JONAS BREYER
RECHTSANWALT

Rechtsanwaltskanzlei Breyer
Schiersteiner Straße 37a
65187 Wiesbaden

Jonas Breyer
Rechtsanwalt

T +49 [redacted]
F +49
M +49
[redacted]
www.ra-breyer.de

17.08.2018

Kanzlei Breyer ▪ Schiersteiner Straße 37a ▪ 65187 Wiesbaden
Landgericht Berlin
– 57 S 87/08 –
Tegeler Weg 17-21
10589 Berlin

57 S 87/08

In der Zivilsache

Breyer ./. Bundesrepublik Deutschland

wird auf die mündliche Verhandlung vom 28.08.2018 wie folgt vorgetragen:

1. Beweisaufnahme nicht erforderlich

Eine Beweisaufnahme über die Behauptungen der Beklagten erscheint nicht erforderlich: Da die Beklagte unstreitig seit Jahren funktionsfähige Telemedien ohne die beanstandete Surfprotokollierung anbietet, kann sie aus Sicht des Klägers nicht damit gehört werden, die beanstandete Surfprotokollierung sei zur Gewährleistung der Funktionsfähigkeit von Telemedien erforderlich. In sich widersprüchlicher Vortrag kann nicht Grundlage einer Beweisaufnahme sein (BGH, Urteil vom 23. September 2004 – IX ZR 137/03 –, Rn. 23).

Auch der persönlich angehörte Vertreter der Beklagten [redacted] hat in der mündlichen Verhandlung lediglich behauptet, die beanstandete Surfprotokollierung könne „hilfreich“ sein und werde empfohlen, nicht aber, dass sie zwingend erforderlich sei. Das Gericht kann die Angaben der persönlich angehörten Partei seinem Urteil zugrunde legen (Greger in: Zöller, Zivilprozessordnung, 32. Aufl. 2018, § 141 ZPO, Rn. 1a). Wenngleich die Angaben von [redacted] nicht protokolliert worden sind, kann ihre Darstellung im Urteil nachgeholt werden (Greger in: Zöller, Zivilprozessordnung, 32. Aufl. 2018, § 141 ZPO, Rn. 7). Soweit der Prozessbevollmächtigte der Beklagten im Widerspruch zur eigenen Partei eine zwingende Erforderlichkeit behauptet, ist regelmäßig das Vorbringen der Partei der richterlichen Entscheidung zugrunde zu legen (Althammer in: Zöller, Zivilprozessordnung, 32. Aufl. 2018, § 85 ZPO, Rn. 8 m.w.N.). Der Prozessbevollmächtigte ist an persönliche Erklärungen der Partei gebunden und darf diese nicht „berichtigen“ (MüKoZPO/Toussaint ZPO § 85 Rn. 7).

Der Bundesgerichtshof würde ein so begründetes Urteil nicht aufheben, weil er an die Feststellungen der Tatsacheninstanz gebunden ist. Der nun feststehende Sachverhalt ist ein anderer als er dem Bundesgerichtshof zuletzt zur Entscheidung vorlag.

2. Neue Begutachtung und neuer Gutachter nicht erforderlich

Sollte die Kammer dies anders sehen, so hält der Kläger die Voraussetzungen des § 412 ZPO für eine neue Begutachtung durch einen anderen Sachverständigen nicht für gegeben und befürchtet, dass es der Beklagten auf diesem Wege gelingt, ein ihr missliebiges und dem Kläger günstiges Ergebnis der Beweisaufnahme zu beseitigen.

Ist das Gutachten des Sachverständigen Köpsell, ggf. nach der beantragten mündlichen Erläuterung, nicht ausreichend, um der Kammer die Überzeugung von der Wahrheit der zu beweisenden Behauptung zu verschaffen, ist grundsätzlich nach der Beweislast zu entscheiden (Greger in: Zöller, Zivilprozessordnung, 32. Aufl. 2018, § 412 ZPO, Rn. 1), hier also eine Beweislastentscheidung zulasten der Beklagten zu treffen. Alleine, dass bei der Kammer Zweifel verbleiben, erfordert also keine neue Begutachtung.

Es steht zwar im Ermessen des Gerichts, anstelle einer Beweislastentscheidung eine neue Begutachtung anzuordnen. Dagegen spricht hier aber die mit 10 Jahren bereits sehr lange Verfahrensdauer und das Recht des Klägers auf Entscheidung innerhalb angemessener Dauer. Die letzte Begutachtung hat insgesamt über zwei Jahre lang gedauert. Zudem wäre der Kostenaufwand einer vollständig neuen Begutachtung gemessen am Streitwert von 4.000 € unangemessen hoch.

Die Anordnung einer neuen Begutachtung erscheint jedenfalls solange nicht ermessensgerecht, wie die Möglichkeit einer mündlichen Erläuterung und Aufklärung durch den bereits bestellten Sachverständigen nicht ausgeschöpft worden ist. Ohne mündliche Anhörung des Sachverständigen lässt sich nicht beurteilen, ob seine Begutachtung im Sinne des § 412 ZPO genügt oder nicht. Durch mündliche Erläuterung können etwaige Widersprüche aufgeklärt und auch eine Stellungnahme zu den von der Kammer angesprochenen Ausführungen des Oberlandesgerichts Frankfurt am Main gefordert werden.

Jedenfalls müsste mit einer etwaigen neuen Begutachtung aus Sicht des Klägers gemäß § 412 Abs. 1 ZPO zumindest derselbe Sachverständige beauftragt werden, um ihm Gelegenheit zur Erläuterung und zur Aufklärung von Zweifelsfragen zu geben. § 412 Abs. 1 ZPO sieht ausdrücklich die Möglichkeit einer neuen Begutachtung durch denselben Sachverständigen vor.

