

D A T A
D E T O X
K I T



EIN LEITFADEN FÜR WÄHLER:INNEN

7 Tipps für deinen Daten-Detox



WIE NUTZEN POLITISCHE KAMPAGNEN MEINE DATEN, UM MICH AUF IHRE SEITE ZU ZIEHEN?

Vermutlich stößt du überall auf politische Werbung: von den Websites, die du besuchst, über deinen Social-Media-Feed bis hin zu Flugblättern in deinem Briefkasten. Scheinbar dreht sich alles um die Themen, die dir am wichtigsten sind! Und das ist kein Zufall.

Je mehr politische Kampagnen über dich wissen, desto besser können sie Einfluss auf dich ausüben – ganz egal, ob es darum geht, dich als Freiwillige(n) anzuwerben, dich zu einer Spende zu bewegen, deine Stimme zu beeinflussen oder dich am Wahltag ins Wahllokal zu locken.

Zum Glück für die Kampagnen ist es ein Leichtes, Informationen darüber zu finden, wer du bist und wie man deine Aufmerksamkeit gewinnt. Politische Werbung wird zunehmend von den Informationen geprägt, die du in deinem Leben hinterlässt, sowohl online als auch offline. Politische Kampagnen sammeln diese Daten über dich an vielen verschiedenen Orten und nutzen sie, um ein Profil von dir zu erstellen. Anhand dieses Profils können sie herausfinden, welche Kandidat:innen oder politischen Fragen du am ansprechendsten findest, und ihre Botschaften direkt auf dich zuschneiden.

Basierend auf deinem Profil sendet dir eine Kampagne möglicherweise personalisierte politische Botschaften via:

Broschüren, die nach Hause geliefert werden

exklusive Snapchat-Filter

Aufforderungen zum Herunterladen einer offiziellen Kampagnen-App

Werbung auf YouTube oder deinem Smart-TV

E-Mails, Textnachrichten oder Anrufe

der Website eines/einer Kandidat:in

Jetzt fragst du dich vielleicht, ob spezifischere, relevantere Anzeigen nicht besser für dich geeignet wären. Aber denk daran, dass die heutigen digitalen Kampagnen möglicherweise Informationen über deine Gewohnheiten und Interessen verwenden, die du lieber privat halten würdest. Dazu können Details gehören, die nicht einmal als politisch wahrgenommen werden, wie die Websites, die du besuchst, oder die Waren, die du in Geschäften kaufst.

Du hast das Recht zu erfahren, wie deine Informationen verwendet werden, insbesondere wenn sie genutzt werden, um dich vor einer Wahl zu überzeugen oder zu beeinflussen. Tactical Tech hat einige der verbreitetsten datengesteuerten Kampagnentechniken untersucht, die Profile von Wähler:innen auf der ganzen Welt erstellen und sie zu beeinflussen versuchen.

Dieser Data-Detox-Leitfaden für Wähler:innen beschreibt einige der verbreitetsten Methoden, die Kandidat:innen nutzen, um sich deine Unterstützung zu sichern. Wenn du deine Stimme abgibst, solltest du genau wissen, wie und wann diese Überzeugungstechniken bei dir angewendet werden.

1.

WOHER BEKOMMEN KAMPAGNEN INFORMATIONEN ÜBER MICH?

Politiker:innen, politische Parteien und politische Kampagnen interessieren sich für dein Einkaufsverhalten, deinen Lebensstil, deine Online-Aktivitäten und vieles mehr. Aber wie erhalten sie Zugang zu diesen Daten?

Da gibt es eine Reihe von Möglichkeiten: Die Infos können von führenden Datenbrokern, großen Technologieunternehmen, Wählerdatenbanken und anderen bereitgestellt werden.

GROSSE TECHNOLOGIEUNTERNEHMEN: Unternehmen wie Google und Facebook sind für politische Parteien offene Türen zu deinen Daten. Google und Facebook dominieren die digitale Werbebranche, weil sie so viele Daten über ihre Milliarden Nutzer besitzen. Diese reichhaltigen Daten führen dazu, dass Kunden, die auf Google oder Facebook werben möchten – einschließlich Politiker:innen und politische Parteien – Anzeigen kaufen können, die auf ihre bevorzugte Zielgruppe ausgerichtet sind. Politische Parteien und Kandidat:innen geben den Großteil ihres Budgets für diese „Mikrotargeting“-Werbung aus.

