Paul-Olivier Dehaye
aus dem Englischen von Birgit Ahlmann, Nils Erik Flick und Eberhard Zehendner, mit einem Nachwort von Nils Erik Flick

Wie ich einen Blick auf die persönlichen Daten werfen durfte, die ein milliardenschweres Unternehmen über mich besitzt

Turn, Inc. *ist ein* Retargeting*-Unternehmen. Es sammelt Online-Datenspuren und nutzt diese Information, um das Privileg zu versteigern, Ihnen Werbeanzeigen einzublenden. Neben anderen Techniken verwendet es Browsercookies und* Canvas*-Fingerprinting*[1]*, um Ihren Browser – und damit letztlich sogar Ihre Identität – eindeutig zu identifizieren.*

Das Safe-Harbor-Abkommen[2] gibt allen Bürgern und Einwohnern der EU das Recht, die eigenen persönlichen Daten bei Unternehmen wie *Turn* einzusehen.[3] Im April 2015 bat ich *Turns* damaligen Anwalt Max Ochoa[4] (erreichbar über *privacy@turn.com*), mir alle Daten zu übermitteln, die bei *Turn* vorgehalten werden und zu meinen Gerätekennungen (etwa Cookies und Apple-Werbekennungen,[5] siehe unten) gehören. *Turn* stellte sich zunächst gegen dieses Ansinnen, gab aber schnell nach, als ich es zu verklagen begann. Damit sollte es jetzt jede.r leichter haben, an die eigenen Daten zu kommen. Weiter unten erkläre ich, wie es gemacht wird.

Anfängliche Anfragen per E-Mail

Obwohl er mir versicherte, *Turn* nähme die Privatsphäre von Verbrauchern ernst, erhob Ochoa drei Einwände, um *Turns* gesetzlichen Verpflichtungen nicht nachkommen zu müssen.

Sein erster Einwand war im Grunde eine Irreführung: „*Turn* liefert maßgeschneiderte Werbung unter Verwendung ausschließlich nicht persönlich identifizierbarer Information und sammelt keine persönlich identifizierbare Information (PII) als Teil dieses Prozesses." Das Konzept der persönlich identifizierbaren Information entspringt der US-Gesetzgebung und soll Identifizierendes von Nichtidentifizierendem sauber abgrenzen; es ist zudem branchenspezifisch zu interpretieren. Eigentlich war der Begriff bereits überholt, als er ins Gesetz geschrieben wurde. Er wies Anwälten und Technologie-Experten nämlich, so wie sich die Technologie entwickelte, einen sicheren Weg, die im Gesetz festgelegten Schranken zu umgehen: Cookies sind im Web bessere Identifikationsmerkmale als die meisten Vor- und Nachnamenskombinationen. Aus europäischer Sicht ist das Konzept ohnehin reine Fiktion, da die EU-Bestimmungen zum Schutz persönlicher Daten keine bestimmten Identifizierungsmethoden angeben.

Ochoas zweite Abwehr bestand darin, mir anzubieten, aus *Turns* Tracking durch ein Opt-out auszusteigen. Natürlich habe ich nicht angebissen.

Seine dritte Antwort war, *Turn* könne nicht sicher sein, dass die Kennung mir gehöre. Ich bot viele Wege an nachzuweisen, dass ich tatsächlich Besitzer dieser Geräte war: ein Bild mit meinem Gesicht nahe der Geräte, Originalrechnungen, sogar Tausende von Meilen bis zu *Turns* Büros in Redwood City zu reisen (ich plante ohnehin einen Trip in die Bay Area). Nichts davon verfing.

