereich, hier sind u. a. die Informationsweitergaben an die ICE bekannt geworden, die zur Deportation von illegalen Migrant:innen in den USA führten (Biddle, 2021). Unter dem damaligen Namen Reed Elsevier investierte der Konzern zudem neben der CIA in Peter Thiels Palantir, das gerade wieder in Bezug auf den Einsatz in Deutschland diskutiert wird. (<https://www.nytimes.com/2021/09/21/books/review/the-contrarian-peter-thiel-max-chafkin.html>) [zuletzt geprüft am 06.11.2025], <https://www.heise.de/hintergrund/Missing-Link-Machtzentrale-Palantir-eine-Software-lenkt-Organisationen-10463034.html>] [zuletzt geprüft am 06.11.2025]) Zu weitergehenden Verwicklungen zwischen Sicherheitsindustrie, predictive policing und Wissenschaftsinfrastrukturen siehe (Siems, 2025).

18 Es gibt spezielle Elsevier Privacy Principles: „**Value:** We carefully use personal data to help us support customers and individual users through customization/personalization options in our products to inform product development, monitor the performance our systems, ensure data security, and to comply with our legal and contractual obligations. **Transparency:** We tell users about the personal information we collect, including how and why we will use and share it. **Choice:** Users are given choice over the collection, use and sharing of their personal information. **Anonymization:** We depersonalize and aggregate personal information where individual identification is not necessary. **Accountability:** We are committed to acting as a responsible steward of personal information. <https://www.elsevier.com/about/policies-and-standards/privacy-principles> [abgerufen am 06.06.2025]

19 Die Rede von „Analytics“ verschleiern die Tatsache, dass auch ursprünglich nicht für Tracking entwickelte und eingesetzte Technologien zu Trackingzwecken genutzt werden: „*For instance, a third-party analytics service might initially be used in a way that only combines user data within a session, or within a single website. The analytics provider's code might set a cookie via the first-party's domain. But at some point, the analytics code might be updated to enable multi-domain tracking — either by owner of the first-party domain linking together behaviour from multiple different websites, or by the third-party looking to build user profiles themselves. Google Analytics, the most popular web analytics service, gives website operators the option of linking together user behaviour across multiple domains they own. At any point, website operators could use this to track users across their sites, and Google Analytics itself can also do the same thing, across all the websites who embed their analytics code (estimated around 56% of websites as of 2021[.]). As such, web users may find that their web browsing activities are being tracked via Google Analytics and incorporated into a profile about them, potentially even if they have never had an actual Google account, and even if they don't use Chrome (Google's web browser).*“ (Binns, 2022, S. 10f. Herv. YF)

20 Elseviers Cookie-Notice sagt: „*Einige unserer Websites, Anwendungen und elektronischen Mitteilungen enthalten elektronische Kennzeichnungen, die als Zählpixel, Gifs oder Pixel-Tag bekannt sind, eindeutige Identifikatoren und ähnliche Technologien, die dabei helfen, Cookies zu liefern, die Online-Aktivität zu messen, zielgerichtete Werbeanzeigen bereitzustellen oder die Effektivität unserer Werbekampagnen oder anderer Vorgänge zu analysieren. Zuletzt aktualisiert: 7. Dezember 2021*“ <https://www.elsevier.com/legal/cookie-notice-de-de> am 01.07.2024, Herv. YF. “

akademischen Diskurs durch das Papier des Ausschusses für wissenschaftliche Bibliotheken und Informationssysteme der Deutschen Forschungsgemeinschaft 2021 und Beiträge von Björn Brembs, Gerhard Lauer und Renke Siems bekannter geworden. Auch hier bestehen trotz Einsatzes der IT-Forensik prinzipielle Schwierigkeiten, Aussagen über eine Praxis zu machen, die der getrackten Seite nur sehr unsystematisch und asymmetrisch zugänglich ist. Auch wenn konkrete Technologien flüchtig sind, da sie trackerseitig schnell geändert werden können und Nachweise den Status von Momentaufnahmen haben, ist klar, dass verschiedene Trackingformen angewendet werden (DFG AWBI, 2021; Dittmann et al., 2023; Freiberg, 2022; Hanson, 2019; Lynch, 2017; Siems, 2021, 2022). Dabei werden häufig Technologien eingesetzt, die sich rechtlich bestenfalls im Graubereich befinden und höchstwahrscheinlich weder öffentlich noch juristisch legitimiert werden könnten. Tabelle 1 zeigt einige in der Debatte genannte Methoden, ergänzt durch Beschreibungen, Beispiele und Anwendungen sowie mögliche Konsequenzen für den Wissenschaftssektor.

**Tabelle 1:** Übersicht Tracking- und Überwachungsmethoden in der Wissenschaft<sup>21</sup>

Trackingmethode	Beschreibung	Formen, Beispiele	Anwendung	Konsequenzen
<b>Geofencing + IP-Targeting</b>	Ineinergreifende Verfahren der Lokalisierung von Geräten bzw. Personen durch das Hochschulnetz und darin durch mobile Geräte <sup>22</sup>	Geofencing kann zum Tracken von mobilen Geräten verwendet werden, durch GPS, Bluetooth, WLAN und auch Radiowellen (Bashyakarla, o. J., S. 57), IP-Targeting betrifft auch physische Adressen	Lokalisierung von Institutionen und Personen, Überwachung	„gezielte, standortbezogene Übermittlung von Inhalten über die IP-Adresse [...] kann nicht nur bestimmte Geräte, sondern auch hinter den IP-Adressen stehende Haushalte, Betriebe, Institutionen und deren Subnetze wie auch Fachbereiche und Bibliotheken adressieren.“ (Freiberg, 2022, S. 98)
<b>Authentifizierungsform</b>	Anbieter stipulieren die Nutzung bestimmter Authentifizierungsmethoden, die eine anonymisierte Nutzung ihrer Angebote, z.B. nur durch die Authentifizierung als Institutionsmitglied, verunmöglichen <sup>23</sup>	Domainübergreifende Authentifizierungsverfahren: Single-Sign-On, RA21 zu SeamlessAccess.org zu GetFTR	Kontrolle über Nutzer:innen von Bibliotheksdiensten bzw. Hochschulnetzen	Online-Verhalten von eingeloggten Nutzenden wird beobachtet, sie werden auf Verlagsplattformen umgeleitet; „The architecture of GetFTR is designed to take place behind the scenes, with no ability for libraries or other users to opt out“ (SPARC, 2021, S. 8)
<b>Port Scanning</b>	Identifikation durch Ausnutzung von Sicherheitslücken in Browsern/Servern	Suche nach Schwachstellen in Endgeräten oder Netzwerken	Form der Individuierung, Hacking	„Schon die Suche nach offenen Ports auf fremden Rechnern und/oder Netzwerken [...] ist nach deutschem Verständnis am Rand der Legalität, da sie als Vorstufe von entsprechend sanktionierten Tatbeständen (§§ 202c, 303b StGB) gewertet werden kann.“ (DFG AWBI, 2021, S. 11)
<b>Device/Browser- &amp; Personen-Fingerprinting</b>	Individuierung von Geräten sowie geräteübergreifend von Personen über die Erstellung von Profilen ihrer Geräte bzw. biometrischer Merkmale der Gerätebedienung	Double Click, BehavioSec	Identifizierung von Personen durch behavioral-biometrische Profilbildung	Erfassung auch derjenigen, die Maßnahmen gegen Tracking ergreifen bzw. durch institutionelle Sicherheitsmaßnahmen geschützt sind; geräteübergreifende Profilbildung
<b>History-Sniffing</b>	Zugriff auf die Verbindungshistorie im Browser, um das Surfverhalten zu verfolgen (SPARC, 2023, Appendix C-3 und C-4)	über JavaScript	Spionage und Überwachung	„Der Javascript-Code der Third Parties [...] kann [...] auslesen, mit welchem Text der Nutzer sich beschäftigt, zu welchem er als nächstes weiterbrowsst und welche Suchworte er auf der Plattform eingibt.“ (DFG AWBI, 2021, S. 10)
<b>Cookies</b>	Code auf Geräten der Endnutzer:innen, der von first und third party gesetzt wird. Reich von einfacher Analyse bis zu sitzungübergreifender Verfolgung und praktisch nicht entfernbaren Versionen	first / third party cookie, evercookie (QuantCast, KISSmetrics)	Erstellung und Verwertung von Profilen, Analytics als Überwachung von Aktivitäten	Profilerstellung, cross-site-tracking Überwachung digitaler und analoger Aktivitäten
<b>Tracking-Pixel (alternative Bezeichnungen: Zählpixel / Web-Bugs, Web-Beacons, Web-Wanzen)</b>	Elemente, (ähnlich wie Cookies) durch third parties auf Websites platziert, um verschiedene Informationen über das Endgerät zu übermitteln, z.B. IP-Adresse, Betriebssystem, Browser-Konfigurationen. In E-Mails platziert informieren sie third parties darüber, ob eine E-Mail geöffnet wurde	Transparente Ein-Pixel-Bilder, für das Auge unsichtbar, Elsevier cookie notice	Eindeutige Individuierung, Analytics als Überwachung von Aktivitäten, Profilerstellung	Übermitteln an Drittparteien (Google, Adobe, Cloudflare, New Relic) Daten, die zur Identifizierung von Personen führen können (vgl. SPARC, 2023, S. 24); „Der einzige Zweck von Zählpixeln besteht darin, dass der Browser des Nutzers Kontakt mit dem Tracker aufnimmt.“ (Schneider et al., 2014, S. 41)

