EMMA MOORE/DIE POSAUNE

Spioniert Ihr Kaffeehaus Sie aus?

Die Gefahren einer Gesellschaft, in der alles beobachtet wird

- Richard Palmer
- 05.09.2022

I n Kanada ist Tim Hortons überall vertreten. Mit 4300 Filialen gibt es dort etwa dreimal so viele wie McDonalds. Achtzig Prozent der Kanadier gehen mindestens einmal im Monat dorthin.

Und Tim Hortons schaut zu.

Sechs Millionen Kanadier, bei einer erwachsenen Bevölkerung von 31 Millionen, nutzen die Tim Hortons-App, um ihre Getränke zu bestellen. Einer von ihnen war James McLeod von der *Financial Post*, der bemerkte, dass die App seinen Standort verfolgte und einen Antrag auf Informationsfreiheit stellte, um mehr zu erfahren. „Von meinem Zuhause über mein Büro bis hin zu einem Spiel der Blue Jays im Rogers Centre und sogar bis nach Marokko, wo ich im vergangenen Juni Urlaub machte, hat die App des Unternehmens meine Koordinaten aufgezeichnet und an die Server des Unternehmens weitergeleitet“, schrieb McLeod. Anhand dieser Daten fand Tim Hortons heraus, wo McLeod wohnte.

Wenn Ihnen Ihre Privatsphäre am Herzen liegt, dann ist klar, was Sie tun müssen: Machen Sie Ihren eigenen Kaffee.

Aber selbst das könnte nicht ausreichen. Christopher Balding von New Kite Data Labs entdeckte in China hergestellte intelligente Kaffeemaschinen, die Daten nach Peking zurücksenden. Die Kalerm-Maschinen sammelten Informationen darüber, wer sie benutzte, wo sie wohnten, und, wenn sie kommerziell genutzt wurden, auch Zahlungsdaten.

Es ist leicht, solche „Skandale“ abzutun. „Was soll’s?“ werden Sie vielleicht denken. *„Die Kommunistische Partei Chinas weiß, wie ich meinen Kaffee mag.“*

Aber hier geht es um weit mehr als nur um Kaffee. Es ist ein Beispiel dafür, wie verbreitet und sogar alltäglich High-Tech-Überwachung geworden ist.

Zu verkaufen: Sie

Die Kombination von Smartphones und Smart-Homes bedeutet, dass eine noch nie dagewesene Menge privater Daten öffentlich zugänglich ist. Oft sind Ihre Standortinformationen für den Meistbietenden käuflich.

Viele Verkäufer wollen ihr Produkt genau an den richtigen Verbraucher zur richtigen Zeit und am richtigen Ort vermarkten, um ihre Chancen auf einen Verkauf zu maximieren. Dies ist so üblich und automatisiert geworden, dass wir daran gewöhnt sind. Wenn Sie auf Amazon nach Schuhen suchen, werden Sie deshalb noch wochenlang im Internet mit Anzeigen für genau diese Größe und diesen Schuhtyp verfolgt.

Jetzt passiert das auch offline. Laden Sie die App eines Geschäfts oder Einkaufszentrums herunter, und es werden Ihnen wahrscheinlich einige exklusive Angebote gemacht. Die App kann auch aufzeichnen, wo Sie im Geschäft die meiste Zeit verbracht haben und welche Artikel Sie sich wahrscheinlich angesehen haben. Die Produkte, die Sie sich offline angeschaut haben, werden Sie nun auch im Internet verfolgen.

Diese Daten werden kombiniert und verkauft – vielleicht für Marketingzwecke, vielleicht aber auch für andere Zwecke. Es ist

schwer vorstellbar, dass eine Liste mit Daten von Vergewaltigungsopfern oder Opfern häuslicher Gewalt einen unschuldigen Zweck erfüllen könnte. Aber es ist alles verfügbar: Für ungefähr 80 Euro erhalten Sie die persönlichen Daten von 1000 vergewaltigten Frauen.

Einige der wichtigsten Abnehmer dieser Art von Daten sind Regierungen. In den Vereinigten Staaten kaufen der Internal Revenue Service, das Department of Homeland Security und andere Bundesbehörden Daten von Unternehmen wie X-Mode und Venntel. X-Mode sammelt Daten aus über 100 verschiedenen Anwendungen. Der demokratische Senator Ron Wyden beschuldigte die Regierung, „ihre Kreditkarte zu benutzen, um die Verfassung zu umgehen und sensible Informationen ohne Durchsuchungsbefehl zu kaufen." Die Anwälte der Regierung behaupten, dass die Regierung die verfassungsmäßigen Beschränkungen für staatliche Schnüffelei ignorieren kann, weil die Verbraucher ihre Daten freiwillig an diese Apps weitergeben.