Schließlich kündigte ich Ochoa im September 2015 meinen nächsten Schritt an: eine formale Beschwerde. Er antwortete mir ziemlich zuversichtlich:

> *Paul-Olivier, es ist natürlich Ihr gutes Recht, das zu tun. Aber wie bereits erklärt haben wir, wenn uns eine Person eine Kennung schickt, keine Möglichkeit zu validieren, dass diese von einem Gerät dieser Person kommt. Es könnte eine nicht rechtmäßig erlangte Kennung von einem anderen Gerät sein. Wir berücksichtigen daher nur Anfragen von Strafverfolgungsbehörden gemäß einem gültigen Gerichtsbeschluss. Viele Grüße, Max*[6]

Ich muss zugeben, dass ich ein wenig schockiert war. Ochoa deutete damit an, dass ich ein Dieb sein könnte, und dass *Turn* lieber mit Strafverfolgungsbehörden zusammenarbeitet als einen Ausgleich für seine Fähigkeiten zur Datensammlung zu schaffen, etwa durch Bemühungen um Transparenz.

Ist *Turn* noch an *Safe Harbor* gebunden?

Ende September 2015 reichte ich meine Beschwerde beim *Better Business Bureau* ein.[7] Das ist ein privates Schiedsgericht, das von *Turn* beauftragt ist, derartige Beschwerden zu klären. Dieses Verfahren ist für Privatpersonen kostenfrei (*Turn* bezahlt) und stellt die erste Instanz im Rahmen der vom Safe-Harbor-Abkommen vorgesehenen Selbstregulierung dar.

Am 6. Oktober 2015 erklärte der Europäische Gerichtshof (EuGH) im Zuge eines von dem österreichischen Staatsbürger Max Schrems angestrengten Verfahrens[8] die Entscheidung der EU-Kommission für ungültig, der rechtliche Rahmen von Safe Harbor böte den glei-

Paul-Olivier Dehaye

Paul-Olivier Dehaye, SNSF (Swiss National Science Foundation) Professor am Institut für Mathematik der Universität Zürich, publizierte den englischen Originaltext dieses Beitrags in seinem Blog.[16]

chen Schutz wie EU-Datenschutzbestimmungen.[9] Dies störte erst einmal den Vorgang, den ich gerade angestoßen hatte: das *Better Business Bureau* schien willens, die Sache völlig fallenzulassen.

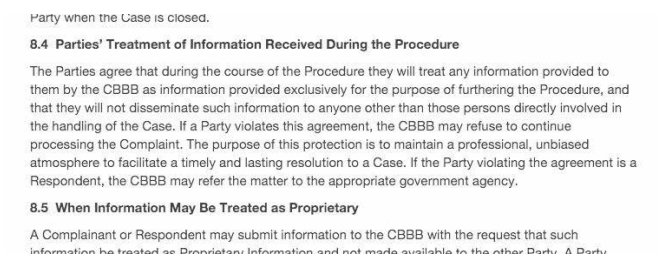
Allerdings müssen Privatunternehmen auf US-Seite im Rahmen von Safe Harbor jährlich Verpflichtungen gegenüber ihren Kunden eingehen. Die EU-Entscheidung hat daran nichts geändert, und entsprechend kündigte die FTC (Federal Trade Commission)[10] auf ihrer Website die Fortsetzung des Programmvollzugs an. Als ich darauf hinwies, erklärte sich das *Better Business Bureau* nach ein paar Wochen bereit, ein Verfahren zu eröffnen.

Das *Safe-Harbor*-Verfahren gegen *Turn*

Sobald das Verfahren erst einmal ernsthaft in Gang gekommen war, erwies sich der Mediator als äußerst professionell. Es wurde sehr schnell klar, dass *Turn* rechtlich keinen guten Stand hatte. *Turn* fragte an, ob ich bereit sei, eine eidesstattliche Erklärung zu unterzeichnen, der gemäß mir die Geräte gehörten, deren Kennungen ich ihnen geschickt hatte. Ich stimmte bereitwillig zu (rückblickend wäre es natürlich geschickter gewesen, diesen Schritt bereits vor Monaten selbst zu unternehmen). Als *Turn* die Erklärung übersandt hatte, zeigte sich, dass sie eine zusätzliche Klausel eingebaut hatten:

