Sven Venzke-Caprarese

Rote Karte für Webspione

YouTube-Videos datenschutzkonform einbetten

Das Einbetten von YouTube-Videos kann die eigene Website bereichern – manchmal allerdings mehr, als man denkt. Zu den Videoinhalten liefert die Google-Tochter nämlich etliche Cookies mit, die unter anderem dem Webtracking dienen. Website-Betreiber geraten so in eine rechtliche Grauzone – oft unbewusst. Ein Ansatz zu einer Lösung ist nur wenige Klicks entfernt.

YouTube-Videos dienen auf vielen Websites als bewegter Blickfang. Der Einbau ist für Site-Betreiber sehr bequem. YouTube erzeugt auf Wunsch einen Einbettungscode in Form einer HTML-Zeile, die man an geeigneter Stelle in den Code der Webseite übernimmt. Das Video wird dann per iframe angezeigt und abgespielt.

Um den Einbettungscode zu erhalten, genügt ein Rechtsklick auf das Video auf dem YouTube-Portal. Alternativ wählt man die unterhalb des Videofensters angebotene Option des „Teilens“ und gelangt nach einem Klick auf „Einbetten“ zu demselben HTML-Code.

Das Einbetten von YouTube-Videos via iframe hat insbesondere wegen urheberrechtlicher Fragen in der Vergangenheit die Öffentlichkeit und die höchsten Gerichte beschäftigt. 2014 hat allerdings der Europäische Gerichtshof (EuGH) entschieden, dass die Einbettung fremder Inhalte in die eigene Website mittels „Framing-Technik“ die Rechte von deren Urhebern nicht verletzt [1]. In Deutschland hat sich der Bundesgerichtshof dieser Sichtweise weitgehend angeschlossen [2]. Also ist zumindest an dieser Front erst einmal Entspannung eingekehrt. Die datenschutzrechtlichen Fragen, die mit einer Einbettung von YouTube-Inhalten verbunden sind, wurden bislang allerdings weniger beachtet.

Kleine Späher als ungebetene Begleiter

Website-Betreiber, die den von YouTube vorgegebenen Einbettungscode in der Standardeinstellung verwenden, sind möglicherweise überrascht, wenn sie das Verhalten ihrer Website anschließend näher betrachten: Beim Aufruf werden plötzlich etliche YouTube-Cookies im System des Website-Besuchers gesetzt. Manche davon weisen eine Lebensdauer von mehreren Jahren auf. Und nicht nur das: Bereits der Aufruf einer Seite mit eingebettetem YouTube-Inhalt führt dazu, dass eine Verbindung zum Google-Werbenetzwerk DoubleClick aufgebaut wird. Jedenfalls weisen Privacy-Werkzeuge wie „Ghostery“ darauf hin.

Die Firefox-Erweiterung „TamperData“ kann Header und POST-Parameter von Webseiten anzeigen und verändern, außerdem HTTP-Anfragen und -Reaktionen verfolgen. Ein Blick damit auf die Seite mit dem Video bestätigt den Verdacht: Schon deren bloßer Aufruf führt dazu, dass unter anderem eine Verbindung zu https://static.doubleclick.net aufgebaut und die Javascript-Datei „ad_status.js“ nachgeladen wird.

