Tracking beim Onlinebanking

Eine Studie von Dr. Sam Macbeth, <sam@cliqz.com>

Cliqz GmbH, https://cliqz.com

July 15, 2016

1 Einleitung

Dass Webseiten die Dienstleistungen von Drittanbietern nutzen, um detaillierte Daten und Statistiken über ihre Nutzer zu bekommen, ist inzwischen ein etablierter Vorgang. Das hat im Internet ein unsichtbares Geschäft entstehen lassen, auf der beim Besuch der Webseite dutzende Firmen dazu eingeladen sind, zu sehen, wer der Nutzer ist und was er sich gerade ansieht [8, 3]. Auf welchen Webseiten diese Werkzeuge auftauchen, wer dahinter steckt und welche Daten die Drittanbieter sammeln, kann man nur mit speziellen Browser-Extensions sehen [1, 4].

Die Betreiber von Webseiten geben diesen Drittanbietern einen Vertrauensvorschuss, wenn sie deren Dienste zu ihrer Website hinzufügen. Denn wenn eine Javascript-Datei eines Drittanbieters auf die Seite geladen wird, so gibt der Webseiten-Besitzer diesem Anbieter die Möglichkeit, die Seite nach dessen Wünschen umzugestalten, sowie jeglichen User-Input abzufangen, komplett andere Skripts zu laden oder sogar selbst wiederum Drittanbieter auf die Seite zu holen, wie es ihnen beliebt. Wenn Bilder von Drittanbietern auf einer Seite angezeigt werden, so ist es diesen Drittanbietern möglich, die Seite zu erkennen, die ein User gerade besucht (über den `Referer`-Header) sowie die IP-Adresse zu lesen. Auch wäre es ihnen möglich, den Browser-User mithilfe von Cookies weiter zu verfolgen [2].

Die Entscheidung, wem man diesen Vertrauensvorschuss gewährt, ist gerade im Bereich des Online-Bankings besonders kritisch. Neben den hohen Sicherheitsanforderungen spielt auch das Thema Privatsphäre eine Rolle. Wer möchte schon, dass seine Bank sensible Informationen über Einkommen und Zahlungen mit Dritten teilt? Um dem Thema Dienstleistungen von Drittanbietern in Online-Banking-Portalen auf den Grund zu gehen, stellen wir diese Studie vor. Es wird anhand von Stichproben untersucht, wo Drittanbieter auf Online-Landing-Pages von deutschen Banken vorkommen, welche Daten sie erhalten können und wer diese Drittanbieter sind. Damit können wir im Anschluss auch auf die Folgen für die Privatsphäre und Sicherheit eingehen.

Diese Studie ist wie folgt strukturiert: In Abschnitt zwei beschreiben wir unsere Studien-Methodologie, in Abschnitt drei die Studienergebnisse und dann evaluieren und diskutieren wir diese in Abschnitt vier. Abschließend fassen wir unsere Ergebnisse in Abschnitt fünf zusammen.

2 Methodik

Die Onlinebanking-Portale der einzelnen Banken wurden aufgerufen und die Abfragen, die auf der Login-Seite, der Onlinebanking-Seite nach erfolgtem Login sowie der Logout-Seite an Dritte übertragen werden, aufgezeichnet. An jeder der so getesteten Stellen hat das Tracking andere Auswirkungen auf Datenschutz und Sicherheit:

- Login-Seite: Tracking-Daten über Besuche der Login-Seite liefern einen starken Hinweis darauf, dass der Nutzer über ein Konto bei dieser Bank verfügt. In den meisten Fällen ist das Onlinebanking-Portal von der eigentlichen Haupt-Website der Bank getrennt, sodass Benutzer, die sich nicht in ihr Konto einloggen wollen, diese Seite kaum aufrufen werden. Darüber hinaus ist es jedem Dritten, der die Erlaubnis hat, JavaScript im Login-Dokument zu laden möglich, die auf dieser Seite eingegebenen Login-Daten der Nutzer auszulesen.
- Nach erfolgtem Login: Tracking an dieser Stelle identifiziert den Nutzer als Kunden der Bank und legt Informationen über abgewickelte Bankgeschäfte, wie beispielsweise Überweisungen oder Kredite offen, wenn solche Informationen aus der URL der Seite abgeleitet werden können. Auch

hier ist JavaScript von Drittanbietern, das in diesen Seiten geladen wird, in der Lage, alle angezeigten Daten auslesen sowie die eingegebenen Daten zu manipulieren.