21 Diese Tabelle ist zum Teil aus Fadeeva (2026) entnommen.

22 „Die Zuordnung lässt sich über mobile Geräte noch verfeinern, da sie von Mobilfunk- und WLAN-Netznoten, RFID-Antennen und je nach Geräteeinstellungen über GPS-Daten registriert werden können.“ (Freiberg, 2022, S. 98)

Diese Übersicht zeigt, dass Wissenschaftler:innen und Studierende bei ihrer Arbeit der kontinuierlichen Beobachtung und Datensammlung ausgesetzt sind. Je nach Kombination der genutzten Anwendungen innerhalb des Forschungszyklus ergibt das ein vollständiges Bild wissenschaftlicher Aktivität: An welchen Themen arbeiten die Personen, welche Programme nutzen sie, welche Artikel laden sie herunter und welche bookmarken sie, was lesen sie wie lange und welche Recherchefragen geben sie in welche Datenbank ein? Wen zitieren sie und wie sieht ihr konkreter Schreibprozess aus? Mit wem kooperieren sie und welche anderen Wissenschaftler:innen oder Institutionen haben sie in welchem Zusammenhang gesucht? Welche Forschungsdaten haben sie geteilt? Nutzen sie ein Labormanagement-Programm?

Auf der Ebene der Forschungsinformations-Anwendungen steigt die epistemische Asymmetrie weiter an. Wenn Fakultäten oder Universitätsleitungen Programme im Bereich Current Research Information System (CRIS) – wie Pure von Elsevier – und Faculty Information System (FIS) – wie Interfolio von Elsevier (s. dazu SPARC, 2022) – verwenden, geben sie einerseits Einblick in ihre Strukturen, Strategien und Interessen. Andererseits werden sie in ihren Entscheidungsprozessen durch intransparente Algorithmen von Medienkonzernen geleitet, in deren Interesse es liegt, eigene Produkte, Publikationsorgane, Plattformen, Messinstrumente und Vertragsbedingungen durchzusetzen. Ein Kernelement ist dabei die Tätigkeit der Konzerne als Datenbroker und eine asymmetrische Kontrolle über Daten. Die Einflussnahme auf wissenschaftsinterne und institutionelle Prozesse ist durch die Machtposition des jeweiligen Konzerns naheliegend, der sich die Rolle innerhalb der verschiedenen Ebenen der Wissenschaftseinrichtungen sichert. Hier könnte eingewendet werden, dass Wissenschaftler:innen die Datenbanken, Forschungstools und Zeitschriften der Konzerne als Publikationsorgane – ob im Open Access oder Subskriptionsmodell – nutzen wollen und Wissenschaftsinstitutionen aus eigenem Bestreben die Services rund um das Forschungsmanagement lizenzieren. Aber dieser Einwand würde an der Komplexität der verschiedenen Systemzwänge vorbeigehen, innerhalb derer sich Wissenschaftler:innen einerseits und Institutionen andererseits befinden. Sowohl die bibliometrisch bestimmten Reputationsmechanismen, denen Wissenschaftler:innen unterworfen sind als auch die kompetitiven und ökonomischen Bedingungen, unter welchen Wissenschaftsinstitutionen agieren, stehen im mehrschichtigen Abhängigkeitsverhältnis (der genannten Datenbanken, Publikationsorgane, Plattformen, Messinstrumente, Rankings etc.) von den Big Five und Clarivate (Chen & Chan, 2021; Holzer, 2022; Münch, 2007; Retzlaff, 2022)<sup>24</sup>.

Damit ist die Problematik des Science Tracking aber noch nicht erfasst, was paradigmatisch an Elsevier/RELX zu sehen ist. Die spezifisch akademischen

23 „[T]hey want to replace the authentication options previously supported by libraries and academic institutions, such as IP range activation, VPN, proxy servers, or anonymous authentication to neutral third parties, as with the Shibboleth service, in favor of their own initiatives (wie 'Research Access 21 (RA21)', 'Seamless Access', or 'Get Full Text Research (GetFTR)')" (Siems, 2021).

24 Hierzu SPARC: „University rankings, journal impact factors, performance-based funding for universities – these have all affected the culture of academic institutions for years and have progressively led to an erosion of control by academic institutions over their own destiny. Data analytics services have a market and are in demand – in spite of all the issues they pose – because academic life has become a race to secure funding. As a result, research assessment is becoming a business opportunity, and one that commercial vendors appear eager to control, regardless of their possible conflicts of interest.“ (SPARC, o. J.-a, S. 29)

Datenabflüsse und damit verbundene Gefahren werden ergänzt durch die bereits genannten Beobachtungs- und Auswertungsergebnisse. Es gibt also nicht nur Tracking einer Person *als Wissenschaftlerin*, sondern unabhängig davon auch Tracking, dem sie *als Privatperson* ausgesetzt ist. Sensible Informationen aus ihrem Privatleben, ihre Einkaufsvorlieben, ihr Wohnort oder Angaben zu ihrem Haushalt, ihrer Familie, ihren Streaming-Diensten, ihren Gesundheitsdaten oder ihr Verhalten auf Social Media – all dies ist durch Profilbildung, Targeting und prädiktive Analytik ein Ziel für Tracking. Beide Bereiche werden im Datenbrokering zusammengeführt, so dass Elsevier einerseits eine große Menge wissenschaftsspezifischer Informationen zusammenführen kann (siehe Tabelle 2) und andererseits Profildaten aus möglichst breiten Quellen bezieht. Darunter nennt Elsevier in der eigenen Privacy Policy „*data suppliers*“, „*third parties*“, „*other entities within RELX*“ (wozu die oben erwähnte LexisNexis-Abteilung gehört) und sehr vage bleibende „*[p]artners with which we offer co-branded services or engage in joint marketing activities*“. Zu den automatisch gesammelten Daten gehören „*Computer, device and connection information, such as IP address, browser type and version, operating system and other software installed on your device, unique device identifiers and other technical identifiers, error reports and performance data; Usage data, such as the features you used, the settings you selected, URL click stream data, including date and time stamp and referring and exit pages, and pages you visited on the Service; [...] For location-aware Services, the physical location of your device.*“<sup>25</sup>

Die Frage, weshalb diese Informationen überhaupt von Elsevier/RELX erhoben werden sollten, muss hier ausgeklammert werden, denn es geht mir um einen anderen Punkt: Es handelt sich nicht allein um die Tracking-Aktivitäten während der Nutzung *einer* Plattform und dabei nicht ausschließlich um Cookies. Die Konzentration auf die jeweilige Website bzw. Plattform und Cookies verdecken jedoch das Ausmaß der Datensammlung und der möglichen Anwendungen (s. Tabelle 2). Elsevier nutzt laut eigener Aussage viele verschiedene Quellen außerhalb des unmittelbaren Kontextes seiner „Services“, z.B. auch LexisNexis. Der Konzern sammelt und teilt Daten über Personen, Forschungsdaten und Daten aus seinen einzelnen, teilweise integrierten Anwendungen – z.B. Forschungsinformationsservices und Wissenschaftsmanagement (Pure, SciVal, Plum X, Analytical Services), Personalmanagement (Interfolio) und natürlich Forschungsanwendungen (Scopus, Mendeley) im engeren Sinne und der Publikationssparte – sowie über Wissenschaftsinstitutionen. Je mehr solcher Anwendungen eine Wissenschaftsinstitution nutzt, umso mehr epistemische Kontrolle gibt sie preis, umso mehr Einflussmöglichkeiten bietet sie für einen global agierenden Datenkonzern wie RELX und umso weiter entfernt sie sich von digitaler Souveränität. Datensammlung, Brokering und aktuelle wie potenzielle künftige Verwertung bilden den Kern dieses Geschäftsmodells: “[W]e have every reason to believe, based on existing data products alone, that publishers are skimming scholars’ behavioral residue on *the prospect of monetization to come.*“ (Pooley, 2022, S. 42, Herv. YF).