Nur höchst hilfsweise sei darauf hingewiesen, dass die TU Dresden den „Lehrstuhl für Datenschutz und Datensicherheit“ von Prof. Pfitzmann inzwischen neu besetzt hat mit Prof. Dr. Thorsten Strufe. Diesen zu beauftragen wäre ein milderes Mittel gegenüber der vollständigen Entziehung des Sachverständigen eines Lehrstuhls, dessen Gutachten Gesichtspunkte der datenschutzfreundlichen Technikgestaltung einbezieht und zugunsten des Klägers ausgefallen ist. Der Kläger weist vorsorglich darauf hin, dass er weder mit Dr. Köpsell noch mit Prof. Dr. Strufe jemals gesprochen hat oder gar persönlich bekannt ist.

Im Übrigen wird auf den Schriftsatz vom 08.01.2013 Bezug genommen, in dem ausgeführt worden ist, warum der Leiter eines vom Bund finanzierten und von diesem abhängigen Instituts (dort: Prof. Martini) nicht als unabhängiger Sachverständiger geeignet ist. Wie bereits im September 2010 schriftsätzlich näher ausgeführt, muss ein Sachverständiger die Beweisfrage fachlich beurteilen können, ohne jedoch ein eigenes berufliches oder wirtschaftliches Interesse an dem Ausgang der Beweisaufnahme zu haben. Zudem sind Kenntnisse in datenschutzfreundlicher Technikgestaltung erforderlich, um die streitige Erforderlichkeitsfrage beurteilen zu können.

3. Fassung der Beweisfragen

Sollte die Kammer eine Neubegutachtung beschließen, so wird angeregt, die Beweisfragen wie folgt zu fassen:

> *Es soll durch Einholung eines schriftlichen Sachverständigengutachtens Beweis erhoben werden über die Behauptungen der Beklagten,*
>
> *a) um die Funktionsfähigkeit der Telemedien der Beklagten zu gewährleisten, sei es erforderlich (nicht lediglich im Sinne von nützlich), die vollständige nicht-anonymisierte Internetprotokolladresse (IP-Adresse) des zugreifenden Hostsystems des Klägers, die im Zusammenhang mit der Nutzung öffentlich zugänglicher Telemedien der Beklagten im Internet übertragen wird, über das Ende des jeweiligen Nutzungsvorgangs hinaus zu speichern oder durch Dritte speichern zu lassen, und zwar nicht nur dann, wenn die Speicherung im Störungsfall zur Wiederherstellung der Verfügbarkeit des Telemediums erforderlich ist,*
>
> *b) nach dem gegenwärtigen Stand der Technik sei es nicht möglich, die Funktionsfähigkeit der Telemedien der Beklagten zu gewährleisten, wenn die Beklagte nur im Störungsfall zur Wiederherstellung der Verfügbarkeit eines Telemediums die vollständige nicht-anonymisierte Internetprotokolladresse (IP-Adresse) des zugreifenden Hostsystems des Klägers über das Ende des jeweiligen Nutzungsvorgangs hinaus speichere oder durch Dritte speichern lasse,*
>
> *c) dass die Beklagte eine Vielzahl von Telemedien bereit stellt, ohne die Internetprotokolladresse (IP-Adresse) des zugreifenden Hostsystems des Klägers über das Ende des jeweiligen Nutzungsvorgangs hinaus zu speichern oder durch Dritte speichern zu lassen, ändere nichts an der Erforderlichkeit einer solchen Speicherung zur Gewährleistung der Funktionsfähigkeit der Telemedien der Beklagten,*
>
> *d) die Speicherung der Internetprotokolladresse (IP-Adresse) des zugreifenden Hostsystems des Klägers über das Ende des jeweiligen Nutzungsvorgangs hinaus schrecke von Störungen der Funktionsfähigkeit der Telemedien der Beklagten („Angriffen“) ab.*
>
> *Der Sachverständige soll in seinem Gutachten auch auf die Ausführungen des Gerichtsgutachters Köpsell, des Parteigutachters Martini sowie das Vorbringen der Parteien im Prozess zu den Beweisfragen eingehen.*

Zur Begründung:

a. Beweisfrage zu a)

Erwägungsgrund 49 der DSGVO erscheint als Maßstab der Beweisfrage zu a) nicht geeignet. Ein Erwägungsgrund ist keine Rechtsvorschrift. Zudem verwendet der Erwägungsgrund unbestimmte Rechtsbegriffe, die einer Begutachtung nicht zugänglich sind (z.B. „vorgegebenen Grad der Zuverlässigkeit“, „widerrechtliche oder mutwillige Eingriffe“, „damit zusammenhängende Dienste“).

Auch der Begriff der „IT-Sicherheit“ (Beweisbeschluss vom 20.05.2010) ist in keiner anwendbaren Rechtsnorm vorgesehen, vom Bundesgerichtshof nicht zugrunde gelegt worden, zu unbestimmt und für eine Begutachtung ungeeignet. Das Bundesamt für Sicherheit in der Informationstechnik definiert den Begriff der „IT-Sicherheit“ wie folgt:

> *„IT-Sicherheit bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind. IT-Sicherheit ist also der Zustand, in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind.“*

Damit geht es um unbestimmte Rechtsbegriffe, die einer Begutachtung nicht zugänglich sind (z.B. „tragbares Maß“, „angemessene Maßnahmen“). Rechtlich maßgeblich ist nicht die „Angemessenheit“ von Maßnahmen, sondern deren strikte „Erforderlichkeit“.