- Nach erfolgtem Logout: Tracking an dieser Stelle identifiziert den Nutzer als Kunden der Bank, da Nutzer nur dann, wenn sie sich aus einer gültig angemeldeten Sitzung abmelden, auf dieser Seite landen. Es ist unwahrscheinlich, dass auf der Logout-Seite private Nutzerdaten angezeigt werden, sodass JavaScript von Dritten an dieser Stelle ein geringeres Datenschutz- und Sicherheitsrisiko darstellt.

Folgendes untersuchten wir im Einzelnen:

- Art des Aufrufs: *JavaScript* oder *Tracking-Pixel*
- Ladekontext: *Hauptdokument (Main)* oder *iFrame*
- Verwendetes Tracking: *Cookie* und/oder *Fingerprint*

Wie bereits erwähnt, führen JavaScript-Aufrufe zu zusätzlichen Sicherheits- und Datenschutzproblemen, wenn dieser Code auch im Kontext des Hauptdokuments geladen wird. Inhalt, der in einem iFrame-Kontext geladen wird ist besser geschützt, da es sich hier um eine Sandbox-Umgebung handelt. Die Tracking-Methode gibt Aufschluss darüber, wie persistent die Tracking-ID ist.

Folgende Banken wurden untersucht:

- ComDirect – `https://kunde.comdirect.de/lp/wt/login`
- Commerzbank – `https://kunden.commerzbank.de/lp/login`
- Consorsbank – `https://www.consorsbank.de/home`
- DAB-Bank – `https://www.dab-bank.de`
- Deutsche Bank – `https://meine.deutsche-bank.de/trxm/db/`
- DKB – `https://www.dkb.de/banking`
- Hypovereinsbank – `https://my.hypovereinsbank.de/login`
- ING DiBa – `https://banking.ing-diba.de/app/login`
- Number26 – `https://my.number26.de`
- Postbank – `https://banking.postbank.de/rai/login`
- Stadtsparkasse München – `https://homebanking.sskm.de/portal/portal/Starten`
- Volksbank Mittelhessen – `https://www.vb-mittelhessen.de`

Die Websites wurden am 7. und 8. Juli 2016 besucht. Die Logins für die untersuchten Banken wurden von Freiwilligen der Cliqz GmbH zur Verfügung gestellt.

3 Ergebnis

Die Onlinebanking-Portale verschiedener deutscher Banken wurden aufgerufen und Daten wie im vorstehenden Abschnitt beschrieben erhoben. Die Ergebnisse für die einzelnen Stellen, an denen Tracking eingesetzt wird, sind in den Tabellen 1, 2 und 3 zusammengefasst.

Bank	Dritte	Typ	Context	Tracking
Commerzbank	keine			
HypoVereinsBank	keine			
PostBank	keine			
Stadtsparkasse	keine			
ING DiBa	keine			
DAB-Bank	keine			
Volksbank	keine			
Deutsche Bank	`seal.verisign.com`	JS	Main	C
ComDirect	`track.adform.net`	Pixel	Main	C
Consorsbank	`eu.ntrsupport.com`	JS	iFrame	C
DKB	`seal.verisign.com`	JS	Main	C
	`seal.websecurity.norton.com`	Pixel	Main	—
	`webtrekk.net`	Pixel	Main	C + FP
Number26	`connect.facebook.net`	JS	Main	—
	`www.google-analytics.com`	Pixel	Main	FP
	`cc-collector.tech26.de`	Pixel	Main	FP
	`cloudfront.net`	JS	Main	—
	`usage.trackjs.com`	Pixel	Main	—
	`doubleclick.net`	Pixel	Main	C + FP
	`google.com`	Pixel	Main	C + FP

„C“ steht für Cookie, „FP“ für Fingerprint.

Tabelle 1: Drittanbieter auf der Login-Seite.