Oben wird Tracking als ubiquitäres Phänomen beschrieben, was in der einen oder anderen Form oder Detailtiefe eine verbreitete Information ist. Auch die Verharmlosung und das Abstreiten von Tracking sind aus dem AdTech-Bereich,

<sup>25</sup> <https://www.elsevier.com/legal/privacy-policy>, [abgerufen am 01.07.2024].

**Tabelle 2:** RELX-Informationsbestand Elsevier (STM)<sup>26</sup>

RELX-Marktsegment	Personenbezogene Daten	Wissenschaftliche Daten, Forschungsdaten	Wissenschaftsmanagement, Institutionen	Anwendungsmöglichkeiten für RELX, Konsequenzen
Science, Technical & Medical, Elsevier <sup>27</sup>	First-Party-Daten: Wissenschaftler:innen, Studierende, Angehörige von Wissenschaftseinrichtungen, Bibliotheken, ScienceDirect, Scopus, Mendeley, Expert Lookup <sup>28</sup> , Pure	Elsevier-Anwendungen: Scopus, Pure, Mendeley, DataSearch, Journal Metrics, Plum X, SSRN, Cell Press, Expert Lookup, Data Monitor, Digital Commons	Elsevier-Anwendungen: SciVal, Pure, Interfolio, Funding Institutional, Analytical Services	Beeinflussung von Forschung und Wissenschaftskommunikation; Epistemische Überlegenheit durch Steuerungswissen und Trackingwissen; Vernetzung der verschiedenen Sparten („risk“-Produkte); asymmetrischer Vorteil gegenüber Institutionen; Etablierung von Brokering als Teil des Wissenschaftszyklus

den Skandalen rund um den Datenschutz der GAFAM-Konzerne und die Nutzung von Social Media bekannt. Weshalb ist der Einsatz dieser Techniken anders zu bewerten, wenn es um Wissenschaft geht? Es gibt darauf einige direkte Antworten. Neben dem Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG), das bereits durch Tracking als solches gefährdet wird, betrifft Science Tracking unmittelbar den besonderen rechtlichen Status der Wissenschaft: Art. 5 Abs. 3 des Grundgesetzes schützt die Wissenschaftsfreiheit: „Kunst und Wissenschaft, Forschung und Lehre sind frei“ sowie auch die Charta der Grundrechte der Europäischen Union Art. 13: „Kunst und Forschung sind frei. Die akademische Freiheit wird geachtet.“ Das ist eine Antwort.

Egal, wie die Legitimierung der Tracking-Praktiken in der Webökonomie beurteilt wird, besteht zudem ein grundsätzlicher Unterschied zwischen der Nutzung von Instagram, TikTok und Shopping-Websites und dem Zugriff auf Quellen und Programme im Arbeitskontext einer wissenschaftlichen Institution. Das Erste verwenden Nutzende freiwillig und zahlen nicht in Form von Lizenzgebühren oder anderen Kosten, sondern mit ihren Daten – mittlerweile ein durchaus bekannter Sachverhalt. Das Zweite wird aus öffentlicher Hand mit extrem hoch bepreisten Gebühren bezahlt<sup>29</sup> und ist ein vermeintlich notwendiges Mittel für Forschung und Lehre. Es ist also weder im relevanten Sinne freiwillig noch lässt sich rechtfertigen, weshalb ein außergewöhnlich hoch bezahltes Produkt gleichermaßen invasive Trackingverfahren nutzt wie durch AdTech-Industrie finanzierte Dienste. Das ist eine zweite Antwort.

Ein wichtiger weiterer Punkt besteht darin, dass solche Praktiken das Vertrauen der Wissenschaftler:innen und Studierenden in ihre Institution, Bibliotheken und die Integrität der Wissenschaft gefährden. Bibliotheken sind hohen arbeits-

26 Abbildung stammt aus Fadeeva (2026).

27 Ohne die Sparten Government, Corporate und Health Organisations.

28 Ab 2024 wird Expert Lookup nicht fortgeführt bzw. ist in die bestehenden Scopus-Anwendungen integriert.

29 Die Kosten der DEAL-Verträge sind transparent, was ein Verdienst der nationalen Verhandlung ist und die übliche Geheimhaltungspraxis der Verlage/Konzerne aufbricht. Transparenz ist eine zentrale Forderung der Open-Access-Bewegung. So ist die offene Diskussion einer für alle Wissenschaftseinrichtungen geltenden Konsequenz möglich, dass nämlich die Kosten für DEAL die Budgets selbst großer Bibliotheken erschöpfen. Darunter leiden nicht nur andere Erwerbungsmöglichkeiten, sondern auch die Möglichkeit, in alternative Publikationsstrukturen zu investieren. Für Wissenschaftler:innen bedeutet das weiteren Druck, in den Zeitschriften der DEAL-Konzerne (und damit des Oligopols) zu publizieren, weil sie so Open-Access-Vorgaben erfüllen.

ethischen Anforderungen<sup>30</sup> an den Schutz ihrer Nutzenden verpflichtet und diese werden von Bibliothekar:innen und bibliothekarischen Verbänden sehr ernst genommen: „*The privacy of library users is and must be inviolable.*“ Diesem Statement der American Library Association schließt sich auch der Deutsche Bibliothekerverband (dvb)<sup>31</sup> an. Bibliotheken können Informationen über Nutzer:innen erst nach Vorlage eines richterlichen Beschlusses herausgeben. Bei den von Bibliotheken bereitgestellten digitalen Services sieht die Situation jedoch anders aus, aber das ist nicht allen klar. Nutzende wähen sich unter dem Schutz ihrer Institution und halten die Nutzung von Angeboten, die z.B. durch die Universitätsbibliothek lizenziert werden oder die für ihre Arbeit und das Studium unverzichtbar sind, für vertrauenswürdig und datenschutzrechtlich sicher. Studierende würden zurecht empört sein, wenn sie in den Räumen der Bibliothek bei ihren Aktivitäten beobachtet oder gefilmt werden würden, genaue Fragen zu ihrem Leben und Verhalten beantworten müssten oder ihre Geräte und Arbeitsunterlagen durchsucht würden. Die Realität der Nutzung von Plattformen wie ScienceDirect, Wiley oder SpringerLink (Freiberg, 2022) ist aber diesem Szenario näher als vermutet.

Dorothea Salo nutzt den Begriff der „physical-equivalent privacy“ (Salo, 2021), um die Diskrepanz zwischen dem gewohnten Schutz der Bibliotheken für ihre Nutzer:innen und der Realität digitaler Angebote aufzuzeigen. Physical-equivalent privacy hat eine E-Ressource, wie Salo sie nennt, nur dann, wenn Nutzende bei der Verwendung einer informationsgleichen analogen Ressource („an information-equivalent physical resource“) nicht mehr Privatsphäre bzw. Schutz der Einrichtung („privacy“) genießen würden als mit der digitalen Ressource (ebd.). Die so einfach scheinende Anforderung ist nicht leicht zu erfüllen und beschreibt die Situation der Bibliotheken, die gewünschte Service bereitstellen müssen. Aber die Datenschutzbedingungen dieser Services widersprechen in einigen Fällen dem Schutzauftrag der Bibliotheken:

„Any patron whose device has a static campus IP address is immediately reidentifiable, as is any patron using a device whose identifier is known to the vendor [...]. Log analysis, web tracking, and behavioral tracking provide additional avenues to reidentification. The documentation for this category states that ‚a Service Provider [vendor] claims that it will not use attributes for purposes that fall outside of the service definition as presented at the time of registration to its users and referred to in metadata.‘ This still allows vendors to sign patrons up to privacy-destroying services by disclosing further attribute use during registration for the service, in the typical and heavily-discredited notice-and-consent dark pattern wearily familiar to scholars of internet privacy and law“ (Salo, 2021).

In Bezug auf das obige Szenario von Studierenden, die in der Bibliothek beobachtet, gefilmt oder deren Geräte inspiziert werden würden, ist Salos

30 Die 30seitige DSGVO-Handreichung für Bibliotheken (Brehm et al., 2018) beinhaltet genaue Erläuterungen zu bibliotheksrelevanten Fragen wie informierte Einwilligung, Auskunftsrecht, Informationspflichten, Auftragsverarbeitung.