Die hier vorgeschlagene Beweisfrage zu a) orientiert sich am (bindenden) Revisionsurteil des Bundesgerichtshofs, dessen zweiter amtlicher Leitsatz lautet:

> *„§ 15 Abs. 1 TMG ist entsprechend Art. 7 Buchst. f der Richtlinie 95/46 EG dahin auszulegen, dass ein Anbieter von Online-Mediendiensten personenbezogene Daten eines Nutzers dieser Dienste ohne dessen Einwilligung auch über das Ende eines Nutzungsvorgangs hinaus dann erheben und verwenden darf, soweit ihre Erhebung und ihre Verwendung erforderlich sind, um die generelle Funktionsfähigkeit der Dienste zu gewährleisten...“*

Auch der EuGH hat zur inhaltsgleichen Datenschutzrichtlinie entschieden,

> *„dass der Zweck, die generelle Funktionsfähigkeit der Dienste zu gewährleisten, die Verwendung der Daten über das Ende eines Nutzungsvorgangs hinaus rechtfertigen kann“ (Ziff. 2 des Tenors).*

Nur insoweit ist das Interesse der Beklagten als „berechtigt“ eingeordnet worden.

Der Kläger hält es – auch angesichts der Bindungswirkung des Revisionsurteils – nicht für zulässig, darüber hinaus noch ganz andere Speicherinteressen und -wünsche der Beklagten einzubeziehen. So stellt der Bundesgerichtshof etwa alleine auf die Funktionsfähigkeit der „Online-Mediendienste“ der Beklagten ab und nicht etwa auf die Funktionsfähigkeit ganz anderer Systeme der Beklagten.

Die vorgeschlagene Beweisfrage zu a) orientiert sich am Klageantrag, indem sie gerade auf die vom Kläger genutzten IP-Adressen abstellt. Im vorliegenden Rechtsstreit ist nicht entscheidungserheblich, ob die Beklagte irgendwelche IP-Adressen speichern darf, sondern ob sie gerade die vom Kläger verwendeten IP-Adressen protokollieren darf, obwohl von der Internetnutzung durch den Kläger unstreitig keinerlei Gefahren für die Beklagte oder ihre Informationstechnik ausgehen. Der Sachverständige wird gegebenenfalls dazu Stellung zu nehmen haben, ob sich etwa erforderliche Speicherungen so begrenzen lassen, dass die IP-Adressen rechtstreuer Nutzer wie des Klägers von ihnen ausgenommen bleiben.

Die vorgeschlagene Beweisfrage zu a) beschränkt sich ferner auf die Speicherung der IP-Adresse über die Dauer des Nutzungsvorgangs hinaus. Dass die IP-Adresse für die Dauer der Übertragung abgerufener Internetseiten gespeichert werden muss, ist zwischen den Parteien unstreitig.

Schließlich nimmt die vorgeschlagene Beweisfrage zu a) den Fall aus, dass die Speicherung im Störungsfall zur Wiederherstellung der Verfügbarkeit des Telemediums erforderlich sei. Diese Frage ist dadurch dem Streit entzogen, dass sie vom Klageantrag ausgenommen ist. Einer sachverständigen Stellungnahme dazu bedarf es infolgedessen nicht.

Die Beweisfrage zu a) stellt abschließend klar, dass der Sachverständige als milderes Mittel die Möglichkeit einer anonymisierten Speicherung von IP-Adressen prüfen soll.

b. Beweisfrage zu b)

Die vorgeschlagene Beweisfrage zu b) knüpft an den Rechtsgedanken des § 14 BImSchG an. Nach dieser Vorschrift kann auf Grund privatrechtlicher Abwehransprüche nicht die Einstellung des Betriebs einer genehmigten Anlage verlangt werden, wenn die Vermeidung benachteiligender Einwirkungen der Anlage „nach dem Stand der Technik nicht durchführbar oder wirtschaftlich nicht vertretbar“ ist. Wäre das Angebot von Telemedien ohne Speicherung von IP-Adressen über die Nutzungsdauer hinaus „nach dem Stand der Technik nicht durchführbar oder wirtschaftlich nicht vertretbar“, so könnte diese Maßnahme als erforderlich angesehen werden. Die bloße Frage, ob die Speicherung von IP-Adressen dem „Stand der Technik dient“ (Beweisbeschluss vom 20.05.2010), ist dagegen zu unbestimmt, um den Gegenstand einer sachverständigen Begutachtung bilden zu können.

Dabei nimmt die vorgeschlagene Beweisfrage zu b) den Fall aus, dass die Speicherung im Störungsfall zur Wiederherstellung der Verfügbarkeit des Telemediums erforderlich sei. Diese Frage ist dadurch dem Streit entzogen, dass sie vom Klageantrag ausgenommen ist.

c. Beweisfrage zu c)

Die vorgeschlagene Beweisfrage zu c) hat die Behauptung der Beklagten zum Gegenstand, die Nichterfassung von Nutzer-IP-Adressen bei der Bereitstellung einiger ihrer Telemedien lasse nicht darauf schließen, dass die Erfassung von Besucher-IP-Adressen auch bei der Bereitstellung der übrigen Telemedien der Beklagten verzichtbar sei. Der Bundesgerichtshof hat es ebenfalls als

wichtig angesehen, der Frage nachzugehen, ob die eigene Praxis der Beklagten deren Vortrag zur Erforderlichkeit nicht widerlegt.

„Die Beklagte verzichtet nach ihren eigenen Angaben bei einer Vielzahl der von ihr betriebenen Portale“ auf eine Surfprotokollierung, wie der BGH wörtlich festgehalten hat (Abs. 41). Diese Feststellung ist dem Beweisbeschluss zugrunde zu legen.

d. Beweisfrage zu d)

Die vorgeschlagene Beweisfrage zu d) hat die zwischen den Parteien streitige und von der Kammer als relevant angesehene Frage zum Gegenstand, ob die beanstandete Surfprotokollierung eine merkliche generalpräventive, abschreckende Wirkung auf „Angreifer“ entfaltet oder nicht. Aus Sicht des Klägers zeigen schon die häufigen Angriffsversuche auf Webserver mit Surfprotokollierung, dass eine abschreckende Wirkung nicht vorhanden ist.