Tabelle 1 zeigt, dass die meisten Banken auf ihrer Login-Seite keine Dienste Dritter nutzen. Von denjenigen, die dies tun,

- zeigen Deutsche Bank und DKB ein Sicherheitssiegel von Verisign. Dieses Siegel wird erzeugt, indem JavaScript eines Dritten in der Seite geladen wird. Dieses Skript wird über ein Cookie bedient und nicht zwischengespeichert, sodass Verisign jedesmal, wenn ein Nutzer diese Seiten aufruft, informiert wird und jeden einzelnen Zugriff einem einzelnen Nutzer zuordnen kann.
- haben ComDirekt und DKB ein Tracking-Pixel der Anbieter Adform bzw. Webtrekk in ihre Login-Seite eingebunden. Diese setzen Cookies sowie Browser-Fingerprinting ein, um Nutzer, die

auf diese Seite zugreifen, zu verfolgen.

- hat Consorsbank ein Chat-Support-Widget in einem iFrame eingebunden. Die Nutzung des iFrames verhindert, dass der Drittanbieter auf private Daten auf der Seite zugreift; die Nutzung des Cookies würde es ihm jedoch gestatten, Nutzer, die diesen Dienst auf anderen Seiten nutzen, zu verfolgen.
- lädt Number26 in seiner Seite JavaScripts mehrerer Dritter wie Facebook, Google und TrackJS, die anschließend Tracking-Daten an den jeweiligen Dritten übertragen.

Bank	Dritte	Typ	Context	Tracking
Commerzbank	keine			
HypoVereinsBank	keine			
PostBank	keine			
Stadtsparkasse	keine			
ING DiBa	keine			
DAB-Bank	keine			
Volksbank	keine			
Deutsche Bank	keine			
ComDirect	keine			
Consorsbank	`eu.ntrsupport.com`	JS	iFrame	C
DKB	`seal.verisign.com`	JS	Main	C
	`seal.websecurity.norton.com`	Pixel	Main	—
Number26	`connect.facebook.com`	JS	Main	—
	`www.google-analytics.com`	Pixel	Main	FP
	`cc-collector.tech26.de`	Pixel	Main	FP
	`cloudfront.net`	JS	Main	—
	`usage.trackjs.com`	Pixel	Main	—
	`doubleclick.net`	Pixel	Main	C
	`www.google.com`	Pixel	Main	C
	`www.facebook.com`	Pixel	Main	C
	`livechatinc.com`	JS	Main	C + FP

„C“ steht für Cookie, „FP“ für Fingerprint.

Tabelle 2: Drittanbieter nach erfolgtem Login.

Tabelle 2 zeigt erneut, dass die meisten Banken nach erfolgtem Login in ihr Onlinebanking keine Dienste Dritter nutzen. Von denjenigen, die dies tun:

- hat Consorsbank wie bereits auf der Login-Seite ein Chat-Support-Widget eingebunden.

- zeigt DKB nach erfolgtem Login weiterhin das Verisign-Siegel, was es Verisign möglich macht, die Seiten, die ein Nutzer innerhalb des Onlinebanking-Portals aufruft, zu verfolgen.
- hat Number26 die gleichen Dritten wie bereits auf der Login-Seite eingebunden sowie zusätzlich ein Chat-Support-Widget, das direkt im Hauptdokument geladen wird. Der Aufruf, damit dieses Widget geladen wird, beinhaltet den Namen sowie die E-Mail-Adresse des Nutzers.

Bank	Dritte	Typ	Context	Tracking
Commerzbank	track.adform.net	Pixel	Main	C
HypoVereinsBank	keine			
PostBank	keine			
Stadtsparkasse	keine			
ING DiBa	keine			
DAB-Bank	adition.com	Pixel	Main	C
Volksbank	keine			
Deutsche Bank	keine			
ComDirect	track.adform.net	Pixel	Main	C
Consorsbank	omtrdc.net	JS	Main	FP
DKB	seal.verisign.com	JS	Main	C
	seal.websecurity.norton.com	Pixel	Main	—
	uip.semasio.net	Pixel	Main	C
	1001.netrk.net	Pixel	Main	C
	www.google-analytics.com	Pixel	Main	FP
	doubleclick.net	Pixel	Main	C
	webtrekk.net	Pixel	Main	C + FP
	www.google.com	Pixel	Main	C + FP
	advertising.com	Pixel	Main	C + FP
	mathtag.com	Pixel	Main	C
	d.turn.com	Pixel	Main	C
	eyeota.net	Pixel	Main	C
	adition.com	Pixel	Main	C
Number26	connect.facebook.com	JS	Main	—
	www.google-analytics.com	Pixel	Main	FP
	cc-collector.tech26.de	Pixel	Main	FP
	cloudfront.net	JS	Main	—

	usage.trackjs.com	Pixel	Main	—
	doubleclick.net	Pixel	Main	C
	www.google.com	Pixel	Main	C
	www.facebook.com	Pixel	Main	C
	livechatinc.com	JS	Main	C + FP

„C“ steht für Cookie, „FP“ für Fingerprint.

