DATENSCHUTZ

Die Keks-Spione

Im Netz wird fast jeder Klick von Hunderten Werbefirmen heimlich ausgewertet. Die Nutzer sind dagegen oft machtlos, die Bundesregierung schützt die Schnüffler. Ein Selbstversuch.

Es waren ein paar harmlose Anzeigen für Kameras, die meinen Verdacht weckten. Verfolgt mich da einer, wenn ich im Internet unterwegs bin? Ich hatte kurz zuvor online nach einer neuen Digitalkamera gesucht. Und plötzlich fiel mir die massive Werbung von Nikon, Canon oder Pentax auf. Zufall? Selektive Wahrnehmung? Oder schaut mir da einer auf die Finger? Das wollte ich genauer wissen.

9.10 UHR: Ich lade mir ein kleines Programm aus dem Netz. „Collusion“ heißt es, ein einfaches Analysewerkzeug, das mir sozusagen erlaubt, unter die Motorhaube meines Rechners zu schauen. Es offenbart, was der so im Verborgenen treibt, während ich mich im Netz treiben lasse.

9.30 UHR: Als Erstes klicke ich auf die Website des „Wall Street Journal“, damit beginne ich oft meine Morgenlektüre. Doch diesmal explodiert ein kleines Feuerwerk auf der Anzeige meines Analysetools: Ein Pünktchen steht für die Website der US-Zeitung, von dort schießen vier Striche in alle Richtungen. Bin ich verwanzt?

Cookies, zu Deutsch: Kekse, werden die kleinen Datenpakete genannt. Viele Websites legen diese Dateien auf meiner Festplatte ab. Sie können festhalten, wann und von wo aus ich welche Website aufrufe. Automatisch habe ich einen Namen bekommen: 3b760f6d-8be9-4363-9b85-abeff205d1ab.

Die Website weiß nun, mit wem sie es zu tun hat. Schon mit dem ersten Klick haben vier weitere Datensammler Dossiers über mich angelegt: gravity, bizographics, dowjoneson, scorecardresearch.

Hinter diesen Namen stecken Marktforscher, die wissen wollen, für was mein Kürzel steht: wo ich sitze, was ich kaufen möchte, ob ich gelangweilt bin, krank oder einsam. Je weiter ich herumklicke von Website zu Website, desto klarer wird für sie, welche Werbung mich interessieren könnte: Kopfschmerztabletten, Partnerbörsen oder eben Kameras? Die US-Marktforschungsfirma Bluekai rühmt sich, was sie alles über Internetnutzer errechnen könnte: Alter, Geschlecht, Sprache, Beruf, Gesundheitszustand, Alter und Geschlecht der Kinder …

9.34 UHR: Ich klicke auf SPIEGEL ONLINE. Weitere Punkte und Linien. Ich fühle mich ertappt: Auch mein eigenes Haus lässt mein Klickverhalten überwachen, unter anderem über die IVW (Informationsgemeinschaft zur Feststellung der Verbreitung von Werbeträgern). Ein Dilemma, das die ganze Medienbranche betrifft.

Unter der Rubrik „What They Know“ – was sie über uns wissen, durchleuchtet das „Wall Street Journal“ die Online-Schnüffelei. Aber das hindert das Blatt natürlich nicht daran, selbst tracken zu lassen: Irgendwie muss die Recherche schließlich bezahlt werden.

13.05 UHR: Nach etwa hundert Klicks bin ich tief verstrickt ins Netz der Werber. Fasziniert beobachte ich, wie meine Software die Überwacher überwacht. Mein Bildschirm zeigt ein verworrenes Knäuel von Tracking-Firmen, die nicht nur selber Daten über mich sammeln, sondern diese untereinander austauschen. „Third Party Tracking“, Beobachtung durch Dritte, wird das genannt.

Ausgewählte Beispiele von Dateien zur Erstellung von Nutzerprofilen

Session Cookies
Diese harmlosen Dateien dienen nur der Wiedererkennung, solange man auf einer Website ist. Sie werden anschließend gelöscht.

Persistent Cookies
Diese Wiedererkennungsdateien bleiben lange erhalten, lassen sich aber leicht löschen.

„Gefällt mir“-Buttons
Facebook trackt Nutzer selbst dann, wenn sie den Button gar nicht geklickt haben.

Flash Cookies
Werden über eine Video-Software verwaltet und nicht vom Browser erkannt.

Zählpixel (Beacons)
Kleine, oft nur ein Pixel große Bilddateien, die beim Öffnen einer Seite automatisch abgerufen werden, um einen Besucher zu identifizieren.

Zombie Cookies
Wiedererkennungsdateien, die nach dem Löschen automatisch wieder installiert werden.