4. Selektive Surfprotokollierung

Nachdem der Beklagtenvertreter bestreitet, dass die IP-Adressen des Klägers von einer Surfprotokollierung ausgenommen werden könnten, präzisiert der Kläger seinen Vortrag dazu wie folgt und stellt ihn unter Protest gegen die Beweislast unter Sachverständigenbeweis:

> *a) Es wäre technisch möglich, dass die Beklagte diejenigen IP-Adressen von einer personenbezogenen Protokollierung der Nutzung ihrer Telemedien ausnimmt, die dem Zugangsanbieter des Klägers (O2/Telefonica) zugewiesen sind. Die Beklagte macht selbst nicht geltend, dass aus diesem Netz die Funktionsfähigkeit ihrer Telemedien gestört werde; vorsorglich wird dies mit Nichtwissen bestritten.*
>
> *b) Es wäre technisch möglich, dass die Beklagte die IP-Adresse nur dann über die Dauer des Nutzungsvorgangs hinaus protokolliert, wenn ein Zugriff einem typischen Angriffsmuster entspricht. Auch auf diese Weise wäre es möglich, das unauffällige und legitime Nutzungsverhalten des Klägers von einer Protokollierung auszunehmen.*
>
> *c) Es wäre technisch möglich, eine Speicherung von IP-Adressen nur im Störungsfall zur Wiederherstellung der Verfügbarkeit des Telemediums vorzunehmen.*

Sollte die Beklagte diesen Vortrag bestreiten, mag ein etwaiger Beweisbeschluss entsprechend ergänzt werden.

Allerdings bleibt es dabei, dass auch ohne solche Differenzierungen und bei vollständigem Verzicht auf eine Protokollierung die Funktionsfähigkeit der Telemedien der Beklagten zu gewährleisten ist, wie die lange Liste der solcherart betriebenen Telemedien der Beklagten zeigt. Dementsprechend hat die Beklagte im Vorprozess selbst zugestehen müssen, dass Angriffe auf die technische Infrastruktur „auch durch andere geeignete Mittel abgewehrt werden können“ (Seite 2 des Schriftsatzes der Beklagten vom 12.12.2006 im Verfahren 5 C 314/06 vor dem Amtsgericht Mitte).

5. Botnetze und Urteil des Oberlandesgerichts Frankfurt am Main

Was das in der mündlichen Verhandlung angesprochene Ziel der „Bekämpfung von Botnetzen“ angeht, fehlt es schon an einem berechtigten Interesse der Beklagten daran. Denn die Funktionsfähigkeit der Telemedien der Beklagten lässt sich trotz bestehender Botnetze durch technische Vorkehrungen gegen Angriffe gewährleisten.

Eine Vorratsspeicherung der Telemediennutzung ist zur „Bekämpfung von Botnetzen“ auch nicht erforderlich. Zur Erkennung infizierter Rechner und Einleitung von Maßnahmen genügt der Einsatz von Fallen („Honeypots“, „Spamtraps“) durch Internet-Zugangsanbieter (Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2011, 10), wie es etwa im Rahmen der sogenannten Anti-Botnetz-Initiative des Verbands der deutschen Internetwirtschaft eco e.V. (*www.botfrei.de*) geschieht. Der Einsatz solcher Fallen erfordert keine Protokollierung der Nutzung der Telemedien der Beklagten.

Allgemein sind die Ausführungen des Oberlandesgerichts Frankfurt am Main mit Urteil vom 28.08.2013 (Az. 13 U 105/07) zu einem Internet-Zugangsanbieter nicht übertragbar auf Telemedienanbieter. In dem dort entschiedenen Fall wollte der Internet-Zugangsanbieter mithilfe von IP-Adressen gegen Missbrauch („Abuse“) seiner eigenen Kunden über sein Netz vorgehen; darum geht es bei der Beklagten nicht. Auch hat der Internet-Zugangsanbieter in jenem Fall bloß gespeichert, wer wann mit welcher IP-Adresse online war und nicht – wie die Beklagte – mit welcher IP-Adresse wann welche Webseite gelesen oder wonach gesucht wurde (Inhalt der Internetnutzung). Die Entscheidung des Oberlandesgerichts Frankfurt am Main ist überdies hinsichtlich der vorgenommenen Abwägung rechtlich unzutreffend. Unter dem Az. 1 BvR 2370/14 ist deswegen eine Verfassungsbeschwerde dagegen anhängig. Es gibt Internet-Zugangsanbieter, die ohne Vorratsspeicherung von IP-Adressen auskommen.

6. Art. 6 DSGVO und Telemediengesetz

Bezüglich der Frage, ob Art. 6 Abs. 1 S. 1 Buchst e) oder f) anzuwenden ist, wird auf die Kommentierung bei Paal/Pauly/Frenzel DS-GVO Art. 6 Rn. 31, beck-online Bezug genommen:

> *„ErwGr 48, 49 nennen auch Unternehmenssachverhalte und IT-Sicherheit, wobei für Behörden Art. 6 Abs. 1 UAbs. 2 gilt.“*

Die Literatur geht also wie der Kläger davon aus, dass die Beklagte im Bereich der Sicherheit ihrer Webserver eine öffentliche Aufgabe wahrnimmt. Der EuGH hat sich wohl nur deshalb auch Buchstabe f) gestützt, weil es bei der Datenschutzrichtlinie auf die Unterscheidung zu Buchstabe e) noch nicht ankam und schon die Vorlagefrage des Bundesgerichtshofs nur Buchstabe f) zum Gegenstand hatte. Nunmehr ist die Unterscheidung relevant, weil bei Buchtstabe e) die Rechtsgrundlage einer Datenverarbeitung durch die Mitgliedsstaaten festgelegt werden müssen (Art. 6 Abs. 3 S. 1 DSGVO) und hier nur das Telemediengesetz als Rechtsgrundlage in Betracht kommt.