Tabelle 3: Drittanbieter auf der Logout-Seite.

Tabelle 3 zeigt, dass mehrere Seiten Tracking-Daten an Dritte übertragen, nachdem sich der Kunde aus dem Onlinebanking abgemeldet hat:

- Commerzbank, DAB-Bank, ComDirect und Consorsbank nutzen alle ein Tracking-Pixel von Werbe- und Webanalyse-Anbietern wie Adform, Adition und Omniture.
- DKB hat gleich mehrere Tracking-Pixel von Google, Advertising.com, Adition, MathTag, Eyeota, Turn, Semasio, Webtrekk und Netzeffekt in seiner Logout-Seite eingebunden.
- Number26 nutzt auf der Logout-Seite die gleichen Drittanbieter wie auf der Login-Seite und innerhalb des Portals.

4 Auswertung und Erörterung

Die Ergebnisse dieser Studie zeigen, dass von den zwölf untersuchten Onlinebanking-Portalen lediglich fünf während einer typischen Onlinebanking-Sitzung keine Daten an Dritte haben durchgehen lassen. Nach erfolgtem Login rufen lediglich die Websites von drei der Banken Dienste von Drittanbietern auf, wobei dies bei einer der Banken in sicherer Weise geschieht. Nach dem Logout wiederum ist das höchste Tracking-Aufkommen festzustellen: Hier überträgt die Hälfte der Websites Daten an große Webtracking- und Webanalyse-Anbieter.

Aus den üblichen Anwendungsfällen der eingesetzten Drittanbieter können wir die Gründe, warum die hier untersuchten Banken deren Dienste auf ihrer Website einbinden, ableiten. Unsere Studie lässt vier primäre Anwendungsfälle erkennen:

- Website-Analyse – Software-as-a-Service-Anbieter, die die Nutzung und Leistung von Websites analysieren (z. B. Google Analytics, TrackJS).
- Marketing- und Business-Intelligence – Werbeunternehmen, die ihren Kunden helfen, die Konversionsrate von Marketingmaßnahmen zu verfolgen. Solche Dienste können beispielsweise die Kunden einer Bank ’tracken‘, um zu verhindern, dass die Bank Neukunden-Werbung an bereits bestehende Kunden schickt, oder um zu ermitteln, wie viele Neukunden eine bestimmte Werbekampagne generiert. Zu den Anbietern solcher Dienste gehören z. B. DoubleClick, Adition, Facebook und Adform.
- Vertrauen – Unternehmen wie Verisign bieten Siegel an, die dem Nutzer die Sicherheit der Banken-Website versichern.
- Support-Tools – Chat-Support-Systeme Dritter gestatten es den Banken, ihren Online-Support auszulagern (z. B. LiveChat, NTR).

Der Einsatz dieser Dienste bringt den Banken einen direkten Vorteil, da er ihnen hilft, eigene Geschäftsprozesse zu optimieren, Kosten zu senken und gegebenenfalls bessere Software-Tools anzubieten, als sie die Bank selbst zu erstellen in der Lage wäre. Allerdings geht er eben auch mit gewissen Risiken einher, was Sicherheit und Datenschutz anbelangt.

4.1 Auswirkungen auf die Sicherheit

Banken sind beliebte Ziele für Betrugs- und Hacking-Versuche und haben deshalb sehr hohe Sicherheitsanforderungen. Man kann dementsprechend davon ausgehen, dass sie an ihre eigenen IT-Systeme allerstrengste Anforderungen stellen, um höchstmögliche Sicherheit zu gewährleisten. Die Einbindung von Diensten Dritter in sichere Bereiche ihrer Website birgt die Gefahr, die Angriffsfläche zu vergrößern: So ist beispielsweise JavaScript, das im Hauptdokument geladen wird, ein potentieller Angriffsvektor und kann, wenn es kompromittiert wurde, vollständig Kontrolle über die Website und die von Nutzern eingegebenen Daten ergreifen. Die in dieser Studie identifizierten Dritten, die JavaScript in der Website von Banken laden, pflegen unter Umständen nicht die gleichen Sicherheitsstandards wie die Bank selbst und können somit das schwache Glied in der Kette sein, über das sich Angreifer Zugriff auf tausende Bankkonten verschaffen könnten.

