Privatsphäre im Internet
Handout zur Vorbereitung

Manuel Ziegler
private@manuelziegler.de
PGP-ID: 0xFC875ACB
PGP-Fingerprint:
C3D6 ACD4 5BD2 6BDE E52D FB75 6EF4 D1CA FC87 5ACB

11. Januar 2016

Inhaltsverzeichnis

Zusammenfassung

Als InternetnutzerIn werden Sie auf Schritt und Tritt von Unternehmen wie Facebook und Google, aber auch von zahlreichen Staaten überwacht. In diesem Vortrag lernen Sie, mit welchen Methoden Sie dabei von den unterschiedlichen Interessensgruppen verfolgt werden und wie Sie sich dagegen verteidigen können.

In diesem Handout zur Vorbereitung sollen Ihnen vor allem kurze Anleitungen zur Installation und Nutzung verschiedener Werkzeuge zum Schutz Ihrer Privatsphäre gegeben werden, sodass Sie diese bereits im Vorfeld des Vortrags auf Ihren Rechnern installieren und ausprobieren können. So können Sie sich dabei auftretende Fragen bereits im Vorfeld notieren und diese Fragen während des Vortrags stellen oder gerne auch bereits vorab per E-Mail an private@manuelziegler.de senden.

Die in diesem Handout beschriebenen Anleitungen beschreiben, sofern nicht anders angegeben, die Installation und Verwendung der diversen Browsererweiterungen für den populären Webbrowser Firefox unter Debian-Linux. Viele der Browsererweiterungen gibt es auch für andere Webbrowser wie Microsofts Internet Explorer oder Googles Chrome. Die Installation und Verwendung kann dabei jedoch von der hier gelieferten Beschreibung abweichen. Sollten Sie Probleme bei der Installation oder Verwendung eines der Tools haben, können Sie mich gerne per E-Mail kontaktieren.

1 BenutzerInnentracking

Unter dem Begriff BenutzerInnentracking sind in diesem Vortrag alle, von im Internet vertretenen Unternehmen praktizierten, Methoden zur Erfassung von Informationen über deren BenutzerInnen, die über die freiwilligen und direkten Angaben letzterer hinausgehen. Demnach lassen sich verschiedene Formen von BenutzerInnentracking unterscheiden:

User Tracking bezeichnet alle Methoden zur Ermittlung einer mehr oder weniger vollständigen Browserhistorie einer NutzerIn.

Geotracking bezeichnet alle Methoden zur Erstellung eines Bewegungsprofils einer NutzerIn.

biometrische Verfahren bezeichnen alle Methoden zur Erkennung einer NutzerIn anhand biometrischer Daten[1].

... neben diesen Methoden zur Verfolgung von NutzerInnen existieren zahlreiche weitere, die in diesem Vortrag jedoch unberücksichtigt bleiben sollen.

Einen Überblick über diverse Trackingtechnologien aus dem Bereich *User Tracking* finden Sie in meinem, im Dezember 2015 bei Hanser Update erschienenen Beitrag [4].

1.1 Self-Destructing Cookies

Das Browserplugin *Self-Destructing Cookies* kümmert sich um Ihre Cookies, mithilfe derer Sie beim Wiederbesuch einer Seite und damit auch seitenübergreifend verfolgt werden können, indem es diese beim Schließen eines Tabs automatisch löscht.

Installieren können Sie *Self-Destructing Cookies* über den Firefox Add-On-Store: `https://addons.mozilla.org/en-US/firefox/addon/self-destructing-cookies/`.

Nach der Installation löscht *Self-Destructing Cookies* automatisch alle Cookies beim Schließen des entsprechenden Tabs. Indem Sie auf das Symbol des Plugins klicken, können Sie jedoch auch einstellen, dass Cookies einer Seite bis zum Schließen des Browserfensters oder dauerhaft erhalten bleiben (siehe Abbildung 1).

1.2 Ghostery

Ghostery ist ein Browser-Plugin zum Blockieren von Anfragen an Domains, deren Betreiber dafür bekannt sind, dass sie NutzerInnen verfolgen. Dabei arbeitet Ghostery ähnlich wie auch die meisten Ad-Blocker (siehe Abschnitt 1.4) mit einer Blacklist.

Sie können Ghostery über die die Unternehmenswebseite unter der URL `https://www.ghostery.com/try-us/download-browser-extension/` in Ihrem Browser installieren (siehe Abbildung 2).