Zur Anwendbarkeit des Telemediengesetzes hat die Beklagte auf die Stellungnahme des Deutschen Anwaltvereins durch den Ausschuss Informationsrecht zum Referentenentwurf eines Zweiten Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und

zur Umsetzung der Richtlinie EU 2016/680 verwiesen (*https://anwaltverein.de/de/newsroom/sn-34-18-2-datenschutz-anpassungs-und-umsetzungsgesetz?scope=modal&target=modal_reader_24&file=files/anwaltverein.de/downloads/newsroom/stellungnahmen/2018/dav-sn_34-18-final.pdf*). Selbst diese Stellungnahme, die klägerseits nicht geteilt wird, geht allerdings von einer Fortgeltung des § 15 TMG aus, soweit er die Speicherung von Informationen zum Gegenstand hat, und zudem von der Fortgeltung der Pflicht zur Ermöglichung einer anonymen Nutzung von Telemedien (§ 13 Abs. 6 TMG), auf die sich der Kläger beruft.

7. Drohende Nachteile durch Protokollierung der Internetnutzung

Da sich die Kammer vom Vortrag des Klägers überrascht gezeigt hat, ihm gehe es unabhängig von der Speicherdauer um die Unterbindung jeder personenbezogenen Aufzeichnung seiner (vollkommen legalen) Nutzung öffentlicher Telemedien über die Dauer der Nutzung hinaus, füge ich diesem Schriftsatz Recherchen des NDR über die drohenden schwerwiegenden Folgen im Fall einer Surfprotokollierung bei.

Beweis: Anlage K1 – Kontoauszug des Beklagten aus 2015.

Wenngleich die dort berichtete Surfprotokollierung mithilfe einer Browser-Erweiterung erfolgte, handelt es sich um dieselben Daten wie sie auch die Beklagte bei vielen Telemedien personenbezogen speichert (Nutzungsdaten).

Jede Vorratsspeicherung von Online-Aktivitäten begründet die Gefahr eines Diebstahls oder Missbrauchs hochsensibler Daten, eines falschem Verdachts oder sonstiger Nachteile. Dass die Beklagte die Sicherheit personenbezogener Daten (einschließlich Protokolldaten) nicht fachgerecht gewährleistet, hat der „Bundeshack“ gezeigt. Unter ständiger Aufzeichnung der Online-Aktivitäten ist eine freie und unbefangene Grundrechtsausübung im Netz nicht möglich.

Vorab ist darauf hinzuweisen, dass auf Beweisantritte verzichtet wird, weil die Beklagte beweisbelastet wird. Sollte die Kammer anderer Auffassung sein, wird um einen Hinweis gebeten.

Mit freundlichem Gruß

Jonas Breyer
(Rechtsanwalt)

panorama 3

Stand: 03.11.2016 10:15 Uhr | Archiv - Lesezeit: ca.5 Min.

Nackt im Netz: Millionen Nutzer ausgespäht

Was wir im Internet tun, zeigt, wer wir sind: Einkaufen, Bank-Geschäfte, Reiseplanung oder Porno - alles geschieht online. Multinationale Firmen machen aus diesen Informationen ein Milliardengeschäft. Sie sind in der Lage, jeden Schritt mitzuzeichnen, den User im Internet unternehmen. Diese Informationen verkaufen sie dann in Paketen weiter - angeblich anonymisiert und ohne Schaden für den Nutzer. Recherchen des NDR zeigen indes, wie einfach sich diese Daten konkreten Personen zuordnen lassen und wie umfangreich sie intime Details aus dem Leben der Nutzer preisgeben.

Nackt im Netz: Millionen Nutzer ausgespäht

Panorama 3 - 01.11.2016 21:15 Uhr

Was wir im Internet tun, wird protokolliert. Und über diese Protokolle verfügen Datenhändler und verkaufen sie. Dabei handelt es sich zum Teil um hochsensible Informationen.

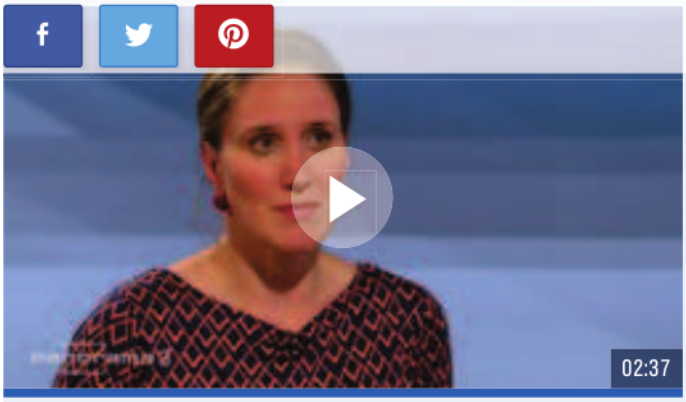
★★★★★

4,43 bei 197 Bewertungen

Informationen zur Sendung

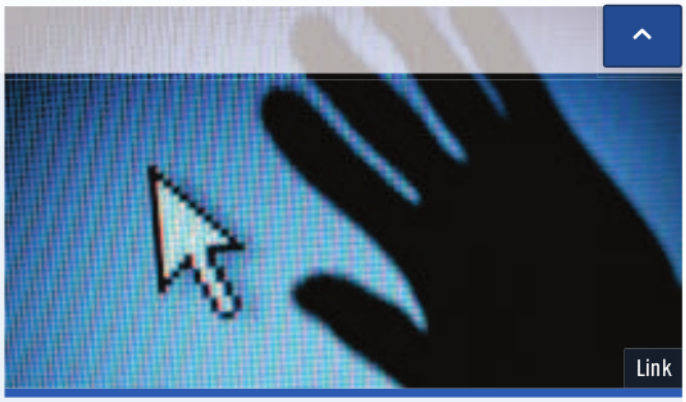
In einer monatelangen Recherche konnten Reporter von Panorama und ZAPP Zugang zu einem umfangreichen Datensatz erlangen und ihn auswerten. Darin enthalten ist jede Bewegung von Millionen von Internet-Nutzern im Monat August. Mit den Daten lässt sich das Leben der User bis in den intimsten Bereich nachzeichnen. In dem Datensatz finden sich neben privaten Nutzern auch Personen des öffentlichen Lebens: Manager, Polizisten, Richter und Journalisten.