4.2 Auswirkungen auf den Datenschutz

Immer, wenn der Dienst eines Dritten aus dem Kontext der Hauptseite heraus aufgerufen wird, erhält dieser Dritte über den HTTP-Header `Referer` Informationen darüber, welche Seite aufgerufen wird, sowie die IP-Adresse des Rechners, von dem aus der Aufruf erfolgt. Kombiniert mit einem Cookie und/oder irgendeiner Art von Browser-Fingerprinting ermöglichen diese Informationen es dem Drittanbieter, einzelne Nutzer, die auf die Website zugreifen, zu unterscheiden. Werden die Dienste dieses Drittanbieters nun auch von anderen Websites im Internet genutzt, gelangt er in die Lage, ein Profil von den Seiten zu erstellen, die ein bestimmter Nutzer besucht. Dieses Vorgehen ist im Internet übliche Praxis, allem voran um Werbung und Empfehlungen gezielt auf die Interessen eines Nutzers zuzuschneiden.

Allerdings betrachten wahrscheinlich viele Nutzer Informationen über die Bank, bei der sie ein Konto unterhalten, als sensibler, als beispielsweise Informationen darüber, welche Zeitungsartikel sie lesen. Mehr noch: Wenn das Tracking während der eingeloggten Sitzung erfolgt, könnten sich sogar Informationen über den Finanzstatus des Nutzers ableiten lassen. Wir möchten darauf hinweisen, dass wir nicht glauben, dass die Daten für derartige Zwecke genutzt werden – die technischen Mittel, die eingesetzt werden, würden den Drittanbietern aber die Möglichkeit dazu geben.

Welches Datenschutzrisiko von den Drittanbietern, die in dieser Studie ermittelt wurden, ausgeht, lässt sich anhand der Reichweite dieser Unternehmen im Internet beurteilen. Je größer die Reichweite, desto umfassender können die Profile, die sie von Nutzern erstellen, theoretisch sein. Die Reichweite der einzelnen Unternehmen können wir anhand von Daten beurteilen, die unsere Anti-Tracking-Software über einen Zeitraum von zwei Wochen bei unseren Nutzern gesammelt hat. Sie ist in Tabelle 4 zusammengefasst:

Dritter	Reichweite	Anzahl der Websites
`google-analytics.com`	44,29 %	790.000
`google.com`	36,89 %	550.000
`www.google.com`	29,76 %	420.000
`doubleclick.net`	30,91 %	400.000
`www.facebook.com`	21,11 %	310.000
`adition.com`	7,62 %	30.000
`mathtag.com`	5,43 %	42.000
`turn.com`	3,64 %	30.000
`track.adform.net`	3,47 %	45.000
`uip.semasio.net`	1,90 %	12.000
`advertising.com`	1,43 %	25.000
`omtrdc.net`	1,42 %	7.200
`webtrekk.net`	0,96 %	3.500
`eyeota.net`	0,40 %	4.800

seal.websecurity.norton.com	0,19 %	1.700
seal.versign.com	0,14 %	1.300
livechatinc.com	0,06 %	2.200
usage.trackJS.com	0,05 %	740
d2zah9y47r7bi2.cloudfront.net	0,03 %	510
netrk.net	0,04 %	890
eu.ntrsupport.com	0,04 %	83
d1fc8wv8zag5ca.cloudfront.net	0,01 %	270
tech26.de	<0,01 %	5

Tabelle 4: Reichweite der Drittanbieter in Prozent der beobachteten Seitenaufrufe (auf zwei Kommastellen gerundet) sowie Anzahl der Domänen, auf denen Dienste dieser Drittanbieter erkannt wurden (auf zwei Ganzzahlen gerundet).