> *Gemäß den Regeln des vom Council of Better Business Bureaus, Inc., verwalteten Better-Business-Bureau-EU-Safe-Harbor-Streitbeilegungsverfahrens stimme ich zu, die Existenz dieser Erklärung und jegliche Information, die ich von Turn Inc. bezogen auf [meine] Kennungen erhalte, vertraulich zu behandeln.*

Die Verfahrensregeln des *Council of Better Business Bureau*s enthalten aber keine derartige Klausel.[11] Sie verlangen von den Teilnehmern lediglich, ein laufendes Verfahren vertraulich zu behandeln. Ich schickte postwendend eine Antwort, in der ich anmahnte, dies würde mehrere meiner anderen Grundrechte (Recht auf ein faires und öffentliches Verfahren, etc.) verletzen, und unterschrieb die Erklärung einfach, nachdem ich die zusätzliche Klausel durchgestrichen hatte. Scheint geklappt zu haben.



Party when the Case is closed.

8.4 Parties' Treatment of Information Received During the Procedure

The Parties agree that during the course of the Procedure they will treat any information provided to them by the CBBB as information provided exclusively for the purpose of furthering the Procedure, and that they will not disseminate such information to anyone other than those persons directly involved in the handling of the Case. If a Party violates this agreement, the CBBB may refuse to continue processing the Complaint. The purpose of this protection is to maintain a professional, unbiased atmosphere to facilitate a timely and lasting resolution to a Case. If the Party violating the agreement is a Respondent, the CBBB may refer the matter to the appropriate government agency.

8.5 When Information May Be Treated as Proprietary

A Complainant or Respondent may submit information to the CBBB with the request that such information be treated as Proprietary Information and not made available to the other Party. A Party

Nach einigen weiteren Wochen (!) Wartezeit erhielt ich schließlich im Januar 2016 Einblick in meine persönlichen Daten. Also? Was war das große Geheimnis? Eigentlich nicht viel … *Turn* hat Verträge mit mindestens einem der Unternehmen *Le Figaro*, *Huffington Post*, *Scout24.ch* und *AfriZap* (die Datenflüsse zwischen diesen sind nicht klar, aber ich werde *Turn* um zusätzliche Erläuterungen bitten). Ich scheine einige Male auf diesen Websites auf *Clickbaits* hereingefallen zu sein, einmal auf meiner Arbeitsstelle. Alles in allem nicht weltbewegend. Aber nachdem ich *Turn* zur Herausgabe meiner Daten veranlasst habe, kann nun jeder dasselbe tun – und sollte es dabei leichter haben. Ich ermutige Sie, dies auch zu tun. Wer weiß, vielleicht wird *Turn* später einmal dem Beispiel seines Konkurrenten *Criteo* folgen, der solche Anfragen sehr viel leichter zu machen versucht.[12]

Wie man *Turn* um seine persönlichen Daten bittet

Muster-Schreiben (Originalfassung, da für die USA bestimmt)

Affidavit of ownership of identifiers

I, XXXXXX, hereby solemnly affirm and certify under penalty of perjury as follows:

1. I am citizen of EUROPEAN COUNTRY, and I currently reside in WHEREVER. [Nur eines von beiden braucht ein EU-Land (oder die Schweiz) zu sein.]

2. I am the owner and controller of Apple mobile devices associated with the following Identifiers for Advertisers ("IDFAs"): [Auflisten, siehe unten.]

3. I am the owner and controller of Android mobile devices associated with the following Google Advertising IDs: [Auflisten, siehe unten.]

4. I am the owner and controller of computers running web browsers associated with the following "uid" cookie values set by the turn.com domain: [Auflisten.]

I solemnly affirm and certify under penalty of perjury that the foregoing is true and correct.