DATENBROKER UND POLITISCHE BERATER:INNEN: Politische Kampagnen können Daten über dich auch von Datenbrokern kaufen. Dabei handelt es sich um große Unternehmen, die oft unglaublich detaillierte Daten über Millionen von Menschen auf der ganzen Welt besitzen. Politiker:innen können diese ausführlichen Daten nutzen, um mehr über ihre Unterstützer:innen oder potenziellen Wähler:innen zu erfahren. Neben Datenbrokern bieten auch Politikberater:innen Wahlkämpfen ihre eigenen maßgeschneiderten Wählerdatensätze an.

ANDERE QUELLEN: Politische Kampagnen können auch Daten über Wähler aus vielen anderen Quellen erhalten, darunter:

- offizielle Wählerregistrierungsunterlagen
- Unterstützerdatenbanken
- Umfragen und Studien, die durch Kundenwerbung und Telefonbanking durchgeführt werden
- Aufzeichnungen der Regierung über die Wahlbeteiligung und erfolgreiche Kandidat:innen aus vergangenen Wahlen in deiner Region

Sogar Details darüber, wo du einkaufst, was du kaufst, was du online postest, deine Kreditwürdigkeit und deine Ausbildung liefern politischen Parteien mehr Informationen, anhand derer sie lernen, dich zu verstehen und zu erreichen.

TIPP 1: Ändere deine Gewohnheiten

Wenn dein Konsumverhalten für politische Kampagnen so wertvoll ist, warum veränderst du es nicht einfach? Du könntest deiner Kundenkarte eine Pause gönnen, im stationären Handel gelegentlich mit Bargeld bezahlen oder es dir zweimal überlegen, ob du dich für regelmäßige Newsletter anmeldest und deine Kontaktdaten angibst.

Wenn du herausfinden möchtest, wie Verbraucherdaten genutzt werden, um Kampagnen voranzutreiben, dann wirf einen Blick auf : <https://ourdataourselves.tacticaltech.org/posts/consumer-data>



→ 2.

WAS SAGEN MEINE SOZIALEN MEDIEN ÜBER MICH AUS?

Hast du über eine Demonstration zum Klimawandel getwittert? Verwendest du Ausrufezeichen in deinen Facebook-Posts, um deine Zweifel auszudrücken? Das mag nach harmlosen Details klingen, aber Hinweise wie diese können politischen Parteien, die dich erreichen wollen, viel über dich verraten. Durch Analyse deiner Beiträge in den sozialen Medien können Unternehmen verstehen, wie du tickst und klickst – ob du wütende oder traurige Nachrichten, blaue oder orange Farben magst oder wie deine Einstellung einem bestimmten Problem gegenüber ist.

Die Methode, anhand deiner Aussagen in den sozialen Medien (und wie du diese triffst), herauszufinden, woran du interessiert bist, nennt man **Digital Listening**. Das „Belauschen“ der sozialen Medien von Personen kann Kandidat:innen Aufschlüsse darüber geben, was die Öffentlichkeit über sie denkt. Auf diese Weise kann dieses Verfahren Kampagnen dabei unterstützen, die Themen zu identifizieren, die den Wähler:innen wichtig sind. So können sogar politische Einflussnehmer:innen lokalisiert werden, indem in Erfahrung gebracht wird, wer das politische Narrativ prägt.

Nachdem analysiert wurde, was auf Twitter über ein weites Themenfeld vom Brexit bis zur Marihuana-Gesetzgebung gesagt wird, könnte eine Kampagne beispielsweise drei Botschaften erstellen: eine für diejenigen, die es leid sind, über ein bestimmtes Thema zu sprechen, und jeweils eine für diejenigen, deren Meinung in die eine oder andere Richtung tendiert.

Eine weitere Möglichkeit, wie Kampagnen Daten über deine Online-Aktivitäten sammeln können, besteht darin, verschiedene Variationen einer Anzeige oder E-Mail zu testen. Dies wird als **A/B-Testing** bezeichnet. Die Wahlkämpfer:innen können so analysieren, welche Inhalte, Farben und Schlagzeilen dich dazu bringen, zu spenden, zu liken oder etwas in deinen sozialen Medien zu teilen.