DER SPIEGEL

Im Netz der Schnüffler

Grafische Darstellung der Überwachung durch Tracking-Firmen

● auf PrivacyChoice verzeichnete Tracker

9.30 Uhr
Der Test beginnt mit dem „Wall Street Journal“. Von hier werden bereits Informationen an vier Sites weitergegeben.

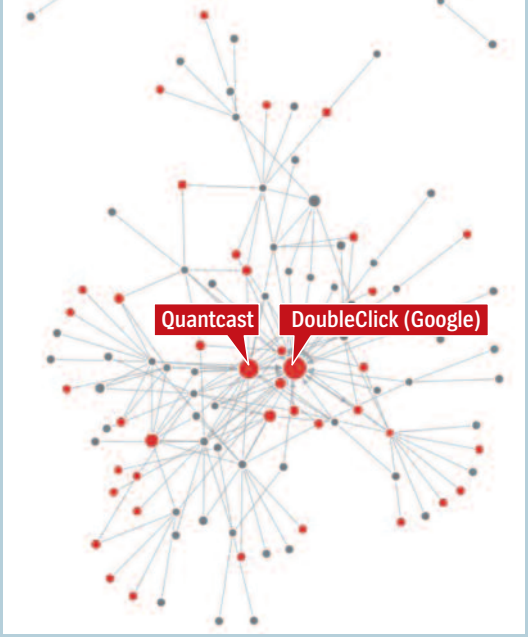
Screenshots der Transparenz-Software „Collusion“; Download unter www.mozilla.org/collusion

Wer für ein Produkt nicht zahlt, der ist nicht Kunde, sondern Ware. So lautet das Motto der Kostenloskultur – und bringt damit das Dilemma auf den Punkt: Wer nicht mit Geld zahlt, zahlt eben mit Daten. An der Oberfläche scheint es, als säße ich allein im Büro – ich nehme ja nicht wahr, dass ich mich mit jedem Klick auf einer globalen Bühne bewege, beobachtet von Hunderten Geräten und denen, die Zugang zu ihnen haben. Keiner meiner Zuschauer hat sich mir vorgestellt, keiner um Erlaubnis gebeten.

13.35 UHR: Hunderte verschiedener Firmen haben mich inzwischen beobachtet. Doch das Gewusel auf dem Monitor beginnt Form anzunehmen. Dick sitzen zwei Punkte wie Spinnen im Netz: die Firma Quantcast und der Dienst DoubleClick von Google. Beide heften sich durch kleine Spitzeldateien an meine Fersen und verfolgen mein Tun allein heute auf jeweils 40 verschiedenen Websites: Suchanfragen, die ich stelle, Artikel, die ich lese, Videos, die ich schaue.

Auf meiner Festplatte sitzen nun über 200 Cookies. Aber ist das so schlimm? Die Industrie beteuert, die Kekse seien ja nicht mit meinem Namen verbunden, sondern nur mit einer abstrakten Folge aus Buchstaben und Zahlen.

Allerdings wäre es für Datenbanker ein Leichtes, Name und Chiffre zusammenzuführen – wenn sie dies wollen. In den Vereinigten Staaten zum Beispiel nutzen inzwischen selbst herkömmliche Läden verhaltensbasierte Werbung. Das „New York Times Magazine“ berichtet vom Fall einer minderjährigen Schülerin, die regelmäßig in einem Target-Kaufhaus in der Nähe von Minneapolis einkaufte. Als



13.35 Uhr
Ein ganzes Netz aus Tracking-Firmen überwacht den Browser, sie tauschen untereinander Informationen aus. Teils laufen Informationen von 40 Websites bei einer Firma zusammen, um zu protokollieren, was der Nutzer liest, kauft und welche Videos er schaut.

15.17 Uhr
Anfrage an die Website PrivacyChoice mit der Bitte, das Tracking zu stoppen. Die Website verschickt die Anfrage an 215 Partnerfirmen. Das Tracking soll so deutlich verringert beziehungsweise gestoppt werden.

17.13 Uhr
Kaum eine Veränderung. Nach nur zwei Stunden hat die Überwachung wieder ihren alten Stand erreicht.

DER SPIEGEL

sie plötzlich Werbung für Babykleidung und Kinderbetten bekam, beschwerte sich der Vater beim Filialleiter: Sei das eine Aufforderung an Teenager, schwanger zu werden? Es stellte sich heraus, dass seine Tochter wirklich ein Kind erwartete.

Durch das Beobachten des Klickverhaltens können Werber geheime Wünsche erraten, die sich Kunden nicht einmal selbst eingestehen. Doch mittlerweile haben die Firmen dazugelernt: Sie tarnen ihre gezielten Angebote, indem sie etwa die Windelwerbung durch Weinwerbung ergänzen. Denn Marktforscher wissen: Kunden, die sich nicht beobachtet fühlen, kaufen mehr.