DATE – NAME – SIGNATURE

1. Legen Sie eine Sammlung möglichst vieler Ihrer persönlichen Kennungen an: Ihre *turn.com*-Browsercookies (das ist nicht schwer, suchen Sie im Web nach einer Anleitung für Ihren Browser), IDFAs unter iOS (siehe unten),[5] Google Advertising IDs unter Android (siehe unten). Jede dieser Kennungen sollte eine lange alphanumerische Zeichenkette sein.

2. Unterschreiben Sie eine eidesstattliche Erklärung, dass diese Bezeichner zu Ihren Geräten gehören, und scannen Sie sie ein (siehe oben stehendes Muster).

3. Schicken Sie eine E-Mail mit der ausdrücklichen Bitte um die zu diesen Kennungen gehörenden Daten an *privacy@turn.com*, und fügen Sie den Scan eines amtlichen Ausweises und Ihre eidesstattliche Erklärung bei.

4. Erinnern Sie *Turn* ggf. nach 30 Tagen an seine Verpflichtungen.

5. Hoffentlich hat *Turn* jetzt seine Lektion gelernt und ist seiner Auskunftspflicht nachgekommen. Wenn nicht, legen Sie Beschwerde beim *Better Business Bureau*[13] oder bei der *FTC*[14] ein (denn in diesem Fall liegt augenscheinlich fortgesetztes pflichtwidriges Verhalten vor).

Tipps für die Praxis

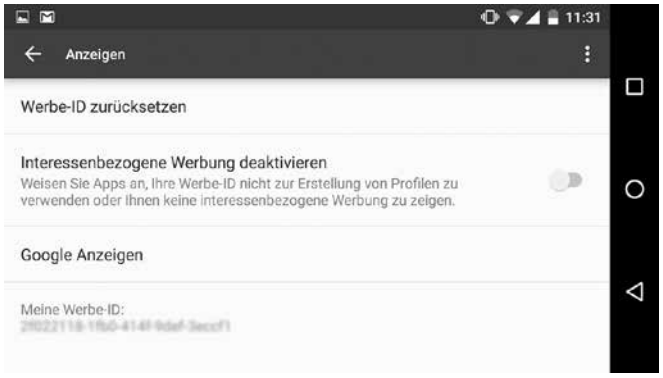
IDFAs ermitteln (iOS)

Installieren Sie die Anwendung „The Identifiers“[15] und schauen Sie unter „Advertising identifier“ nach. (Falls Sie eine bessere Lösung kennen, teilen Sie mir diese bitte mit.)

Google Advertising ID ermitteln (Android)

Schauen Sie auf Ihrem Android-Gerät unter „Google Settings“ > „Ads“ > „Your advertising ID“ nach.

[Deutsche Variante: „Google Einstellungen“ > „Anzeigen“ > „Meine Werbe-ID“]



Die Standard-Einstellungen bei Android 6.0.1

Anmerkungen

1 *https://en.wikipedia.org/wiki/Canvas_fingerprinting*
2 *https://en.wikipedia.org/wiki/International_Safe_Harbor_Privacy_Principles*
3 *https://github.com/pdehaye/safe-harbor*
4 *https://www.crunchbase.com/person/max-ochoa%23/entity*
5 *https://apsalar.com/blog/2015/06/all-about-idfa/*
6 *Anmerkung: Im Original ist die Rede von “requests from law enforcement authorities pursuant to valid subpoenas”. Eine subpoena zwingt im US-Recht eine Person, vor Gericht zu erscheinen und Auskünfte oder Beweismittel herauszugeben. Diese (echte oder juristische) Person braucht nicht Zeuge zu sein.*
7 *https://www.auto.bbb.org/EU-Safe-Harbor-Complaint-Form/*
8 *http://schrems.eu*
9 *https://europeanlawblog.eu/?p=2931*
10 *https://safeharbor.export.gov/list.aspx*
11 *http://www.bbb.org/council/eusafeharbor/about/rules/*
12 *http://info.criteo.com/mycriteoid*
13 *http://www.bbb.org/council/eusafeharbor/bbb-eu-safe-harbor-dispute-resolution-program/*
14 *https://www.ftc.gov/faq/consumer-protection/submit-consumer-complaint-ftc*
15 *https://itunes.apple.com/us/app/the-identifiers/id564618183*
16 *Paul-Olivier Dehaye: How I peeked at the personal data a billion dollar company holds about me. https://medium.com/@pdehaye/how-i-peeked-at-the-personal-data-a-billion-dollar-company-holds-about-me-61a446642cd9 (Stand: 19.01.2016)*