Unternehmen oder Organisationen sind sich nicht immer darüber im Klaren, ob sie das Verhalten in sozialen Medien überwachen. Dadurch wird es schwierig, mit Sicherheit zu sagen, ob du „belauscht“ wirst. Du solltest jedoch davon ausgehen, dass deine Beiträge, Klicks und Antworten verwendet werden können, um nachzuvollziehen, welche politischen Themen dich interessieren, wenn du in einem öffentlichen Online-Raum wie Twitter deine Meinung kundtust, ein öffentliches Facebook-Konto besitzt oder in öffentlichen Facebook-Gruppen Beiträge verfasst und mitteilst, wie du zu einem bestimmten Thema stehst.

TIPP 2: Passe deine Social-Media-Einstellungen an

Es gibt einige Schritte, die du auf Social-Media-Plattformen unternehmen kannst, um den Umfang der Nutzung deiner Daten für zielgerichtete politische Werbung zu reduzieren.

Überprüfe deine Profilooptionen und -einstellungen auf Möglichkeiten zum Ändern der Anzeigen- und Marketingpräferenzen und/oder zum Löschen deines Aktivitätsverlaufs auf verschiedenen Plattformen, um diese weniger mit deinen Online-Aktivitäten zu verknüpfen.

Lies doch mal: <https://datadetoxkit.org/en/privacy/profile>



3.

HABE ICH DER WEITERGABE MEINER DATEN ZUGESTIMMT?

Politische Parteien müssen deine Erlaubnis einholen, bevor sie deine personenbezogenen Daten erheben können. Wenn du allerdings auf einer Website, einem Newsletter oder in einer App auf „**Akzeptieren**“ klickst, ist möglicherweise nicht klar, welche personenbezogenen Daten du preisgibst. Wenn das Kleingedruckte in Datenschutzrichtlinien oder Haftungsausschlüssen unklar oder versteckt ist, kann es schwierig sein, genau zu wissen, welche Daten erfasst und wie diese verwendet werden.

Vielleicht hast du schon einmal gesehen, dass dir dieselbe Anzeige überall im Internet folgt. Das ist kein Zufall! Unternehmen verwenden eine Kombination aus Cookies und Tracking-Pixeln (zusammen mit anderen Tools), um Benutzer:innen zu orten, während sie im Internet surfen oder über ein Mobiltelefon auf Dienste zugreifen. Diese Tools ermöglichen es Werbetreibenden zudem, dich mit einer zielgerichteten Anzeige zu verfolgen.

Eine politische Partei kann beispielsweise deinen Klick auf ihre Facebook-Werbung verfolgen, die mit ihrer Website verlinkt ist, und dadurch sehen, welche Teile ihrer Website du ansiehst, z. B. ihre Bildungspolitik oder Spendenseite. Anhand dieser Informationen können sie dich dann mit einer auf diesen Themen basierenden Anzeige ansprechen, und die dieselbe Anzeige auf anderen unabhängigen Websites anzeigen, die du besuchst.

Organisationen, die Websites betreiben, müssen dazu zwar deine Zustimmung einholen, allerdings klickst du höchstwahrscheinlich auf „Alle Cookies akzeptieren“. Dies stellt oft die einzige Möglichkeit dar, schnell auf die Informationen der Website zugreifen zu können. Dadurch verlierst du gegebenenfalls die Kontrolle darüber, wie deine personenbezogenen Daten verwendet werden.

TIPP 3: Sichere deine mobilen und Desktop-Browser ab

Du kannst Folgendes tun, um einigen dieser von politischen Parteien genutzten Online-Tracker einen Schritt voraus zu sein:

Verwende, sofern möglich, den Privat-/Inkognito-Browsing-Modus

Installiere Browsererweiterungen wie

Privacy Badger: <https://www.eff.org/privacybadger>

uBlock Origin: <https://github.com/gorhill/uBlock>

um Tracker abzuwehren. (Da es sich hierbei um Browser-Erweiterungen handelt, siehst du weiterhin gezielte Werbung in den von dir verwendeten Apps.)

Aktiviere „Do Not Track“ in deinen Browsereinstellungen (Websites müssen sich nicht daran halten, aber diese Funktion gibt ihnen zu verstehen, dass du mit dem Tracking nicht einverstanden bist).