31 S. z.B. die Stellungnahme des dvb zum Umgang mit sensiblen Daten von Nutzenden in [https://www.bibliothekerverband.de/sites/default/files/2020-12/2013\\_11\\_13\\_dvb\\_Stellungnahme\\_Bibliotheken\\_im\\_Spannungsfeld.pdf](https://www.bibliothekerverband.de/sites/default/files/2020-12/2013_11_13_dvb_Stellungnahme_Bibliotheken_im_Spannungsfeld.pdf) [zuletzt abgerufen am 07.11.2025]

Position eindeutig: Was in analoger Weise in den Bibliotheksräumen nicht erlaubt wäre, darf auch online nicht stattfinden. Dabei sieht sie die Zuständigkeit auch bei Bibliotheken: *„Merely moving such surveillance and surveillance-fueled manipulation online cannot excuse it, yet many librarians have allowed, facilitated, encouraged, and even performed commercial surveillance on library patrons largely without challenge.“* (Salo, 2021) Auch wenn die Rolle von Bibliotheken in Bezug auf Science Tracking ambivalent ist, tragen sie sicherlich keine alleinige Verantwortung für die aktuellen Tracking-Praktiken. Diese Verantwortung liegt bei der trackenden Seite. Bibliotheken gehören zu den Akteurinnen der digitalen Transformation der Publikationspraxis, deren Rolle und Auftrag sich stark wandeln. Sie treiben die Entwicklung einer unabhängigen digitalen Infrastruktur voran und übernehmen Publikationsdienste. Eine stärkere Positionierung gegenüber Science Tracking wäre wünschenswert, nicht nur, um den negativen Effekten in Bezug auf das Vertrauen der Nutzenden entgegenzuwirken.<sup>32</sup>

#### 4 Auswirkung auf Wissenschaftler:innen

Nach der bisherigen Charakterisierung ist Science Tracking in seinen Methoden und Zielen invasiv, durchdringend und umfassend. Für Wissenschaftler:innen (und in bestimmten Hinsichten auch Studierende) ist Getracktwerden in der einen oder anderen Form unausweichlich, gleichzeitig ist es grundsätzlich asymmetrisch und nicht kontrollierbar. Die Gefahren für Wissenschaftler:innen, die an politisch heiklen oder gefährlichen Themen arbeiten und sich dem Verlust der professionellen Anonymität als Forschende ausgesetzt sehen, sind schwerwiegend. Im Zusammenhang mit Science Tracking werden Fälle genannt, bei denen Wissenschaftler:innen die Visa für Länder verweigert wurden, zu deren Politik sie sich innerhalb ihrer Arbeit kritisch äußerten, z.B. China. *„[T]he Chinese government has already induced certain scientific publishers to block access to specialist articles in China for users whose topics are a thorn in the side of the regime. China has also imposed sanctions on individual scientists and research institutes who are working in these research fields. If science companies sell personal data to governments – about who is reading and downloading which specialist articles – further researchers can become the target for sanctions.“* (Reda, 2022) Im Zusammenhang mit solchen Gefahren werden oft Selbstzensur und ein „chilling effect“ auf die jeweilige Forschung befürchtet. Diese mehr oder weniger direkten negativen Effekte sind bekannt. An dieser Stelle möchte ich eine Auswirkung auf Wissenschaftler:innen diskutieren, wenn diese mehr Einsicht in die Formen von Science Tracking erlangen.

Science Tracking beschränkt sich nicht allein auf konkrete wissenschaftliche Ergebnisse oder Gegenstände (wie z.B. bei Wirtschaftsspionage). Durch derart umfassendes, asymmetrisches und unausweichliches Tracking ergibt sich eine subtilere, aber nicht weniger schädigende Wirkung für die Wissenschaft als gesellschaftliche Institution. Diese Schädigung entsteht infolge des Wissens darum, als Privatperson *und* als Wissenschaftlerin konstant und systematisch exponiert und vulnerabel zu sein, überwacht zu werden, ohne kontrollieren zu können, was mit Informationen über das eigene Leben und Verhalten geschieht.

<sup>32</sup> S. Roßnagel (2022) zur Aufgabe der Bibliotheken im Umgang mit Science Tracking.

Eine Wissenschaftlerin kann dieses Wissen subjektiv als mehr oder weniger belastend erleben. Trotzdem befindet sie sich in der Position epistemischer Auslieferung, wenn sie bei ihrer Arbeit nicht mehr vom Schutz ihrer Privatheit als Person ausgehen kann. Warum ist das wichtig? Wissenschaftliches Arbeiten hat häufig ein hohes Maß an Eigenverantwortung, Kreativität und Freiheit – in der Auswahl von Themen, Herangehensweisen und Lösungsversuchen, im Stellenwert der eigenen Fachmeinung. Wissenschaftler:innen folgen strengen methodischen und wissenschaftsethischen Ansprüchen, handeln aber oft nach eigenem fachlichen Ermessen und eigener Verantwortung. Die wechselseitige Unterstellung der wissenschaftlichen Integrität ist – bis zur gegenseitigen Vermutung – die Voraussetzung für wissenschaftliche Arbeit. Gerade durch dieses hohe Maß an Autonomie ist die Trennung zwischen Privatperson und Wissenschaftlerin in einer bestimmten Hinsicht fließend. Die trackingbedingte Einflussnahme auf sie als Person könnte die Wissenschaftlerin *direkt* bei ihrer Arbeit behindern. Zudem könnte jedoch *indirekt* auch ihre wissenschaftliche Integrität kompromittiert werden. Wer sich als Person exponiert, vulnerabel oder überwacht fühlt, ist nicht mehr in der gleichen Situation, frei forschen zu können. Wer Wissenschaftler:innen als exponierte, vulnerabel oder überwachte Personen annimmt, begünstigt damit *prima facie* Zweifel an ihrer wissenschaftlichen Integrität. Für dieses Verständnis der Wissenschaftlerin als Person ist Autonomie an Privatheit (als Gegenteil von Exponiertheit und Überwachtwerden) gebunden und beides Voraussetzung für unabhängige Wissenschaft. Was heißt das konkret in Bezug auf Privatheit und Science Tracking?

Rössler (2005, S. 9) identifiziert drei Dimensionen von Privatheit: i) „decisional privacy“, den Bereich von Handlungen und Entscheidungen einer Person, ii) „informational privacy“, die Grenzen des Wissens anderer über diese Person und iii) „local privacy“, das private Zuhause, der eigene Rückzugsraum. Science Tracking beinhaltet genau solche Praktiken, die systematisch Privatheit und Autonomie zerstören: Kontinuierliche und unausweichliche Beobachtung, Profilierung, Bewertung durch intransparente, unerreichbare Dritte mit diversen Interessen und Motivationen. Eine Funktion des Tracking besteht darin, (iii) den persönlichen Rückzugsraum und (ii) die Grenzen des Wissens (informational privacy) anderer über eine Person aufzuheben und durch das Wissen der Person um diesen Eingriff ihr Verhalten zu beeinflussen. Als Person wird die Wissenschaftlerin durch den Verlust von diesen beiden Dimensionen erpressbar, so dass ihre (i) decisional privacy im Arbeitsbereich gefährdet wird. Abbildung 2 zeigt einen Ausschnitt des Analyse tools zum Privatheitsbegriff von Mulligan et al. (2016) (linke und mittlere Spalte) in meiner Anwendung auf die Wissenschaft (rechte Spalte). In der linken Spalte (Privatheitsdimension) und mittleren Spalte (Frage) werden grundsätzliche Fragen zum Privatheitsbegriff präzisiert. In Anwendung auf die Wissenschaft erhält Privatheit folgende Lesart: Privatheit ist wichtig für die wissenschaftliche Arbeit und persönliche Sicherheit sowie für die Selbstbestimmung. Im Wissenschaftsbereich wird Privatheit durch die gesetzliche Wissenschaftsfreiheit als Abwehrrecht gegen den Staat begründet sowie als Persönlichkeitsrecht (Recht auf informationelle Selbstbestimmung). Als Gegenkonzept zu Privatheit können Arbeitsbedingungen gekennzeichnet werden, in denen sich Wissenschaftler:innen als gefährdet,

privacy dimension	interrogation	Wissenschaftsaspekt
theory: object	what's privacy for?	Selbstbestimmung, Arbeit als Wissenschaftler:in, persönliche Sicherheit
theory: justification	why should this be private?	Persönlichkeitsrecht, Wissenschaftsfreiheit
theory: contrast concept	what's not private?	kompromittiert/manipuliert, gefährdet/vulnerabel, abhängig
theory: exemplar	what's an example?	Beeinflussung (Verhalten, Karriere), Gefährdung der Forschungsfreiheit
protection: target	privacy of what?	persönliche Daten, Forschungsergebnisse, wissenschaftliche Profile, Kontakte
protection: subject	whose privacy is at stake?	Wissenschaftler:innen, Studierende, Angehörige von Wissenschaftseinrichtungen