HINTERGRUND



Datenhandel: Wie schütze ich mich?

01.11.2016 21:15 Uhr
Panorama 3
Autorin Svea Eckert erläutert im Gespräch mit Susanne Stichler die Gefahren des Datenhandels und sagt, was man dagegen tun kann. Komplette Sicherheit gibt es aber nicht. **Video (02:37 min)**



Hintergrund: Browser-Erweiterungen

Eine der Browser-Erweiterungen, die für das ausspionieren verantwortlich ist, ist "Web of Trust". WOT sammelt mehr Daten als erforderlich - ohne Einwilligung der Nutzer. **extern**

Geheimnisse über Privates und Berufliches

Ihre Web-Verläufe geben intime Geheimnisse aus dem Berufs- und Privatleben preis: Informationen zu laufenden Polizei-Ermittlungen, die Sadomaso-Vorlieben eines Richters, interne Umsatzzahlen eines Medien-Unternehmens und Web-Recherchen zu Krankheiten, Prostituierten und Drogen.


Der Daten-Experte Andreas Dewes ist erschrocken, in welchem Umfang Daten einsehbar sind.

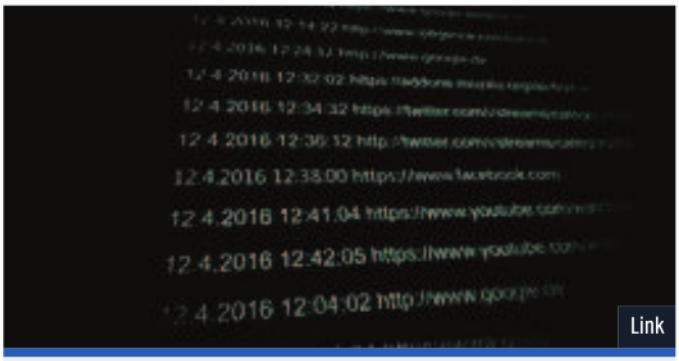
Für Big Data Scientist Andreas Dewes ein Unding. "Für mich war sehr überraschend, wie einfach man einen Großteil der Daten deanonymisieren konnte. Die Privatsphäre des Nutzers wird in keinster Weise respektiert."

Eine zentrale Rolle spielen offenbar kostenlose Zusatzprogramme mit einer versteckten Ausspähfunktion. In den Recherchen des NDR fiel etwa eine Browser-Erweiterung der Firma "Web of Trust" (WOT) auf. WOT bietet eigentlich einen Service an, der dem Nutzer dabei helfen soll, sicher zu surfen: Die Erweiterung prüft die Integrität von Webseiten, bewertet besuchte Seiten anhand eines Ampel-Systems im Hinblick auf Sicherheit.

Im Hintergrund protokolliert und übermittelt die Erweiterung aber auch die Daten zum Surf-Verhalten des Nutzers an einen Server im Ausland. Dort wird ein Profil erstellt, bei dem Datum, Uhrzeit, Ort und angesteuerte Web-Adresse gemeinsam mit einer Nutzer-Kennung abgespeichert werden. Diese Daten gehen dann an Zwischenhändler. Von einem dieser Zwischenhändler haben Panorama und ZAPP ihren Datensatz bezogen.

WEITERE INFORMATIONEN

Daten trotz Anonymisierung personalisierbar



Tipps zum sicheren surfen

Mit gezielten Maßnahmen kann man sich gegen die meisten Daten-Spione schützen. Unser gemeinnütziger Kooperationspartner Mobilsicher.de zeigt, wie es geht. **extern**

Der Hamburgische Datenschutzbeauftrage Johanens Caspar kritisiert das Vorgehen von WOT.

Auf Anfrage teilte WOT mit, in seinen Datenschutzrichtlinien werde darauf hingewiesen, dass bestimmte Daten gesammelt und mit Dritten geteilt werden. WOT unternehme aber große Anstrengungen diese zu anonymisierten. WOT weist auf seiner Webseite darauf hin, dass die Erweiterung Daten wie etwa Web-Adressen abgreift und an Dritte weitergibt. Reporter des NDR konnten in Stichproben mehr als 50 Nutzerinnen und Nutzer persönlich identifizieren, zum Beispiel über E-Mail-Adressen, in denen der Name steht, Anmeldenamen oder andere Bestandteile der aufgerufenen URLs.

Der Datenschutzbeauftrage Hamburgs, Johannes Caspar, kritisisiert das Vorgehen von WOT. "Zur Weitergabe von personenbezogenen Daten brauchen Unternehmen grundsätzlich eine Einwilligung der Betroffenen." Dazu müsse der Nutzer genau wissen, wozu er zustimmt. Dies sei bei WOT nicht der Fall. "Eine massive Auswertung der Daten sei daher nach deutschem Recht "nicht zulässig", so der Datenschützer.

Die Daten lassen Rückschlüsse darauf zu, wann sich einzelne Nutzer wo aufgehalten haben und erlauben so, Bewegungsprofile zu erstellen. Insgesamt umfasst der ausgewertete Datensatz mehr als zehn Milliarden Web-Adressen, aufgerufen von rund drei Millionen Usern aus Deutschland.