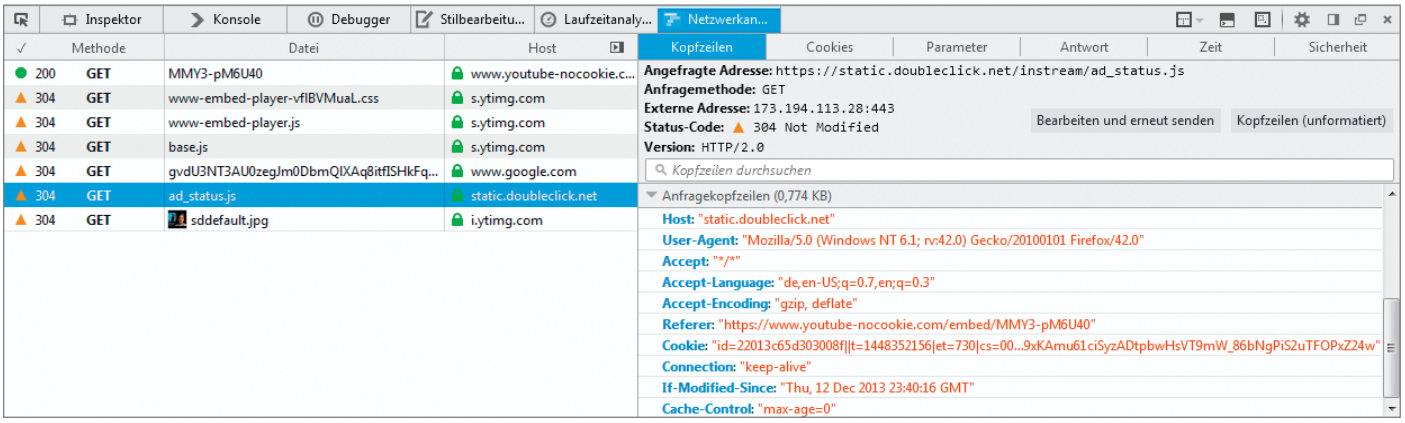
Dies geschieht auch dann, wenn das eingebettete Video selbst weder angeklickt noch abgespielt wird. Die Verbindung zu DoubleClick führt zwar nicht dazu, dass neben den YouTube-Cookies auch DoubleClick-Cookies gesetzt werden. Falls sich aber im Browser-Cache bereits einer der „Kekse“ des Werbenetzwerks befindet, werden die Cookie-IDs an DoubleClick übertragen.

Konflikte durch die Hintertür

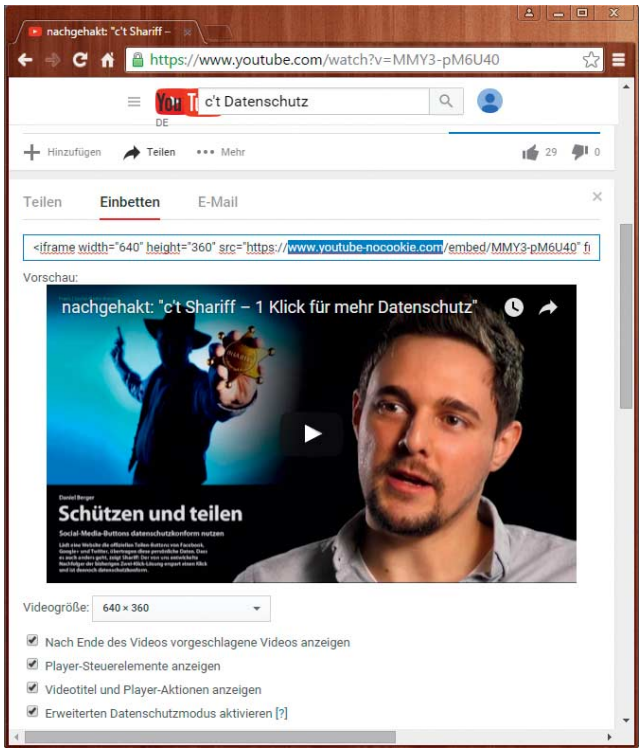
Rechtlich ist diese Situation für Website-Betreiber alles andere als komfortabel. Nach § 13 des Telemediengesetzes (TMG) müssen sie die Nutzer ihrer Seiten in der Datenschutzerklärung umfassend informieren. Das betrifft insbesondere die durch den Seitenaufruf gesetzten Cookies und die dadurch ausgelöste Datenverarbeitung. Was sich aber hinter den Cookies und hinter der Verbindung zum DoubleClick-Werbenetzwerk verbirgt, können Website-Betreiber nicht wirklich wissen – nur ahnen.

So lässt sich die wichtige Frage, wer eigentlich den Aufruf der eingebetteten Inhalte verfolgt, nicht belastbar beantworten. Ist es YouTube? Oder das DoubleClick-Netzwerk? Daraus ergibt sich eine weitere Unsicherheit. Wenn mit dem Seitenaufruf ein Web-Tracking einhergeht, müssen Website-Betreiber die Besucher nach § 15 Abs. 3 TMG darüber informieren und ihnen Gelegenheit zum Widerspruch geben. Es macht die Sache nicht einfacher, dass der Begriff Web-Tracking rechtlich gesehen eher weit zu fassen ist: Man versteht darunter nicht nur das Setzen neuer Tracking-Cookies, sondern auch das Auslesen gespeicherter Cookies und deren Verwendung – etwa zum Zweck der Werbung.