Abbildung 2: Analysetool von Mulligan, Koopman & Doty (2016) mit der Anwendung auf Wissenschaft

vulnerabel oder abhängig erfahren. Sie können in solchen Bedingungen unter Verdacht der Manipulierbarkeit geraten, ihr Urteil und ihre Integrität können angezweifelt werden. Diese Kompromittierung erfolgt durch die tracking-durchzogenen Arbeitsbedingungen bzw. Handlungen *anderer*, nicht durch ihre eigenen Handlungen.<sup>33</sup>

Wie schon erwähnt bringt die wissenschaftliche Arbeit viel Freiheit für Entscheidungen, so dass es auch viele subtile, schwierig nachzuweisende Möglichkeiten der Beeinflussung gibt. Je mehr epistemische Asymmetrie zwischen der Wissenschaftlerin und der trackenden Seite (also dem dominierenden Konzern bzw. den Konzernen im Kontext ihrer Arbeit) besteht, desto größer ist die Auswahl an Inhalten für Erpressung und Beeinflussung: persönliche Daten der Wissenschaftlerin oder ihrer Angehörigen, für sie relevante Forschungsdaten und natürlich durch die Einflussnahme auf der Ebene des Wissenschaftsmanagements. Der Schaden für die Wissenschaftlerin, z.B. der Verdacht der Befangenheit bei einem wichtigen Gutachten (zugunsten des Konzerns), besteht bereits durch ihre informationelle Auslieferung als getrackte Seite, nicht erst durch den Nachweis konkreter Einflussnahme. Zudem ist klar, dass die Wissenschaftlerin keine (ii) informational privacy oder (iii) lokale Privatheit ihres Rückzugsortes aufrechterhalten kann, wenn sie davon ausgeht, dass ihr Privatleben einem für ihren Arbeitsbereich relevanten Konzern möglicherweise bis ins kleinste Detail transparent ist. In diesem Sinne ist wissenschaftliche Arbeit zumindest in bestimmten Bereichen größerer Autonomie nicht mit dem Verlust von Privatheit vereinbar, der mit Science Tracking einhergeht.

## 5 Science Tracking und Open Access

Nachdem hauptsächlich Science Tracking behandelt wurde, möchte ich den Zusammenhang mit Open Access wieder aufgreifen. Wieso werden diese beiden so unterschiedlichen Folgen der Digitalisierung der Wissenschaft hier verbunden? Theoretisch hat Open Access nichts mit Tracking zu tun; praktisch sehr viel. Es gibt eine sehr aktive internationale Open-Access-

<sup>33</sup> Siehe hier auch den Vergleich zum Konzept des Panoptikums in Siems (2022).

Community und strukturelle Bewegung zur Stärkung wissenschaftsgeleiteten Publizierens in Diamond-Open-Access (Council of the & European Union, 2023; Mounier & Aspaas, 2023) und Projekte wie SeDOA<sup>34</sup> und DIAMAS<sup>35</sup>. Die Open-Access-Transformation an Universitäten findet jedoch zu einem beträchtlichen Teil weiterhin in Form von Transformationsverträgen in Abhängigkeit von Konzernen statt und zwar als ein zunehmender Plattformisierungsprozess der Wissenschaft (Chan, 2019; Dobusch & Heimstädt, 2023; Ma, 2023). Dabei ist es entscheidend, dass diese Plattformisierung in überwiegendem Maße durch die Vorgaben und Interessen der plattformbetreibenden Datenanalyse-Konzerne bestimmt wird.<sup>36</sup>

Nick Shockey fasst die Problematik zusammen, die SPARC (2023) in Bezug auf Elseviers Plattform ScienceDirect kurz vor dem Elsevier-DEAL-Vertragsabschluss herausarbeitet: „By analyzing the privacy practices of the world’s largest publisher, the [SPARC] report describes how user tracking that would be unthinkable in a physical library setting now happens routinely through publisher platforms. The analysis underlines the concerns this tracking should raise, particularly when the same company is involved in surveillance and data brokering activities. Elsevier is a subsidiary of RELX, a leading data broker and provider of ‚risk‘ products that offer expansive databases of personal information to corporations, governments, and law enforcement agencies.“ (Shockey, 2023)

Ein Beispiel für diese Dynamik und eine mögliche negative Entwicklungsrichtung für Deutschland ist der sogenannte Dutch Deal<sup>37</sup> (2020–2024). Im Jahr 2019, als in Deutschland noch kein Elsevier-Vertrag zustande kam, wurden Details aus Verhandlungen zwischen Elsevier und dem niederländischen Universitätenkonsortium VSNU bekannt. Elsevier wollte dabei auf Umsatzwachstum beim Publizieren im Open Access verzichten und dafür im Open-Access-Vertrag die Implementierung der eigenen Anwendungen zur Datenanalyse an niederländischen Universitäten verankern. Außerdem waren verschiedene „Pilotprojekte“ mit Elsevier-Produkten und Universitäten angedacht. Diese Konstellation, in einem landesweiten Vertrag Open Access an Produkte zu binden, die Elsevier an der Konkurrenz vorbei einen Zugang zu verschiedenen Ebenen von Wissenschaftseinrichtungen geben und neue Abhängigkeiten schaffen würde, stieß auf scharfe Kritik (Aspesi, 2019; Knecht, 2019; Rijcke, 2020; SPARC & Aspesi, 2020).

Bisher ist im DEAL-Vertrag mit Elsevier nichts Ähnliches angeklungen, auch die beiden anderen DEAL-Verträge mit Springer Nature und Wiley haben keine weiteren Produkte an den Vertrag gebunden, zumindest ist dies nicht bekannt geworden. Allerdings sind solche Entwicklungen erwartbar, weil Transformationsverträge aus der Perspektive der Konzerne nicht das Ziel haben, das sie für die wissenschaftliche Community haben. Erstere, die Konzerne, wollen möglichst viel Geld verdienen und ihre vorteilhafte Position ausbauen. Letztere, die wissenschaftliche Community, ist nicht kommerziell motiviert,

34 <https://diamond-open-access.de/> [zuletzt abgerufen am 07.11.2025]

35 <https://diamasproject.eu/> [zuletzt abgerufen am 07.11.2025]

36 Es gibt zahlreiche weitere wissenschaftstheoretische, ethische und politische Fragestellungen rund um den Status und die Verwendung von (Forschungs)Daten (Augsberg & Gehring, 2022; Bundesregierung, 2021; Datenethikkommission, 2019).

37 [https://www.openaccess.nl/sites/default/files/legacy/documenten/countersigned\\_ukb\\_elsevier\\_sd\\_2020-2024\\_agreement\\_geredigeerd.pdf](https://www.openaccess.nl/sites/default/files/legacy/documenten/countersigned_ukb_elsevier_sd_2020-2024_agreement_geredigeerd.pdf) [abgerufen am 10.06.2025]

sondern durch die intrinsischen Ziele der Wissenschaft. Diese Community sieht in Open Access einen Ausweg aus einer unhaltbar gewordenen Abhängigkeit<sup>38</sup> im Publikationsbereich. Sie geht davon aus, dass Transformationsverträge eine temporäre Übergangslösung<sup>39</sup> sind. Nach der Transformation soll es zu einer vollständigen Umstellung der Publikationsfinanzierung kommen und die etablierte Praxis der Rechteabgabe an Verlage endgültig vorbei sein. Das wäre nicht im Sinne des Oligopols der Big Five<sup>40</sup>.