Nutze die anderen Ressourcen des Data Detox Kits, um die Kontrolle über das Anzeigen-Tracking zu übernehmen



WIE WERDEN POLITISCHE ANZEIGEN AUF MICH AUSGERICHTET?

Social-Media-Plattformen haben Zugriff auf alle möglichen potenziell nützlichen Daten über Wähler:innen, was sie perfekt für politische Kampagnen macht. Die Kampagnen können Facebook (zu dem Instagram gehört), Google (zu dem YouTube und die Google-Suche gehört) und Snapchat verwenden, um dich mit gezielten Anzeigen auf der Grundlage von Kategorien wie Alter, Standort und Geschlecht anzusprechen. Sie können aber auch sehr spezifische Informationen verwenden, z.B. welche Art von Inhalten du auf deinen Plattformen ansiehst, was du „likst“ oder kommentierst.*

Darüber hinaus bieten Social-Media-Plattformen besondere Dienste speziell für politische Kampagnen an. Vielleicht ist dir gar nicht bewusst, dass Facebook es politischen Kampagnen ermöglicht, ihre Wählerlisten auf Facebook hochzuladen, damit sie personalisierte Werbung nur an die Personen auf diesen Listen senden können. Facebook gestattet politischen Werbetreibenden sogar, direkt auf Personen mit ähnlichen Profilen wie die Wähler:innen auf ihren Listen abzu zielen.

Facebook hat politischen Kampagnen zudem geholfen, ihre Anzeigen basierend auf den psychologischen Merkmalen der Benutzer zu optimieren und auszurichten. Der Fall Cambridge Analytica hat gezeigt, wie eine Datenfirma große Mengen von Facebook-Daten verwendet hat, um Wähler:innen in Profile einzuteilen, je nachdem, für wie „offen, gewissenhaft, extrovertiert, umgänglich oder neurotisch“ sie gehalten wurden. Obwohl die meisten Menschen von Cambridge Analytica gehört haben, ist womöglich unbekannt, dass diese und ähnliche Techniken von vielen anderen Unternehmen genutzt werden, um ein Profil von dir als Verbraucher:in oder Wähler:in zu erstellen.

TIPP 4: Bleib informiert

Um mehr Einblick in die politische Werbelandschaft zu gewinnen, kannst du dir Folgendes ansehen:

Facebook-Werbebibliothek:

<https://de-de.facebook.com/ads/library>

Google Transparency Report:

<https://adstransparency.google.com/political>

Snap Political Ads Library:

<https://www.snap.com/de-DE/political-ads>

Du kannst diese Ressourcen nutzen, um einzusehen, wie viel Geld Kampagnen für welche Anzeigen an welchen Standorten ausgegeben haben, sowie einige grundlegende Informationen zur demografischen Ausrichtung zu erhalten. Diese Transparenz-Tools sind jedoch noch nicht in allen Ländern verfügbar, in denen politische Werbung unterstützt wird.

Außerdem kannst du einen Blick auf das **Ad.Watch-Projekt**: <https://ad.watch> werfen, welches eine andere Version der Facebook-Werbebibliothek bietet, oder die Installation der „**Who Targets Me**“-Erweiterung: <https://whotargets.me/> in Betracht ziehen, um das Crowdsourcing politischer Anzeigen auf Facebook zu unterstützen.

*Hinweis: Seit November 2019 überarbeiten viele Unternehmen, darunter Facebook, Twitter und Google, ihre Richtlinien für politische Werbung auf ihren Plattformen (oder erwägen Berichten zufolge eine Überarbeitung).



WOHER KENNEN KAMPAGNEN MEINE POLITISCHE EINSTELLUNG?

Dein Standort sagt viel über dich aus. Allein zu wissen, in welcher Stadt und in welcher Nachbarschaft du wohnst, kann viel darüber preisgeben, welche Themen dir wichtig sind. Das Gleiche gilt für Informationen darüber, wohin du gehst.

Deine Anwesenheit in einer bestimmten Kneipe an einem Freitagabend oder in einer Andachtsstätte kann beispielsweise Informationen über deine Einstellung zu bestimmten Themen vermitteln, was für politische Kampagnen wertvoll ist. Wenn diese deine politische Ausrichtung kennen, können sie mit bestimmten Anzeigen deine Aufmerksamkeit erregen – oder dich auch einfach ignorieren.