Die Verantwortung für ein möglicherweise unzulässiges Webtracking auf YouTube abschieben zu wollen, ist keine Lösung. Genau genommen setzt erst die Einbettung des Videos durch den Website-Betreiber die fragliche Datenverarbeitung in Gang. Die



Wer den Netzwerkverkehr genauer untersucht, stellt fest: Der Aufruf einer Webseite mit eingebetteten YouTube-Videos führt automatisch auch zu einer Verbindung mit dem DoubleClick-Netzwerk (links im Bild). Sofern aus vorherigen Sessions bereits DoubleClick-Cookies im Browser gespeichert sind, werden diese im Rahmen der Anfrage mit übertragen (rechts im Bild).



YouTube bietet die Möglichkeit, Videos im erweiterten Datenschutzmodus einzubetten. Die Option dafür muss man jedoch erst einmal finden.

Situation, in der dieser Betreiber sich dann wiederfindet, ist vergleichbar mit der Lage, die bei der direkten Einbindung von Social-Media-Plug-ins entsteht: Auch hier setzt der Aufruf der Seite, in die die Plug-ins eingebunden sind, den entscheidenden Mechanismus in Gang. Er ist es, der dem Betreiber der Social-Media-Plattform eine umfangreiche Datenverarbeitung ermöglicht.

Zurückhaltung auf Kommando

Als pragmatische Lösung bietet sich eine Option an, die YouTube seit Jahren bei der Erzeugung des Einbettungscodes anbietet, aber ausgesprochen gut versteckt: Man nimmt die Einbettung der Videos im „erweiterten Datenschutzmodus“ vor. Um diesen Modus zu aktivieren, ruft man zunächst die YouTube-Seite auf, auf der sich das eigentliche Video befindet. Nach der Wahl von „Teilen“, „Einbetten“ und „Mehr anzeigen“ erscheint schließlich die Option „Erweiterten Datenschutzmodus aktivieren“.

YouTube beschreibt dessen Arbeitsweise so: „Wenn du diese Option aktivierst, werden von YouTube keine Informationen über die Besucher auf deiner Website gespeichert, es sei denn, sie sehen sich das Video an“ [3]. Wenn das dazugehörige Auswahlkästchen aktiviert ist, ändert sich der im Einbettungscode vorgesehene Link: Aus „www.youtube.com“ wird „www.youtube-nocookie.com“.

Tatsächlich bedeutet der Datenschutzmodus ein geringeres Rechtsrisiko für Website-Betreiber. Die Überprüfung einer Seite mit einem solchermaßen eingebetteten Video zeigt, dass beim Aufruf tatsächlich keine Cookies mehr gesetzt werden. Allerdings finden sich unter anderem im „Local Storage“ des Webbrowsers noch Daten, die über die jeweilige Session hinaus gespeichert werden. Unter ihnen ist auch eine sogenannte Device-ID, deren Funktion unklar ist.

Auch wenn Videos im „erweiterten Datenschutzmodus“ in eine Webseite eingebettet worden sind, nimmt der Browser eines Besuchers beim Aufruf dieser Seite dennoch automatisch mit dem DoubleClick-Werbenetzwerk Kontakt auf. Dieser Umstand bleibt problematisch. Darf man Google an dieser Stelle vertrauen und davon ausgehen, dass tatsächlich keine Informationen des Besuchers gespeichert werden – zumindest solange dieser das eingebettete Video nicht ablaufen lässt? Schon aus rein pragmatischen Gründen werden viele Website-Betreiber sich darauf verlassen und verbleibende Restrisiken in Kauf nehmen. In ihren Datenschutzerklärungen sollten sie dann aber zumindest darauf hinweisen, dass YouTube-Videos im „erweiterten Datenschutzmodus“ in ihren Seiten eingebettet sind. Die Nutzer sollten erfahren, dass der Aufruf der Seiten zu einer Verbindungsaufnahme mit YouTube und dem DoubleClick-Netzwerk führt. Man sollte ihnen auch nicht verschweigen, dass schon ein Klick auf das Video weitere Datenverarbeitungsvorgänge auslösen kann, auf die der Website-Betreiber keinen Einfluss mehr hat.