In Kanada nutzen nicht nur Coffeeshops diese Daten. Im Dezember 2021 gab die kanadische Gesundheitsbehörde zu, dass sie während der Pandemie 33 Millionen Handys überwacht hat. Sie hatte einen Vertrag mit BlueDot abgeschlossen, um zu verfolgen, wie genau sich die Kanadier an die Abriegelungsmaßnahmen hielten, wann die Menschen ihre Häuser verließen, wie weit sie reisten und wie lange sie unterwegs waren.

Das vielleicht beunruhigendste Beispiel betrifft die Proteste am 6. Januar 2021 vor dem US-Kapitol. Das FBI (Bundeskriminalamt) nutzte Daten von Google, um die Teilnehmer zu verfolgen, und stellte dann über 10 000 Haftbefehle aus. Hier bestraft die Regierung diejenigen, die an einem Protest teilgenommen haben, der ihr nicht gefällt, und verwendet dazu Smartphone-Daten.

Wer hört zu Hause mit?

Diese Praktiken halten Einzug in die Haushalte. Wie Smartphone-Daten stehen auch Smart-Home-Daten zum Verkauf. „Die kontinuierliche Einbindung der Kunden und die Bereitstellung eines hervorragenden Kundenerlebnisses wird viel einfacher, wenn man weiß, was im Leben des Kunden zu einem bestimmten Zeitpunkt passiert", rühmt sich ein Datenbroker.

Welche Art von Daten könnten das sein? „Was die Verbraucher morgens als Erstes tun, wie sie mit Ihrem Gerät interagieren, wo sie das Wochenende verbringen und so weiter", heißt es auf der Website. „Diese Daten können dazu verwendet werden, das Verhalten Ihrer Kunden besser zu verstehen.

Die Sicherheitsvorkehrungen bei intelligenten Geräten sind notorisch schlecht, so dass Sie möglicherweise nicht nur von Datenmaklern beobachtet werden. Nehmen Sie Smart-TVs mit eingebauter Kamera. Die FBI-Außenstelle in Portland warnte: „Abgesehen von dem Risiko, dass Ihr Fernsehgerätehersteller und App-Entwickler Sie abhören und beobachten kann, kann der Fernseher auch ein Einfallstor für Hacker sein, die in Ihr Haus eindringen wollen.

Zu denjenigen, die sich in diese Geräte einschleusen, gehören auch Geheimdienste. WikiLeaks veröffentlichte Details zu einem Tool namens Weeping Angel, das von der CIA (Zentrale Geheimdienstbehörde) und dem MI5 entwickelt wurde und Samsung-Smart-TVs in verdeckte Maulwürfe verwandelte. Es ermöglichte diesen Behörden den Zugriff auf das Mikrofon, die Wi-Fi-Anmeldedaten und den Browserverlauf.

Hersteller von intelligenten Lautsprechern und Heimkameragerät geben in der Regel Daten an die Regierung weiter, wenn sie einen Durchsuchungsbefehl erhalten. Einige Hersteller sind sehr undurchsichtig, was ihre Beziehung zur Regierung angeht, sodass es schwer ist, zu wissen, wie viel sie weitergeben. Aber zumindest sind diese Beziehungen durch Durchsuchungsbefehle eingeschränkt – obwohl die Proteste vom 6. Januar zeigen, dass dieser rechtliche Vorbehalt auch missbraucht werden kann.

In Übersee kann man sich leicht schlimmere Ergebnisse vorstellen. Schottland hat vor kurzem die Gesetze über „Hassreden" auf den privaten Bereich ausgedehnt. Bestimmte Äußerungen sind sogar im privaten Umfeld gesetzlich verboten. Wie lange wird es dauern, bis jemand für Kommentare belangt wird, die über seinen intelligenten Lautsprecher abgehört wurden?

Die Verbindungen zu China sind sogar noch bedenklicher. Die Kaffeemaschinen von Kalerm sind nicht die einzigen intelligenten Geräte, die von Unternehmen mit Verbindungen zur Kommunistischen Partei Chinas hergestellt werden. „China sammelt Daten über wirklich alles und jeden", sagte Christopher Balding. „Als Produktionszentrum der Welt können sie diese Fähigkeit in alle Arten von Geräten einbauen, die in die ganze Welt gehen" (*Washington Post,* 14. Juni).