Kontoauszüge und Personalausweis im Netz

Wie nackt sich die Nutzer im Netz unfreiwillig darstellen, zeigt das Beispiel eines Managers aus Hamburg. Sein Datensatz beinhaltet unter anderem eine Reihe von Links zu einem Online-Speicher-Dienst, bei dem er Unterlagen zu einem Hausbau abgelegt hat. Jeder, der diese Adressen kennt, kann darüber Kontoauszüge, Architektenzeichnungen, Lohnabrechnungen mit Hinweisen auf das Bonus-System des Arbeitgebers, eine Kopie des Personalausweises und detaillierte Auszüge aus den Unterlagen zu einem Bankkredit abrufen.

Kriminelle könnten Identität kapern

Dabei sind Namen und Anschrift des Managers und seiner Frau ebenso sichtbar wie Telefonnummern und E-Mail-Adressen. Kriminelle könnten mit Hilfe dieser Unterlagen die Identität des Mannes kapern oder ihn mit den Details zu seinem Surf-Verhalten erpressen.

Um an die Informationen zu gelangen, haben die NDR Reporter eine Schein-Firma gegründet, die vorgeblich im "Big Data"-Geschäft aktiv ist. Gleich mehrere Firmen zeigten sich bereit, die Web-Daten

deutscher Internet-Nutzer zu verkaufen - ein Unternehmen bot die nun ausgewerteten Daten schließlich als kostenlose Probe an. Datenpakete wie dieses bieten unzählige Firmen an.

Die meisten Unternehmen betonen in ihren Datenschutzerklärungen, sie würden keine persönlichen Daten erheben, die Rückschlüsse auf die Identität der Nutzer zulassen. Die Recherche von Panorama zeigt, dass sich den Informationen durchaus die betreffenden Personen zuordnen lassen.

Zwischenhändler vertreiben Datenpakete

Die Software-Entwickler agieren indes oft aus dem Ausland, vermittelt werden die Erweiterungen zum Beispiel über Server in den USA. Häufig vertreiben Zwischenhändler dann die großen Datenpakete. Viele kommen aus Israel, einige bedienen sich auch Briefkastenfirmen in notorisch intransparenten Ländern wie Panama oder den Britischen Jungferninseln. Ein Betroffener, der sich in Deutschland juristisch gegen den Verkauf seiner Daten zur Wehr setzen möchte, hat in so einer Konstellation wenig Aussicht auf Erfolg.

Dieses Thema im Programm:
Panorama 3 | 01.11.2016 | 21:15 Uhr

Drucken

Artikel kommentieren

Eintrag 71 bis 74 von 74

Tom schrieb am 08.11.2016 20:00 Uhr:

@Thomas Konrad schrieb am 03.11.2016 21:09 Uhr:
Werter "Namensvetter", schau Dir doch mal bitte folgendes an und bilde Dir ein eigenes Urteil ;-)
https://www.youtube.com/watch?v=6eybE5GVROk

Tom schrieb am 08.11.2016 20:04 Uhr:

@Maria da Silva schrieb am 03.11.2016 22:16 Uhr:
auch für Sie empfehle ich folgendes Video und ein eigenes Urteil für sich bilden ;-)
https://www.youtube.com/watch?v=6eybE5GVROk

p.s.: @Kommentatoren: die letzten beiden Beiträge dürfen natürlich gerne zusammengefasst werden :-)

Sebastian schrieb am 23.04.2017 17:04 Uhr:

Zwei. 2 Kategorien von Browser-Erweiterungen schließe ich aus gründen des Datenschutzes und der Sicherheit aus zu nutzen und rate davon ab:

1. Erweiterungen die Websites auf Phishing oder Malware untersuchen. zB Anti-Phishing- und Anti-Malware-Erweiterungen.
2. Erweiterungen die zum speichern und verwalten von Anmeldedaten (Kontodaten) dienen.

Stand: 03.11.16 10:15 Uhr

Nackt im Netz: Auch intime Details von Bundespolitikern im Handel

von Svea Eckert, Jasmin Klofta & Jan Lukas Strozyk

Vertrauen ist für Politiker ein hohes Gut: im Gespräch mit Bürgern, bei der Vorbereitung von Sitzungen und im Umgang mit Interessengruppen. Was aber, wenn alle Informationen zur Themen-Recherche, zu Reisen, zu Gesprächspartnern offen im Internet zum Kauf angeboten werden? Nach Recherchen von Panorama wurden Bundespolitiker durch Browser-Erweiterungen ausgespäht. Das kann sie angreifbar machen und ihre politische Arbeit behindern.

Nackt im Netz: Intime Details von Politikern im Handel
Panorama Recherchen zeigen, wie Nutzer durch Browser-Addons ausgespäht werden. Bei Politikern kann dies ihre Unabhängigkeit bedrohen. Die Datenspur führt bis ins Bundeskanzleramt.

"Man wird erpressbar"

Was das konkret bedeutet, zeigt der Fall

ZUM SEITENANFANG

Valerie Wilms fühlt sich ausgeforscht.

von Valerie Wilms, Bundestagsabgeordnete der Grünen aus Pinneberg in Schleswig-Holstein. Die Browser-Daten zeigen Reiseverläufe von Wilms, geben Hinweise auf ihre Steuerdaten und lassen Einblicke in ihre politische Arbeit zu: "Natürlich kann es schaden. Man wird damit durchaus erpressbar", sagt Wilms in Panorama. Sie fühle sich "nackt demjenigen gegenüber, der die Daten hat", so Wilms weiter.

Informationen von Vertrauten der Kanzlerin

In den Daten tauchen auch Politiker auf, die in hochsensiblen Bereichen arbeiten: Helge Braun zum Beispiel. Der CDU-Mann ist Staatsminister bei der Bundeskanzlerin. Er gilt als Vertrauter von Angela Merkel. Über den Computer eines seiner Mitarbeiter sind Brauns Informationen in den Datensatz gelangt. Den Politiker überrascht vor allem, "dass es oftmals ungeachtet der Unzulässigkeit des Datenabflusses schwierig ist, als Anwender diesen überhaupt nachzuvollziehen", wie Braun auf Panorama-Anfrage sagt.