Es liegt natürlich nicht in ihrem Interesse, die eigene Machtposition und Gewinnmargen von bis zu 38 Prozent aufzugeben (Larivière et al., 2015; SPARC, 2019). Die großen Konzerne haben ihre Haltung von anfänglich scharfer Kritik von und Widerstand gegen Open Access (vgl. z.B. Tennant, 2018) zugunsten einer neuen Strategie geändert, die für sie mittlerweile mindestens so lukrativ ist wie das vorherige Subskriptionsmodell. In Bezug auf das Publizieren beinhaltet das weiterhin ausschließlich riesige Pakete mit Zeitschriften aus ihren Portfolios, die Bibliotheken gar nicht brauchen. Diese Pakete werden Bibliotheken in einem i) „hybriden Modell“ angeboten, also weiterhin auf Basis von Subskription, aber mit der Möglichkeit, einzelne Artikel gegen zusätzliche Gebühren, Article Processing Charges (APC), in Open Access zu überführen. Diese Strategie wird ergänzt durch gelegentliche ii) Überführung („flipping“) mancher Titel in das APC-Modell als reine Gold-Open-Access-Zeitschriften und schließlich iii) Open-Access-Transformationsverträge. Letztere sollen irgendwann von einer Kalkulation, die sich aus den Gebühren der Vorjahre und Anteilen von Subskriptions- und Publikationsteil zusammensetzt, zu einem rein auf Publikationsgebühren basierenden Modell übergehen. Wann das passieren soll und wie der Übergang von Zeitschriften zu Gold Open Access stattfinden soll, lässt das Format nicht zufällig unbeantwortet.

Die grundlegenden Probleme der Big Deals (ALLEA, 2022; Butler et al., 2023; Morais et al., 2019; SPARC, o. J.-b) bleiben unadressiert: Dazu gehören die Infragestellung des Paketformats, das die Budgets der Bibliotheken ausreizt und andere Ausgaben verhindert; eine transparente, angemessene Kostenberechnung für eine Publikationsdienstleistung (statt der überhöhten Gebühren der Vorjahre); die Infragestellung der Zusammenarbeit mit Konzernen, deren Geschäftsmodell auf Datenhandel basiert, durch die starke Abhängigkeiten der Wissenschaftsinstitutionen fortgesetzt werden und die aufgrund von Interessenkonflikten Objektivitätskriterien unterlaufen. Diese Ziele wurden bereits teilweise formuliert (Arbeitskreis Forum13+, 2022; Pampel et al., 2022), jedoch bleibt die Frage offen, ob sie mit Hilfe von Transformationsverträgen der bisherigen Form überhaupt erreichbar sind.

In Hinblick auf die Veränderungen der Erforschung von Wissenschaftskommunikation ist Weingart & Taubert (2016) zuzustimmen, dass lediglich die Betrachtung der formalen Seite des wissenschaftlichen Publizierens zu kurz greift. Weder die Komplexität der Open-Access-Transformation noch das Phänomen Science Tracking als inhärentes Element der Kooperation mit den

38 „Due to the publisher’s oligopoly, libraries are more or less helpless, for in scholarly publishing each product represents a unique value and cannot be replaced [...]“ (Larivière et al., 2015, S. 12).

39 Vgl. Schwerpunktinitiative „Digitale Information“ (Pampel et al., 2022).

40 „Large publishers are global companies, and for them even a research-intensive country the size of the UK or Germany is only part of a much larger commercial market. Protecting the integrity and profitability of that market is the publishers’ legitimate aim, and driving a hard bargain with them is a tall order for dispersed buyers.“ (Johnson et al., 2017, S. 31).

etablierten kommerziellen Playern lassen sich so befriedigend erfassen. Es braucht mindestens die Berücksichtigung der Bedingungen von Publikations- und Reputationsmechanismen, nämlich der digitalen Publikations- und Forschungsinfrastrukturen sowie der jeweiligen Trägerorganisationen. Erst auf dieser Ebene können auf einer Seite kommerzielle Player positioniert werden, deren Geschäftsmodelle auf Datenextraktion und Analytics beruhen und deren Infrastrukturen, Produkte und Open-Access-Angebote an diese Geschäftslogiken gebunden sind. Auf der anderen Seite stehen wissenschaftlich getragene Einrichtungen mit unabhängigen Infrastrukturen, Publikationsorganen und forschungsunterstützenden Anwendungen. Auf Basis dieser Unterscheidung können verschiedene Modelle von Open Access und Open Science differenziert werden. Genauso kann dann Science Tracking als aktuelle Praxis von Open Access in Form von Transformationsverträgen differenziert werden. Ich möchte mit einer pessimistischen und einer optimistischen Sichtweise auf die Zukunft von Open Access enden.

## 6 Ausblick(e)

Die Fortführung der Zusammenarbeit mit Datenanalyse-Konzernen, wie sie durch die hier analysierten DEAL-Verträge aktuell besteht, lässt eher eine *pessimistische* Zukunftserwartung von Open Access und Open Science aufkommen. Ein negatives Szenario droht, wenn die Open-Access-Transformation im institutionellen Bereich weiterhin etablierte Publikationsstrukturen fortsetzt, während nicht-kommerzielle Scholar-led-Alternativen selten eine stabile Finanzierung erhalten oder die nötigen Entwicklungsmittel. Dabei bewegt sich die Digitalisierung der Wissenschaft dahin, a) einen großen Teil der Publikations- und Forschungstätigkeit auf proprietäre Plattformen zu verlagern und b) Open Access an die Fortführung der früheren Big Deals zu binden und Transformationsverträge zum Vehikel neuer Abhängigkeiten zu wenden. Durch die Plattformisierung könnten vorhandene offene und öffentliche Strukturen, Forschungsdaten, Metadaten, Open-Science-Ergebnisse etc. in die proprietären Plattformen und Anwendungen integriert werden, die diverse Tracking-Methoden nutzen.<sup>41</sup> Dies ist schon der Fall beim Zugang zu Literatur in Open Access bei den entsprechenden Konzernen – Open-Access-Artikel können im Default-Modus erst über die Nutzung der Plattform erreicht werden und nicht z.B. datenschutzkonform über ein Repositorium der Hochschule. Auf Grundlage ihrer Marktstellung, ihrer digitaler Ressourcen und ihres asymmetrischen Wissensvorsprungs durch Datentracking könnten Datenanalyse-Konzerne künftig bzw. können teilweise bereits die Nutzung und Zusammenführung ihrer Anwendungen aus dem Forschungszyklus, Anwendungen im Bereich CRIS/FIS und Anwendungen für die Forschungsförderung forcieren. Damit könnten sie künftig die verschiedenen Ebenen des Wissenschaftssektors durchdringen, einen systematischen Wissensvorsprung vor den Wissenschaftseinrichtungen erringen und Einflussmöglichkeiten auf wissenschafts- und institutionsinterne Prozesse ausüben. Weitere Schritte könnten „Pilotprojekte“ (Dutch Deal) zur

41 Elsevier arbeitet daran, den Forschungssektor möglichst innerhalb des Elsevier-Biotops zu verlagern, z. B. mit eigenen Datenverarbeitungsangeboten (**Data Sets**) einer Suchmaschine für Förderungen (**Funding Institutional**) und dem Angebot, Repositorien (bepress und Digital Commons) für Universitäten, aber auch Studiums- und Prüfungssoftware (**HESI**) bereitzustellen. Die Präsenz im Gesundheitssektor habe ich hier nicht berücksichtigt. [Alle Links zuletzt geprüft am 25.07.2024]

Entwicklung gemeinsamer Produkte werden, über die sie weiter reichende Befugnisse bekommen.

Eine *optimistische* Zukunftserwartung beruht auf einer zumindest schrittweisen Herauslösung aus den hier behandelten Abhängigkeiten und folgt den Empfehlungen des Wissenschaftsrats (2023). Darin gibt es dauerhafte Maßnahmen zur Stärkung der Cybersicherheit wissenschaftlicher Einrichtungen; den Ausbau öffentlich geförderter digitaler Infrastrukturen und Plattformen; transparente Open-Source-Lösungen und die dauerhafte Förderung von Diamond Open Access. Hierzu gehört natürlich auch die Berücksichtigung der disziplinspezifischen Bedarfe, die sich nicht in der Publikation von Zeitschriftenaufsätzen erschöpfen sowie der nötige Spielraum für künftige Entwicklungen (DFG Deutsche Forschungsgemeinschaft, 2020). Die Umsetzung dieser Ziele fällt in die „*Gestaltung des digitalen Raumes als Daueraufgabe von Wissenschaftseinrichtungen*“ (Wissenschaftsrat, 2023, S. 7) und ist damit ein grundlegendes Anliegen einer digital souveränen Wissenschaft.