Es ist zu beachten, dass bereits eine Reichweite von 1 % sehr hoch ist – denn das bedeutet, dass bei einem durchschnittlichen Nutzer von jeder hundertsten Seite, die er aufruft, Daten übertragen werden. Dass mehr als die Hälfte der Drittanbieter eine Reichweite von mehr als 1 % besitzen zeigt, dass diese Unternehmen in der Lage sind, umfangreiche Profile von Nutzern zu erstellen, und das in den meisten Fällen über zehn- oder hunderttausende verschiedener Internetseiten hinweg. Wie wir gezeigt haben, kann dieses Profil auch Informationen über die Bank, bei der der Einzelne ein Konto besitzt, enthalten.

Dem Tracking solcher Drittanbieter lässt sich jedoch durch Einsatz von Anti-Tracking-Tools wie beispielsweise Cliqz Anti-Tracking entgegenwirken. Dieses Tool löscht die Cookies aus den Aufrufen von Diensten Dritter sowie die übertragenen Fingerprint-Daten. Auf diese Weise wird die Möglichkeit, ein Profil des Nutzers zu erstellen, effektiv unterbunden.

5 Schlussbetrachtung

Die vorliegende Studie zeigt das Ausmaß des Trackings in den Onlinebanking-Portalen deutscher Banken. Wir stellen fest, dass über die Hälfte der untersuchten Banken an der einen oder anderen Stelle ihres Onlinebanking-Prozesses Tracking einsetzen. Die Auswirkungen, die dieses Tracking für die Sicherheit und den Datenschutz nach sich zieht, wurden erörtert und die Reichweite gemessen, die die eingesetzten Tracking-Anbieter erzielen.

Wir können nicht mit Sicherheit sagen, was die Gründe für die Nutzung der Dienstleistungen von Drittanbietern sind. Die Effekte auf die Sicherheit und die Privatsphäre sind vielleicht nicht bekannt oder sie wurden überprüft und für akzeptabel befunden. Die begleitenden Umstände der Zusammenarbeit mit Drittanbietern können sich aber jederzeit ändern, da Drittanbieter per Definition außerhalb der Kontrolle des Seitenbetreibers liegen. Beispielsweise könnte der Verkauf eines Drittanbieters auslösen, dass die Daten der Kunden des Seitenbetreibers ebenfalls zum Verkauf stehen [7].

Um ihre Privatsphäre zu schützen installieren Internet-User immer öfter Software, mit der sie steuern können, welche Daten von Webseiten an Drittanbieter gesendet werden. Ein paar Beispiele: Ghostery [4], Disconnect [1] und Firefox Tracking Protection [6] nutzen dauerhaft-redigierte Listen mit bekannten Tracking-Dienstleistern, um zu verhindern, dass Daten-Anfragen von eben diesen Dienstleistern beantwortet werden. Privacy Badger [5] blockt mit einem heuristischen Ansatz gleich alle Drittanbieter. Der Cliqz Browser und die Cliqz Browser-Erweiterung für Firefox nutzen einen datenbasierten Ansatz um Tracking zu verhindern [8]. Bei den Bankenportalen, die in dieser Studie getestet wurden, hätte Cliqz Anti-Tracking alle Cookies entfernt sowie alle Versuche verhindert, den Nutzer anhand seines digitalen Fingerabdruck zu verfolgen.

Quellennachweis

[1] Disconnect. Disconnect. `https://disconnect.me/`.

[2] P. Eckersley. How unique is your web browser? In *Proceedings of the 10th International Conference on Privacy Enhancing Technologies*. Springer-Verlag, 2010.

[3] S. Englehardt and A. Narayanan. Online tracking: A 1-million-site measurement and analysis. [Technical Report], May 2016.

[4] Ghostery. Ghostery. `https://ghostery.com/`.

[5] H. P. Jason Bau, Jonathan Mayer and J. C. Mitchell. A promising direction for web tracking countermeasures. In *Proceedings of Web 2.0 Security and Privacy (W2SP)*. IEEE Computer Society, 2013.

[6] G. Kontaxis and M. Chew. Tracking protection in firefox for privacy and performance. In *Proceedings of Web 2.0 Security and Privacy (W2SP)*. IEEE Computer Society, 2015.

[7] A. Peterson. Bankrupt radioshack wants to sell off user data. but the bigger risk is if a facebook or google goes bust. Washington Post, March 26th 2015.

[8] Z. Yu, S. Macbeth, K. Modi, and J. M. Pujol. Tracking the trackers. In *Proceedings of the 25th International Conference on World Wide Web*, pages 121–132. International World Wide Web Conferences Steering Committee, 2016.