Ein Klick für mehr Datenschutz?

Für denjenigen, der es genau nimmt, beantwortet auch die Einbettung von YouTube-Videos im „erweiterten Datenschutzmodus“ nicht alle datenschutzrechtlichen Fragen.

Es gibt eine Alternative, mit deren Hilfe Website-Betreiber durchaus den Einfluss und die Kontrolle über die mit dem Seitenaufruf zusammenhängende Datenverarbeitung zurückgewinnen: Ähnlich wie schon bei der Frage der datenschutzkonformen Einbindung von Social-Media-Plug-ins kommt auch für die Einbettung von YouTube-Videos eine Lösung in Betracht, welche beim Seitenaufruf nur ein vom eigenen Webserver geladenes Vorschaubild anzeigt und die eigentlichen Video-Inhalte erst nach einem Klick auf das Vorschaubild nachlädt beziehungsweise abspielt.

Ein Beispiel für eine solche Umsetzung zeigt etwa der Internet-Auftritt des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz unter www.youngdata.de/google/facts. Hier wird beim Seitenaufruf lediglich ein Vorschaubild angezeigt, welches der Server des Site-Betreibers ausliefert. Sobald der Nutzer mit der Maus über das Bild fährt, erscheint folgender Hinweistext: „Zum Aktivieren des Videos musst Du auf den Link unten klicken. Wir möchten Dich darauf hinweisen, dass nach der Aktivierung Daten an den jeweiligen Anbieter übermittelt werden.“

Wenn der Nutzer auf den Link klickt, wird das YouTube-Video im „erweiterten Datenschutzmodus“ eingebettet und gestartet. Diese Lösung führt dazu, dass Daten erst dann an Dritte übertragen werden, wenn der Besucher die Funktionen des eingebundenen Inhalts auch tatsächlich nutzt. Bemerkenswert ist, dass die auf youngdata.de präsentierte Lösung auf einem eigens entwickelten Typo3-Plug-in beruht. Dieses ist allerdings bislang nicht öffentlich verfügbar, sondern wurde zunächst nur Landesbehörden in Rheinland-Pfalz zur Verfügung gestellt [4].

Gesucht: ein Königsweg für alle

Es bleibt zu hoffen, dass sich für eingebettete YouTube-Inhalte künftig ähnliche Lösungen etablieren, die Website-Betreiber ohne großen Aufwand nutzen können. Zu klären wären zuvor allerdings wieder mal urheberrechtliche Fragen: Es ist durchaus möglich, dass die Anzeige eines Vorschaubildes die Rechte des Video-Urhebers verletzt. Die eingangs erwähnten Gerichtsentscheidungen des EuGH und des BGH stellen nämlich nur für die Einbindung via iframe einen Freibrief aus. Gerade eine solche Einbindung will man bei der dargestellten Lösung im Hinblick auf das Vorschaubild aber vermeiden.

Möglicherweise gibt das Zitierrecht des § 51 im deutschen Urheberrechtsgesetz (UrhG) eine Grundlage für die Verwendung eines Thumbnails her. Auch eine passende Anwendung der BGH-Urteile zur rechtmäßigen Verwendung von Vorschaubildern durch Suchmaschinenbetreiber [5] kommt in Betracht. Solche Überlegungen sind aber spekulativ. Je nachdem, welche Video-Inhalte man auf diesem Umweg einbetten will, ist jedenfalls Vorsicht geboten. (psz@ct.de)

Literatur

[1] EuGH, Beschluss vom 21. 10. 2014, Az. C-348/13 (alle Online-Fundstellen siehe c’t-Link)
[2] BGH, Urteil vom 9. 7. 2015, Az. I ZR 46/12
[3] Videos und Playlists einbetten, Erläuterungsseite von Google in der YouTube-Hilfe
[4] 24. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (Ziffer III.1.3)
[5] BGH, Urteil vom 29. 4. 2010, Az. I ZR 69/08 (Vorschaubilder I); BGH, Urteil vom 19. 10. 2011, Az. I ZR 140/10 (Vorschaubilder II)

c't Dokumente und Entscheidungen: ct.de/yyrw