## Referenzen

- Acar, G., Eubank, C., Englehardt, S., Juarez, M., Narayanan, A., & Diaz, C. (2014). The Web Never Forgets: Persistent Tracking Mechanisms in the Wild. *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 674–689. <https://doi.org/10.1145/2660267.2660347>
- ALLEA. (2022). *ALLEA Statement on Open Access Publication Under "Big Deals" and the New Copyright Rules*. <https://doi.org/10.26356/BigDeals>
- Andrejevic, M., & Gates, K. (2014). Big Data Surveillance: Introduction. *Surveillance & Society*, 12(2), 185–196. <https://doi.org/10.24908/ss.v12i2.5242>
- Arbeitskreis Forum13+. (2022). „Forum 13+“-Spektrum zur Bewertung von Open Access-Transformationsverträgen und Verlagsangeboten: Stand Oktober 2021. <https://doi.org/10.3249/UGOE-PUBL-12>
- Aspesi, C. (2019). *Leaked Dutch Contract with Elsevier Raises Significant Alarm Bells*. <https://sparcopen.org/news/2019/leaked-dutch-contract-with-elsevier-raises-significant-alarm-bells/>
- Augsberg, S., & Gehring, P. (Hrsg.). (2022). *Datensouveränität*. Campus Verlag.
- Bashyakarla, V. (o. J.). *Third-Party Tracking: Cookies, beacons, fingerprints and more*. Abgerufen 14. Dezember 2023, von <https://ourdataourselves.tacticaltech.org/posts/third-party-tracking/>
- Biddle, S. (2021). LexisNexis to Provide Giant Database of Personal Information to ICE. *The Intercept*. <https://theintercept.com/2021/04/02/ice-database-surveillance-lexisnexis/>
- Binns, R. (2022). *Tracking on the Web, Mobile and the Internet-of-Things*. arXiv. <https://doi.org/10.48550/ARXIV.2201.10831>
- Bolin, G., & Jerslev, A. (2018). Surveillance through media, by media, in media. *Northern Lights*, 16(1), 3–21.
- Brehm, E., Knaf, K., & Talke, A. (2018). *Datenschutz ab Inkrafttreten der Datenschutz-Grundverordnung – Handreichung für Bibliotheken*. Institutionelles Repositorium der Leibniz Universität Hannover.

- Bundesregierung. (2021). *Datenstrategie der Bundesregierung*.
- Butler, L.-A., Matthias, L., Simard, M.-A., Mongeon, P., & Haustein, S. (2023). The Oligopoly's Shift to Open Access. How the Big Five Academic Publishers Profit from Article Processing Charges. *Quantitative Science Studies*, 1–33. [https://doi.org/10.1162/qss\\_a\\_00272](https://doi.org/10.1162/qss_a_00272)
- Chan, L. (2019). *Platform Capitalism and the Governance of Knowledge Infrastructure*. <https://doi.org/10.5281/ZENODO.2656601>
- Chen, G., & Chan, L. (2021). University Rankings and Governance by Metrics and Algorithms. In E. Hazelkorn & G. Mihut (Hrsg.), *Research Handbook on University Rankings: Theory, Methodology, Influence and Impact* (S. 424–441). Edward Elgar Publishing. <https://doi.org/10.4337/9781788974981>
- Christl, W., & Toner, A. (2024). Pervasive identity surveillance for marketing purposes. A technical report on personal data processing for LiveRamp's RampID identity graph system based on an analysis of software documentation. *Cracked Labs*. <https://crackedlabs.org/en/identity-surveillance>
- Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM*, 31(5), 498–512. <https://doi.org/10.1145/42411.42413>
- Council of the, & European Union. (2023). *COUNCIL CONCLUSIONS ON HIGH-QUALITY, TRANSPARENT, OPEN, TRUSTWORTHY AND EQUITABLE SCHOLARLY PUBLISHING*. <https://data.consilium.europa.eu/doc/document/ST-9616-2023-INIT/en/pdf>
- Crotty, D. (2023). *Quantifying Consolidation in the Scholarly Journals Market*. <https://scholarlykitchen.sspnet.org/2023/10/30/quantifying-consolidation-in-the-scholarly-journals-market/>
- Datenethikkommission. (2019). *Gutachten der Datenethikkommission*. <https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.html>
- DFG AWBI, A. für W. B. U. I. (2021). *Datentracking in der Wissenschaft: Aggregation und Verwendung bzw. Verkauf von Nutzungsdaten durch Wissenschaftsverlage. Ein Informationspapier des Ausschusses für Wissenschaftliche Bibliotheken und Informationssysteme der Deutschen Forschungsgemeinschaft*. <https://zenodo.org/record/5900759>
- DFG Deutsche Forschungsgemeinschaft. (2020). *Digitaler Wandel in den Wissenschaften*. Zenodo. <https://zenodo.org/record/4191344>
- Dittmann, J., Altschaffel, R., & Kiltz, S. (2023). *Webtracking durch Wissenschaftsverlage – eine Spurensuche: Was wird genutzt, was darf man und was kann/muss/sollte man dagegen tun?*
- Dobusch, L., & Heimstädt, M. (2023). The structural transformation of the scientific public sphere: Constitution and consequences of the path towards open access. *Philosophy & Social Criticism*, 1–19. <https://doi.org/10.1177/01914537231203558>
- Drake, T., Gulliver, S., & Harle, J. (o. J.). *Research Publishing Is an Under-Recognised Global Challenge*. <https://www.cgdev.org/sites/default/files/research-publishing-under-recognised-global-challenge-opportunities-g20-act.pdf>
- Eisenegger, M. (2021). Dritter, digitaler Strukturwandel der Öffentlichkeit als Folge der Plattformisierung. In M. Eisenegger, M. Prinzing, P. Ettinger, & R.

- Blum (Hrsg.), *Digitaler Strukturwandel der Öffentlichkeit: Historische Verortung, Modelle und Konsequenzen* (S. 17–40). Springer Fachmedien Wiesbaden. <https://doi.org/10.1007/978-3-658-32133-8>
- Fadeeva, Y. (2026). *Wissenschaftstracking und Lock-in-Effekt*. Melusina.
- Fraunhofer-Institut für Sichere, I. (2020). *Privacy und Big Data: Studie des Verbundprojektes ‚Cybersicherheit für die digitale Verwaltung‘*.
- Freiberg, M. (2022). Third-Party-Tracking bei Wiley und Springer: Analyse und Ausblick. *ABI Technik*, 42(2), 96–104. <https://doi.org/10.1515/abitech-2022-0017>
- Fuchs, C. (Hrsg.). (2012). *Internet and surveillance: the challenges of Web 2.0 and social media*. Routledge. <https://doi.org/10.4324/9780203806432>
- Giroux, H. A. (2015). Totalitarian Paranoia in the Post-Orwellian Surveillance State. *Cultural Studies*, 29(2), 108–140. <https://doi.org/10.1080/09502386.2014.917118>
- Hanson, C. (2019). *User Tracking on Academic Publisher Platforms*. <https://www.codyh.com/writing/tracking.html>
- Holzer, A. (2022). Die Vermessbarkeit der Wissenschaft Digitalisierung, wissenschaftliches Publizieren, Verhaltenstracking und Wissenschaftsbewertung. In N. Mößner & K. Erlach (Hrsg.), *Kalibrierung der Wissenschaft: Auswirkungen der Digitalisierung auf die wissenschaftliche Erkenntnis* (S. 163–182). transcript Verlag. <https://doi.org/10.14361/9783839462102>
- Hoofnagle, C. J., Soltani, A., Good, N., Wambach, D. J., & Ayenson, M. D. (2012). Behavioral Advertising: The Offer You Cannot Refuse. *Harvard Law & Policy Review*, 6, 273–296.
- Johnson, R., Fosci, M., Chiarelli, A., Pinfield, S., & Jubb, M. (2017). *Towards a competitive and sustainable OA market in Europe - a study of the open access market and policy environment*. Zenodo. <https://doi.org/10.5281/ZENODO.401029>
- Keegan, J., & Eastwood, J. (2023). From „Heavy Purchasers“ of Pregnancy Tests to the Depression-Prone: We Found 650,000 Ways Advertisers Label You. *The Markup*. <https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you>
- Knecht, S. de. (2019). *Leaked document on Elsevier negotiations sparks controversy - ScienceGuide*. <https://www.scienceguide.nl/2019/11/leaked-document-on-elsevier-negotiations-sparks-controversy/>
- Lamdan, S. (2022). *Data Cartels The Companies That Control and Monopolize Our Information*. Stanford University Press. <https://doi.org/10.1515/9781503633728>
- Larivière, V., Haustein, S., & Mongeon, P. (2015). The Oligopoly of Academic Publishers in the Digital Era. *PLOS ONE*, 10(6), e0127502. <https://doi.org/10.1371/journal.pone.0127502>
- Lauer, G. (2022). Datentracking in den Wissenschaften. *o-bib. Das offene Bibliotheksjournal / Herausgeber VDB*, 1–13 Seiten. <https://doi.org/10.5282/O-BIB/5796>