Nach der Installation von Ghostery werden Sie anhand eines Assistenten durch die einzelnen Schritte der Einrichtung geführt. Dabei können Sie festlegen, welche Tracking-Unternehmen von Ghostery blockiert werden und in welcher Form Sie darüber in Kenntnis gesetzt werden, welche Tracking-Unternehmen Sie auf der besuchten Seite verfolgen.

[1] Dazu gehören Verfahren zur Gesichtserkennung, zur Erkennung von Fingerabdrücken, Retina-Scanner, usw. aber auch sogenannte stylometrische Verfahren [1], sowie Verfahren, die NutzerInnen anhand der für sie charakteristischen Tippgeschwindigkeit erkennen.

Abbildung 1: Sie können mit Self-Destructing Cookies festlegen, ob Cookies einer Seite dauerhaft, bis zum Schließen des Tabs oder bis zum Schließen des Browserfensters erhalten bleiben sollen.

1.3 Privacy Badger

Privacy Badger ist ein von der Electronic Frontier Foundation entwickeltes Browserplugin, das anhand von Cookies, anderen Browserspeicher-Technologien und Canvas-Fingerprinting zunächst beobachtet, welche Unternehmen eine NutzerIn unerlaubt verfolgen. Stellt *Privacy Badger* fest, dass ein Unternehmen die NutzerIn verfolgt, blockt das Plugin weitere Anfragen von der entsprechenden Domain.

Sie können *Privacy Badger* unter der URL `https://www.eff.org/privacybadger` mit einem Klick auf den Button „Install Privacy Badger“ installieren (siehe Abbildung 3).

Direkt nach der Installation wird *Privacy Badger* keine Domains blockieren, schließlich konnte das Plugin soweit auch noch kein Tracking feststellen (siehe Abbildung 4). Nach einiger Zeit werden Sie jedoch feststellen, dass *Privacy Badger* beginnt, Anfragen an bestimmte Domains zu blockieren.

Indem Sie die in Abbildung 4 sichtbaren Schieberegler auf „blocked“ oder „blocked cookies“ stellen, können Sie Anfragen an die entsprechende Domain manuell blockieren, oder verhindern, dass Cookies an diese Domain gesendet werden.

1.4 AdBlockPlus/uBlock

AdBlockPlus und *uBlock* sind eigentlich sogenannte Ad-Blocker, mithilfe derer Werbeanzeigen auf Webseiten unterdrückt werden. Das diente ursprünglich dazu, den kommerziellen Anstrich des Internets ein wenig zu reduzieren, hat aber den positiven Nebeneffekt, dass das in den Snippets der Ad-Provider integrierte *User Tracking* blockiert wird.

1.4.1 AdBlockPlus

AdBlockPlus können Sie über die Webseite der Browsererweiterung installieren: `https://adblockplus.org/`. Hier gibt es auch eine deutsche Anleitung: `https://adblockplus.org/de/getting_started`.