Standortdaten sind nicht nur Informationen darüber, wo du dich auf einer Karte befindest. Sie zeichnen auch ein Bild davon, was du gerne tust und woran du interessiert bist. In praktisch jedem Wahlkampf auf der ganzen Welt wird irgendeine Form von Standortdaten verwendet, um auf Menschen abzu zielen.

Nahezu alle Kampagnen nutzen große Technologieplattformen, um Werbung geografisch auszurichten (basierend darauf, wo du dich befindest und wohin du gehst). Dies geschieht unabhängig davon, ob es sich um eine bestimmte Stadt, ein spezielles Viertel, eine Nachbarschaft oder sogar einen einzelnen Haushalt handelt.

Geotargeting kann viele Formen annehmen, aber die drei häufigsten Arten sind:

- Erstellung einer virtuellen „Geozone“ um einen bestimmten Punkt in der realen Welt (z. B. ein bestimmtes Gebäude oder Ereignis), der eine politische Botschaft auslöst, wenn Personen ihn passieren
- Ermittlung der ungefähren Standorte von Wähler:innen anhand ihrer IP-Adressen
- Verwendung von demografischen Informationen wie Postleitzahlen, um politische Botschaften an die Wähler:innen zu richten

Nicht nur Unternehmen, die sich auf Dienste für politische Kampagnen spezialisiert haben, führen diese Art von standortbasiertem Targeting durch. Es ist bekannt, dass auch andere Unternehmen, die Standortinformationen sammeln oder Zugriff darauf haben, diese Daten an politische Parteien weitergeben. Beispielsweise lieferte die Weather Channel App Standortinformationen für politische Anzeigen, während Snapchat eine beliebte Plattform für politische Parteien ist, um Wähler mit Werbung basierend auf ihrem Standort anzusprechen.

TIPP 5: Lass nicht jeden wissen, wo du dich aufhältst

Denkst du darüber nach, an einer politischen Kundgebung oder Demonstration teilzunehmen oder einfach nur in dein Wahllokal zu gehen? Dann ergreife einige Maßnahmen gegen standortbasiertes Targeting, indem du deine Standortdaten im Auge behältst.

Lösche deine Standortspuren von deinen Mobilgeräten:
<https://datadetoxkit.org/en/privacy/essentials#step-2>



→ 6.

VERSCHAFFE DIR GEHÖR



Wenn du mehr dafür tun willst, die Kontrolle darüber zu erlangen, wie deine personenbezogenen Daten bei Wahlen verwendet werden, dann kannst du helfen, andere aufzuklären.

TIPP 6: Sprich das Thema an

Sprich mit Vertreter:innen und politischen Parteien in deiner Nähe oder schreibe sie an und frage nach, wie sie deine Daten in ihrer politischen Kampagne verwenden.

Falls du Bedenken hinsichtlich einer bestimmten Praxis hast, wie beispielsweise der Erstellung von standortbezogenen Profilen, schreibe den Wahlbehörden oder rufe sie an, um ihnen deine Meinung mitzuteilen.

7. ←

BEZIEHE STELLUNG

Die komplexe und unklare Art und Weise, wie diese Wahlkampftechnologien eingesetzt werden, kann dazu führen, dass du dich zunehmend entmutigt und von einem der wichtigsten Prozesse in einer Demokratie – dem Wahlakt – losgelöst fühlst. Wenn du verstehst, wie deine Daten verwendet werden, um dich bei einer Wahl zu beeinflussen, bist du in der Lage, fundiertere politische Entscheidungen treffen. Falls du andere dazu befähigen willst, dasselbe zu tun, dann gib diese Informationen weiter.

TIPP 7: Informiere deine Community

Sprich mit deinen Freunden und deiner Familie darüber, wie deine (und deren) Informationen während der Kampagnensaison verwendet werden und wie sich dies auf euch auswirkt. Je mehr Menschen Bescheid wissen und je mehr Wirbel um das Thema entsteht, desto wahrscheinlicher ist es auch, dass es angesprochen wird, also teile diesen Leitfaden bitte mit anderen!