Nachwort von Nils Erik Flick

Soweit der Erfahrungsbericht von Paul-Olivier Dehaye. Das Vorhandensein von Menüpunkten wie „Advertising ID“ bringt eines auf den Punkt: Das Problem sind nicht allein opportunistische Datensammler, sondern auch schädliche Default-Einstellungen und ausspähungsfördernde Mechanismen in den Systemen, die wir mehrheitlich nutzen. Das Problem betrifft uns jedoch alle, unabhängig von der Computernutzung – der entfesselte Überwachungskapitalismus lässt sich nicht auf das Web beschränken, sondern dringt durch die Digitalisierung des Alltags mehr und mehr in Bereiche vor, in denen selbst wachsamste Verbraucher.innen schutzlos sind.

Das Recht bleibt hinter dieser rasanten Entwicklung zurück, auch weil die einzelnen Angriffe auf die informationelle Selbstbestimmung unterschwellig oder diffus sind und daher zu wenige Beschwerden aufkommen – und sicher auch, weil man eine milliardenschwere Industrie nicht abwürgen mag, so unmoralisch sie auch sein mag: *Datenreichtum*.

Das Ironische und Traurige an den existierenden Auskunftsrechten ist: Wer Unternehmen damit Arbeit und Kosten machen will, muss selbst Zeit und Mühe investieren. Wer Datenschutz einfordern will, muss erst einmal bestätigen, dass die Daten richtig sind, und er oder sie stellt damit den Personenbezug erst her (und muss diese sensiblen Daten, die es eigentlich zu schützen galt, womöglich unverschlüsselt übermitteln). Ein Schelm, wer einen *Catch-22*[1] darin wittert! Ähnliches gilt bei dem theoretisch vom Bundesdatenschutzgesetz zugesicherten Recht, sogar Videoaufnahmen aus privaten Überwachungskameras anfordern zu können, auf denen man zu sehen ist – nach §34 besteht theoretisch ein derart weitreichendes Auskunftsrecht. Doch eine Mitarbeiterin eines Landesdatenschutzamtes deutete mir gegenüber an, ich müsse dem Unternehmen unter Umständen ein Foto zukommen lassen. Na toll!

Trotzdem ist das Schaffen einer Gegentransparenz eine nicht gering zu schätzende Taktik in der Bekämpfung des Daten-Kapitalismus. Wer ein genaues Bild von den Mitteln der Industrie – sowie detaillierte und verbriefte Antworten – hat, kann besser dagegen vorgehen.

Anmerkungen

1 *Catch 22, also Falle 22 oder Trick 22 – das ist die ebenso irrsinnige wie ausweglose Dienstanweisung für das amerikanische Bombengeschwader, der zufolge Bomberpilot Yossarian nur dann von weiteren Einsätzen verschont bleibt, wenn er als verrückt anerkannt wird. Roman von Joseph Heller, 1955*

Nils Erik Flick *ist Doktorand in der Informatik an der Carl von Ossietzky Universität Oldenburg und seit 2011 FIfF-Mitglied. Seine Forschungsschwerpunkte sind Software-Verifikation und formale Sprachen, seine Interessengebiete u. a. Computer-Sicherheit und Kryptologie.*
Kontakt: flick@informatik.uni-oldenburg.de