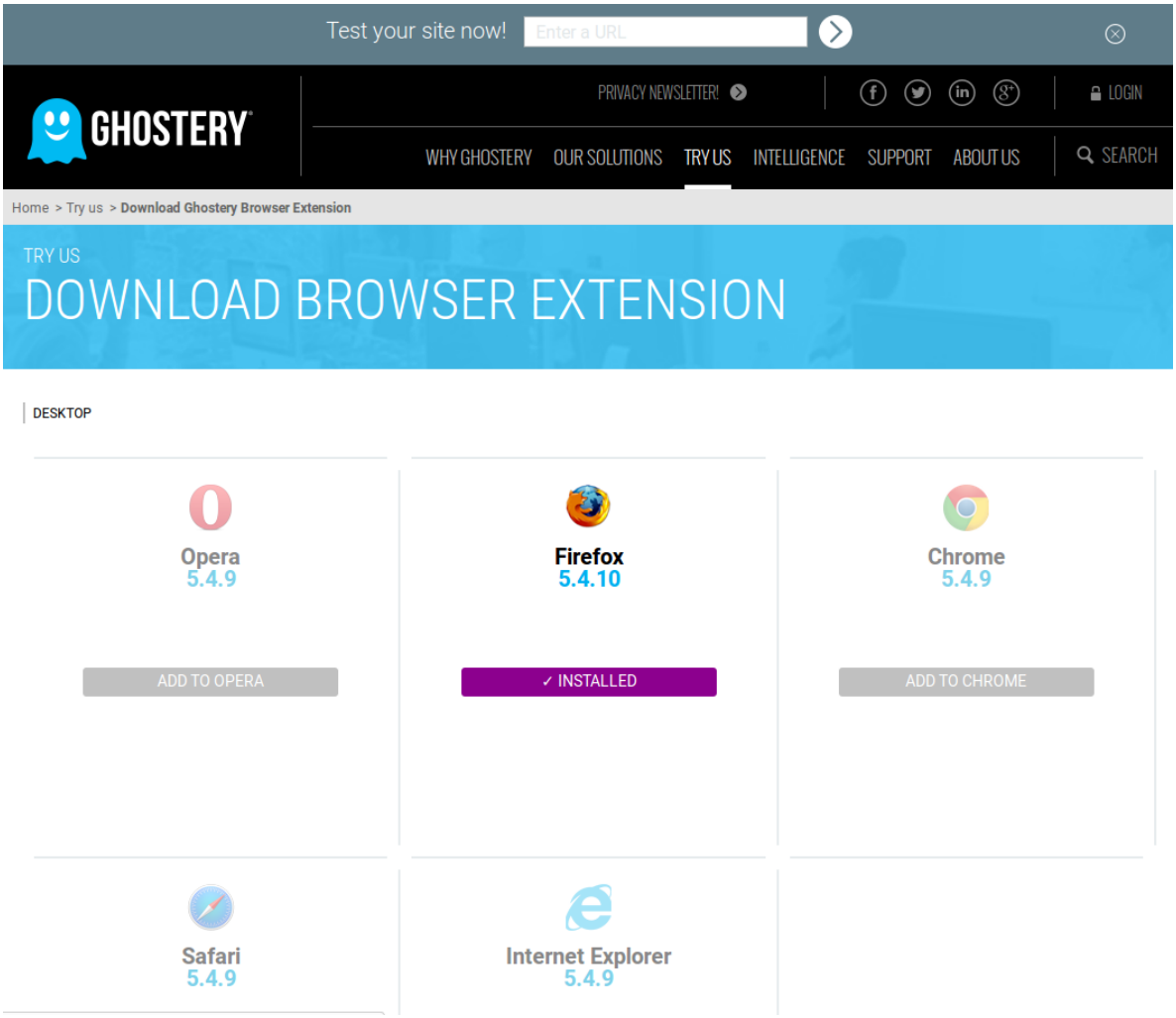

Abbildung 2: Sie können Ghostery über die Webseite des Unternehmens installieren.

1.4.2 uBlock

Auch die Browsererweiterung *uBlock* erhalten Sie über die Webseite des Projekts: `https://www.ublock.org/`.

Die Bedienung von *uBlock* ist denkbar einfach. Sie können den Ad-Blocker durch einen Klick auf das I/O-Symbol für eine Seite aktivieren und deaktivieren (siehe Abbildung 5).