"Dann müssen Gesetze her"

Will im Zweifelsfall mit Gesetzen gegen die Datenhändler vorgehen: Lars Klingbeil.

Betroffen zeigt sich auch Lars Klingbeil, netzpolitischer Sprecher der SPD aus Niedersachsen. Sein Name taucht in dem ausgewerteten Datensatz ebenfalls auf. Auch bei ihm führt die Spur zum Rechner eines Mitarbeiters. "Ich habe nicht gewusst, dass solche Sachen identifizierbar sind. Vielleicht ist man da naiv an der Stelle, aber da braucht man auf jeden Fall Aufklärung darüber, welche Daten eigentlich erhoben werden und was mit den Daten dann passiert", sagt er Panorama. Wenn sich herausstelle, dass man den Firmen nicht einfach vertrauen könne, "dann müssen Gesetze her", so Klingbeil.

Viele Politiker unter den Ausgeforschten

Im Datensatz finden sich die Namen weiterer Politiker aus ganz Deutschland: Der Mecklenburger Frank Junge (SPD), im Finanzausschuss für den Haushalt der Bundesrepublik verantwortlich. Oder Waltraud Wolff aus Sachsen-Anhalt, die im Fraktionsvorstand der SPD ist und die Brandenburger Abgeordnete Annalena Baerbock (Grüne), Mitglied im Wirtschaftsausschuss. Der Europaparlamentarier Martin Häusling, ebenfalls von den Datensammlern bloßgestellt,

reagiert geschockt: "Aus sowas kann ja jeder ablesen, an was ich arbeite, wo ich selber Recherchen mache, mit wem ich mich treffe."

Menschen, die Häusling oder den anderen Abgeordneten politisch schaden wollen, könnten mit Hilfe dieser Daten Informanten und Gesprächspartner enttarnen und ihre Strategien nachvollziehen - und damit deren Arbeit sabotieren. "Wir brauchen als Abgeordnete Vertrauensschutz“, so Häusling.

Daten einer Tarnfirma angeboten

Um an die Informationen zu gelangen, hatten die NDR-Reporter eine Schein-Firma gegründet, die vorgeblich im "Big Data"-Geschäft aktiv ist. Gleich mehrere Unternehmen zeigten sich bereit, die Web-Daten deutscher Internet-Nutzer verkaufen zu wollen - ein Unternehmen bot die nun ausgewerteten Daten schließlich als kostenlosen Probe-Datensatz an.

SO KÖNNEN SIE SICH SCHÜTZEN

Tipps zum sicheren surfen

Mit gezielten Maßnahmen kann man sich gegen die meisten Daten-Spione schützen. Unser gemeinnütziger Kooperationspartner Mobilsicher.de zeigt, wie es geht. | **extern**

Hintergrund: Browser-Erweiterungen

Eine der Browser-Erweiterungen, die für das ausspionieren verantwortlich ist, ist "Web of Trust". WOT sammelt mehr Daten als erforderlich - ohne Einwilligung der Nutzer. | **extern**

Browser-Erweiterungen verantwortlich

Allem Anschein nach wurden sie über Browser-Erweiterungen, sogenannte Addons, erhoben: Diese kleinen Zusatz-Programme dienen sich als praktische Helfer an. Doch einmal installiert, übermitteln sie im Hintergrund alle besuchten Seiten eines Nutzers an einen Server, wo die Daten zu Nutzerprofilen gebündelt werden.

"Web of Trust" gibt Daten weiter

Durch Stichproben konnte Panorama eine dieser Erweiterungen ausmachen. Es handelt sich um das Programm "Web of Trust", kurz WOT. Die Erweiterung prüft die Integrität von Webseiten - eine nützliche Funktion, die dem Nutzer ein sicheres Surfen garantieren soll. Gleichzeitig übermittelt die Software offenbar im Hintergrund die Adresse jeder besuchten Seite an einen Server, wo die Daten ohne Wissen des Nutzers gespeichert und weiterverarbeitet werden. WOT ist mutmaßlich nur eine von zahlreichen Erweiterungen, die so agieren und für einen steten Datenstrom bei den Zwischenhändlern sorgen.

Auf Anfrage teilte WOT mit, in seinen Datenschutzrichtlinien werde darauf hingewiesen, dass bestimmte Daten gesammelt und mit

Dritten geteilt werden. WOT unternehme aber große Anstrengungen diese zu anonymisierten. In den Nutzungsbedingungen listet das Unternehmen zwar klar auf, dass Daten des Nutzers wie Ort, Datum, Zeit und Webadresse abgegriffen werden. Nutzer stimmen diesen Bedingungen stillschweigend zu. Allerdings betont das Unternehmen, dass es sich dabei um anonyme, nicht personenbezogene Daten handle. Über Methode und Grad der Anonymisierung schweigt die Firma.

Auswertung rechtlich nicht zulässig

Für Datenschützer Johannes Caspar ist die Auswertung der Daten in Deutschland verboten.

Der Hamburgische Datenschutzbeauftragte Johannes Caspar kritisiert das Geschäftsmodell von WOT: "Zur Weitergabe von personenbezogenen Daten brauchen Unternehmen grundsätzlich eine Einwilligung der Betroffenen - die liegt aber nicht vor. Die Bezeichnung 'anonymisiert' ist hier nicht richtig“, erklärt Caspar weiter, eine massive Auswertung der Daten sei daher nach deutschem Recht "nicht zulässig“.

Dieses Thema im Programm:
Das Erste | Panorama | 03.11.2016 | 21:45 Uhr