Viele Kunden sind ahnungslos, wie ihr Klickverhalten überwacht wird. Sollte daher der Gesetzgeber Grenzen setzen? Die EU hatte 2009 beschlossen, so könne es nicht weitergehen, und eine „E-Privacy"-Richtlinie zum Schutz vor zu viel Schnüffelei im Netz (2009/136/EG) erlassen.

Die Richtlinie unterscheidet zwischen zwei Sorten von Cookies: Jene, die für das technische Funktionieren von Websites „unbedingt erforderlich" sind (etwa um Waren in einen digitalen Einkaufskorb legen zu können), dürfen bleiben. Schnüffelcookies dagegen, die nur der Überwachung dienen, bedürfen künftig einer Einwilligung.

Einige EU-Länder, darunter Frankreich und Großbritannien, haben die Cookie-Richtlinie in nationales Recht umgesetzt. Ab und zu poppt dort seither beim Surfen ein zusätzliches Fenster auf, das sinngemäß fragt: Wenn Sie diesen kostenlosen Dienst weiter nutzen wollen, würden wir Sie gern beobachten. Dürfen wir?

Deutschland aber hinkt hinterher, der von der EU gesetzte Termin ist seit dem 25. Mai 2011 verstrichen. „Die sogenannte Cookie-Regelung ist eine zwingend umzusetzende europäische Vorgabe, aber die Umsetzung wurde bislang ignoriert", schimpft der Bundesdatenschutzbeauftragte Peter Schaar. Die Bundesregierung spielt auf Zeit und setzt auf Selbstverpflichtungen der Industrie.

15.17 UHR: Wie gut funktionieren solche Selbstregulierungskräfte des Marktes andernorts? Ich teste den US-Dienst PrivacyChoice, der verspricht, das Tracking auf Wunsch zu unterbinden. Ein Klick entfacht ein Feuerwerk auf meinem Bildschirm: An 215 Firmen ergeht die Bitte, mich nicht weiter zu verfolgen.

17.13 UHR: Mein Ersuchen, in Ruhe gelassen zu werden, wurde nicht erhört. Schon ist mein Rechner wieder verstrickt ins Netz der Kekse. DoubleClick verfolgt mich wie zuvor über 40 Websites. Ich habe mir eine weitere Software heruntergeladen namens „Do Not Track". Sie hat alle Zugriffsversuche von Marktforschern, die sie aufspüren konnte, geblockt – insgesamt 138 in rund zwei Stunden. Ich schalte die Cookie-Funktion im Menü meines Browsers ab. Aber auch das nützt nur bedingt.

„Viele Tracking-Firmen führen die Nutzer absichtlich hinters Licht", sagt Ashkan Soltani, ein Tracking-Experte aus Washington. „Deaktivierte Cookies werden manchmal nach zehn Tagen einfach erneut aktiviert und gelöschte Cookies automatisch erneut installiert." Mittlerweile gebe es Hunderte neuartige Programme, gezielt darauf ausgelegt, schwer auffindbar zu sein.

18.31 UHR: Ich wühle in den Einstellungen meines Browsers und schalte alle Cookies ab. Paradoxer Nebeneffekt: Je mehr ich meinen Browser aufrüste mit Zusatzprogrammen und Spezialeinstellungen, desto einzigartiger wird sein „Fingerabdruck". Gerade mein paranoid abgeschirmter Rechner macht mich noch leichter verfolgbar.

18.43 UHR: Ein „Pling" kündigt eine Mail aus dem Silicon Valley an. „Okay, ich bin Schuld an dem Schlamassel", schreibt Lou Montulli. Ich hatte ihn gefragt, wie ich mich vor den Cookie-Monstern schützen könne. Denn Montulli müsste es wissen: Er war es, der 1994 mit Mitte 20 mit einem Kollegen bei dem Browser-Hersteller Netscape die ersten Cookies erfand. Sein Ziel: Komfort und Sicherheit erhöhen und elektronischen Handel erleichtern.

Selbst Montulli scheint ratlos, wenn es um Schutz vor der Schnüffelei geht. Die guten alten Cookies seien ja harmlos im Vergleich zu den neuen Tracking-Methoden, sagt er. Fazit: „Wenn Ihnen das Thema am Herzen liegt, sollten Sie Lobbyarbeit für Kundenrechte machen."

23.21 UHR: Genervt greife ich zur Selbsthilfe und starte „Tor", einen Verschlüsselungsdienst. Tor verwischt meine Spuren, ein konspiratives Spezialwerkzeug, beliebt bei Hackern, Schlapphüten und Dissidenten in Diktaturen wie China.

Gern nutzt dieses Programm niemand. Tor ist langsam, Tor ist nervig. Es verspricht zwar etwas Schutz vor den Keks-Spionen. Doch das Dilemma zwischen Kostenloskultur und Datenschutz löst man so nicht

Hilmar Schmundt