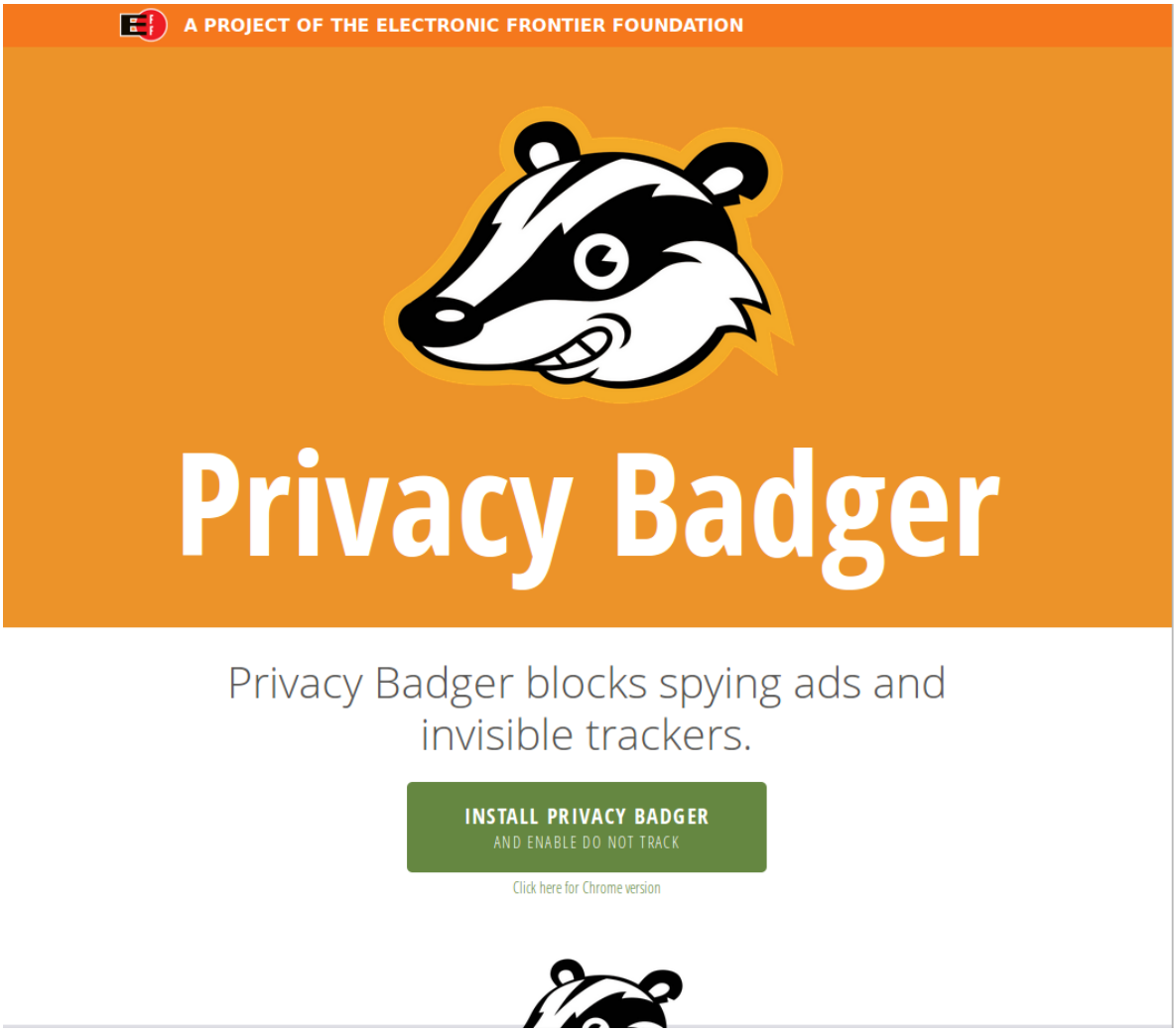

Abbildung 3: Installation des Privacy Badgers.

2 Staatliche Überwachung

Staatlicher Überwachung zu entgehen ist deswegen besonders schwer, weil nicht nur enorme Aufwände zur Verfolgung von NutzerInnen betrieben werden, sondern die Staatsgewalt des jeweiligen Staates die Ausnutzung der zentralisierten Infrastruktur des Internets ermöglicht. Auf diese Art und Weise können zumindest sogenannte Metadaten in einer beängstigend flächendeckenden Art und Weise gesammelt werden, die die gleichzeitige Überwachung beinahe aller InternetnutzerInnen ermöglicht. Die seit 2013 von Edward Snowden veröffentlichten Dokumente zeigen, dass die ausführenden Geheimdienste dabei sowohl die Infrastruktur des Internets kompromittieren [3], als auch Unternehmen zur Herausgabe der Daten von NutzerInnen ihrer Angebote zwingen bzw. „überreden“ [2]. Dabei werden diese Daten nicht

Abbildung 4: Privacy Badger in Aktion.

nur in individuellen, gerichtlich genehmigten Fällen abgegriffen, sondern im großen Stil und über eigens für die Geheimdienste eingerichtete Schnittstellen abgefragt [2].

Gegen die Überwachung mithilfe der bei Unternehmen gespeicherten Daten kann man sich wehren, indem man die in Abschnitt 1 beschriebenen Werkzeuge einsetzt und auf die Preisgabe überflüssiger Informationen an Unternehmen verzichtet. Wesentlich schwieriger ist es, sich gegen die Überwachung mithilfe der kompromittierten Internet-Infrastruktur zu verteidigen. Grundsätzlich könnte der alltägliche Einsatz kryptografischer Protokolle verhindern, dass Geheimdienste Inhalte Ihrer Kommunikation abgreifen. Zum Schutz Ihrer Metadaten, der mindestens ebenso wichtig ist, wie der Schutz der Inhalte, eignet sich die Verwendung des Tor-Browsers.