- LexisNexis, R. S. (2023). *Experience the Power of One: Secure and Seamless Identity Solution*. <https://www.carahsoft.com/learn/resource/22231-experience-the-power-of-one-secure-and-seamless-identity-solution#resources>
- Lisker, M. (2023). *Von der (Un-)Möglichkeit, digital mündig zu sein Tracking-Infrastrukturen und die Responsibilisierung des Individuums im Internet*. Masterarbeit.
- Lynch, C. (2017). The rise of reading analytics and the emerging calculus of reader privacy in the digital world. *First Monday*. <https://doi.org/10.5210/fm.v22i4.7414>
- Lyon, D. (2015). *Surveillance after Snowden*. Polity Press.
- Ma, L. (2023). The Platformisation of Scholarly Information and How to Fight It. *LIBER Quarterly: The Journal of the Association of European Research Libraries*, 33(1), 1–20. <https://doi.org/10.53377/lq.13561>
- Morais, R., Stoy, L., & Borrell-Damián, L. (2019). *2019 Big Deals Survey Report. An Updated Mapping of Major Scholarly Publishing Contracts in Europe*.
- Mounier, P., & Aspaas, P. P. (2023). DIAMAS: Supporting high quality Diamond Open Access publishing. *Open Science Talk*, 48. <https://doi.org/10.7557/19.6862>
- Mulligan, D. K., Koopman, C., & Doty, N. (2016). Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 374(2083), 20160118. <https://doi.org/10.1098/rsta.2016.0118>
- Münch, R. (2007). *Die akademische Elite: zur sozialen Konstruktion wissenschaftlicher Exzellenz*. Suhrkamp.
- Pampel, H., Bertelmann, R., Hillenkötter, K., Mittermaier, B., Pieper, D., Schäffler, H., Seeh, S., & Tullney, M. (2022). *Empfehlungen für transformative Zeitschriftenverträge mit Publikationsdienstleistern: Handreichung der Schwerpunktinitiative „Digitale Information“ der Allianz der deutschen Wissenschaftsorganisationen vor dem Hintergrund der Umsetzung der Open-Access-Strategie 2021–2025 der Allianz der deutschen Wissenschaftsorganisationen*. <https://doi.org/10.48440/ALLIANZOA.045>
- Pooley, J. (2022). Surveillance Publishing. *The Journal of Electronic Publishing*, 25(1). <https://doi.org/10.3998/jep.1874>
- Reda, F. (2022). *Tracking Science: How Libraries can Protect Data and Scientific Freedom*. ZBW MediaTalk. <https://www.zbw-mediataalk.eu/2022/01/tracking-science-how-libraries-can-protect-data-and-scientific-freedom/>
- Retzlaff, E. (2022). Wer bewertet mit welchen Interessen wissenschaftliche Publikationen? Eine Skizzierung des Einflusses kommerzieller Interessen auf die Forschungsauswertung. In N. Mößner & K. Erlach (Hrsg.), *Kalibrierung der Wissenschaft: Auswirkungen der Digitalisierung auf die wissenschaftliche Erkenntnis* (S. 139–162). transcript Verlag. <https://doi.org/10.14361/9783839462102>
- Reuter, M. (2024). *LiveRamp: Datenfirma unterhält „privates Bevölkerungsregister“*. <https://netzpolitik.org/2024/liveramp-datenfirma-unterhaelt-privates-bevoelkerungsregister/>
- Rijcke, S. de. (2020). *Elsevier and the Dutch Open Science goals*. <https://www.leidenmadtrics.nl/articles/s-de-rijcke-cwts-leidenuniv-nl>

- Rössler, B. (2005). *The value of privacy*. Polity.
- Roßnagel, A. (2022). Third-Party-Tracking – ein Problem aus Sicht des Datenschutzes?: Interview mit Prof. Dr. Alexander Roßnagel, Hessischer Beauftragter für Datenschutz und Informationsfreiheit. *ABI Technik*, 42(2), 105–107. <https://doi.org/10.1515/abitech-2022-0018>
- Ryan, J. (2022). *ICCL report on the scale of Real-Time Bidding data broadcasts in the U.S. and Europe*. <https://www.iccl.ie/news/iccl-report-on-the-scale-of-real-time-bidding-data-broadcasts-in-the-u-s-and-europe/>
- Ryan, J., & Christl, W. (o. J.). *Europe's hidden security crisis: How data about European defence personnel and political leaders flows to foreign states and non-state actors*. <https://www.iccl.ie/digital-data/europes-hidden-security-crisis/>
- Salo, D. (2021). Physical-Equivalent Privacy. *The Serials Librarian*, 81(1), 20–34. <https://doi.org/10.1080/0361526X.2021.1875962>
- Schneider, M., Enzmann, M., & Stopczynski, M. (2014). *SIT Technical reports. 2014,01: Web-Tracking-Report*. Fraunhofer-Verlag.
- Shockey, N. (2023). *SPARC Report Urges Action to Address Concerns with ScienceDirect Data Privacy Practices*. <https://sparcopen.org/news/2023/sparc-report-urges-action-to-address-concerns-with-sciencedirect-data-privacy-practices/>
- Siems, R. (2021). *When your journal reads you – user tracking on science publisher platforms*. <https://doi.org/10.5281/ZENODO.4683778>
- Siems, R. (2022). Lesen der Anderen. o-bib. *Das offene Bibliotheksjournal / Herausgeber VDB*, 1–25. <https://doi.org/10.5282/O-BIB/5797>
- Siems, R. (2024). Subprime Impact Crisis. Bibliotheken, Politik und digitale Souveränität. *Bibliothek Forschung und Praxis*. <https://doi.org/10.1515/bfp-2024-0008>
- Siems, R. (2025). Wissenschaft als datafizierter Raum. In Y. Fadeeva, S. Franz, D. Kampkaspar, M. Seltmann, T. Steyer, & N.-O. Walkowski (Hrsg.), *Reputation ohne Paywall? Wissenschaftliches Publizieren im digitalen Wandel*. Melusina Press. <https://www.melusinapress.lu/projects/1981-5838>
- SPARC. (o. J.-a). *2020 Update - SPARC Landscape Analysis and Roadmap for Action*.
- SPARC. (o. J.-b). *Emerging Concerns: The Bigger Deal (From the 2020 update report)*. Abgerufen 8. Dezember 2023, von <https://infrastructure.sparcopen.org/2020-update/the-bigger-deal>
- SPARC. (2019). *Landscape Analysis: The Changing Academic Publishing Industry – Implications for Academic Institutions*.
- SPARC. (2021). *2021 Update: SPARC Landscape Analysis and Roadmap for Action*.
- SPARC. (2022). *Elsevier's Acquisition of Interfolio: Risks and Responses*. <https://infrastructure.sparcopen.org/interfolio-acquisition>
- SPARC. (2023). *Navigating Risk in Vendor Data Privacy Practices - An Analysis of Elsevier ScienceDirect*.
- SPARC, & Aspesi, C. (2020). *The Dutch Consortia/Elsevier Contract: The Real Risks*. <https://infrastructure.sparcopen.org/dutch-consortia-elsevier-contract>

- Tau, B. (2024). *Means of control: how the hidden alliance of tech and government is creating a new American surveillance state* (First edition). Crown.
- Tennant, J. (2018). Elsevier are corrupting open science in Europe. *The Guardian*. <https://www.theguardian.com/science/political-science/2018/jun/29/elsevier-are-corrupting-open-science-in-europe>
- Valentino-DeVries, J., Singer, N., Keller, M. H., & Krolik, A. (2018). Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret. *The New York Times*. <https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html>, <https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html>
- Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society*, 12(2), 197–208. <https://doi.org/10.24908/ss.v12i2.4776>
- Weingart, P., & Taubert, N. C. (Hrsg.). (2016). Wandel des wissenschaftlichen Publizierens – eine Heuristik zur Analyse rezenter Wandlungsprozesse. In *Wissenschaftliches Publizieren: zwischen Digitalisierung, Leistungsmessung, Ökonomisierung und medialer Beobachtung* (S. 3–40). De Gruyter Akademie Forschung.
- Wissenschaftsrat. (2023). *Empfehlungen zur Souveränität und Sicherheit der Wissenschaft im digitalen Raum*. 65 pages. <https://doi.org/10.57674/M6PK-DT95>
- Zuboff, S. (2019). *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. Profile books.