2.1 Tor-Browser

Der Tor-Browser schützt ihre Privatsphäre im Internet, indem er Ihre IP-Adresse und weitere, typische Metadaten, mithilfe derer Sie eindeutig identifiziert werden können, verbirgt bzw. reduziert.

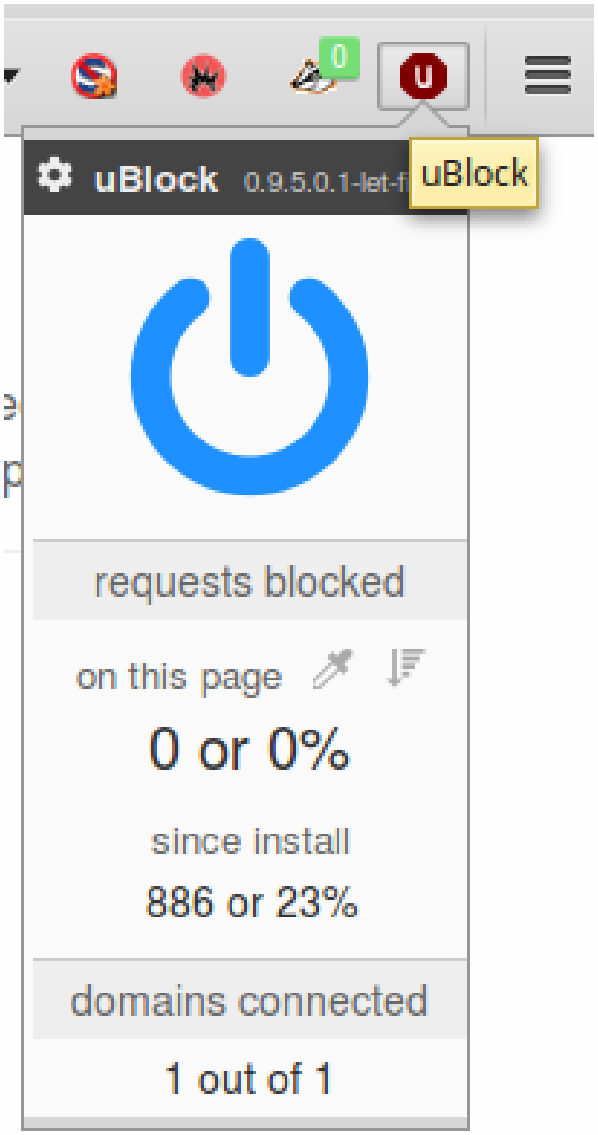

Abbildung 5: So können Sie uBlock für eine Seite aktivieren und deaktivieren.

Sie können den Tor-Browser auf der Webseite des Tor-Projekts für verschiedene Betriebssysteme, darunter Windows, Mac und Linux herunterladen: `https://www.torproject.org/download/download-easy.html.en`. Nach dem Download sollte Tor bereits fertig eingerichtet sein und ohne weitere Installation direkt ausgeführt werden können.

Auf der Seite `https://www.torproject.org/docs/documentation.html.en` finden Sie zahlreiche Anleitungen, die Ihnen Tipps zur Nutzung von Tor geben.

2.2 Orbot/Orfox

Auch für Smartphones gibt es Tor. Hier benötigen Sie die App *Orbot*[2], sowie die App *Orfox*.

Weitere Informationen, sowie Installationsanweisungen finden Sie unter der URL `https://guardianproject.info/apps/orbot/`.

Literatur

[1] Marcelo Luiz Brocardo, Issa Traore, Sherif Saad, and Isaac Woungang. Authorship verification for short messages using stylometry. In *Proc. of the IEEE Intl. Conference in Computer, Information and Telecommunication Systems (CITS 2013)*, 2013. `https://www.uvic.ca/engineering/ece/isot/assets/docs/Authorship_Verification_for_Short_Messages_using_Stylometry.pdf`.

[2] Glenn Greenwald and Ewen MacAskill. Nsa prism program taps in to user data of apple, google and others, Juni 2013. `http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data`.

[3] Craig Timberg. NSA slide shows surveillance of undersea cables, Juli 2013. `https://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html`.

[4] Manuel Ziegler. Sicherheit in sozialen Netzwerken – Nutzertracking im Web 2.0. *Hanser Update*, Dezember 2015. `http://update.hanser-fachbuch.de/2015/12/sicherheit-in-sozialen-netzwerken-nutzertracking-im-web-2-0/`.

[2] Die hier beschriebene Anleitung funktioniert nur für Android-Geräte.