Mikrofone sind in immer mehr Geräten zu finden. Das gilt nicht nur für den intelligenten Lautsprecher von Amazon. Es ist auch der intelligente Staubsauger oder Wasserkocher einer wenig bekannten chinesischen Marke.

Einer der größten Akteure auf dem Smart-Home-Markt ist Tuya; mehr als 5000 Handelsmarken nehmen Tuya-Geräte in ihr Sortiment auf. Das Unternehmen verkauft über 1000 verschiedene Arten von intelligenten Geräten und hat weit über 100 Millionen Produkte verkauft. Wie alle chinesischen Unternehmen sind sie verpflichtet, alle von der chinesischen Regierung geforderten Daten herauszugeben. Tuya könnte „die Massen an Daten – einschließlich geheimer Regierungsdaten –, die in seinen Netzwerken erstellt und geteilt werden, abschöpfen und der chinesischen Regierung zur Verfügung stellen", schrieb der *Hill.* „Es ist gut möglich, dass Tuya die von Sicherheitskameras und angeschlossenen Gesundheitsgeräten erfassten Informationen – um nur zwei Beispiele zu nennen – zurück nach Peking leitet" (30. Juli 2021).

Letztes Jahr wählte das Sicherheitsunternehmen Dark Cubed 10 in den USA verkaufte intelligente Geräte aus. Jedes

einzelne hatte eine Geschäftsverbindung nach China und jedes Produkt wurde dabei beobachtet, wie es ohne unsere Erlaubnis mit der Infrastruktur in China kommunizierte“, schrieb es.

Schlafwandelnd in die Überwachung

Im Juni lieferte China ein alarmierendes Beispiel dafür, was diese Technologie möglich macht.

Einigen chinesischen Banken ging das Bargeld aus und sie begannen, einige Einleger am Abheben von Geld zu hindern. Wütende Einleger planten einen Protest in der Provinz Henan. Ihr Plan scheiterte.

In China ist für das Reisen ein Covid-Pass erforderlich. Diejenigen, die protestieren wollten, sahen plötzlich, dass ihre Gesundheitskarten rot wurden und sie an Ort und Stelle festhielten. Andere, die zwar nach Henan reisen, aber nicht protestieren wollten, waren davon nicht betroffen. *Die Regierung wusste, wer wahrscheinlich protestieren würde, und sperrte sie elektronisch ein.* „Sie legen uns digitale Handschellen an“, beschwerte sich ein gescheiterter Demonstrant. Ein anderer sagte: „Ich kann nichts tun; ich kann nirgendwo hingehen. Man wird behandelt, als wäre man ein Krimineller“.

Die US-Regierung verhaftet bereits Teilnehmer an einer Demonstration, die ihr missfiel. Dass sie ähnliche Maßnahmen wie China ergreift, ist daher nicht schwer, sich vorzustellen.

Doch im Allgemeinen sind wir bemerkenswert unbesorgt über all diese Überwachung. Oder besser gesagt, viele sind besorgt, aber nicht genug, um etwas dagegen zu unternehmen. Wir sind nicht scharf darauf, dass Unternehmen uns verfolgen und unsere Daten verkaufen, aber nicht ausreichend motiviert, um unser Verhalten zu ändern oder diese Unternehmen zu zwingen, sich zu ändern. Intelligente Technik ist einfach zu bequem.

Aber diese Technologie verschafft den Regierungen auf der ganzen Welt einen noch nie dagewesenen Einblick in unser Leben. Und das gibt ihnen eine noch nie dagewesene Macht.

„Staatliche Tyrannei ist Routine in der menschlichen Geschichte“, schreibt Gerald Flurry in seinem neuen Buch *Amerika unter Beschuss.* „Seien wir nicht naiv und glauben wir nicht, dass so etwas bei uns nie passieren könnte. Unsere Vorväter waren nicht dumm. Sie wollten die Freiheit der Amerikaner garantieren. Sie wussten, dass Gott ein Gott der Freiheit ist; Er will, dass wir frei sind. Das ist ein Geschenk Gottes, und das haben sie verstanden!“

Die Verbreitung dieser Technologie und ihre Nutzung durch die Regierung geschah größtenteils während der Amtszeit von Barack Obama. Seitdem sind wichtige Institutionen wie die CIA und das FBI unter der Kontrolle der radikalen Linken geblieben. Während Obamas Amtszeit schrieb Robert Morley in der *Posaune*: „Vielleicht *sind* viele oder sogar die meisten der Menschen, die von Agenten der [National Security Agency] und anderer Strafverfolgungsbehörden ins Visier genommen werden, tatsächlich eine Bedrohung für die USA. Das größere Problem ist jedoch, dass *diese Behörden unter einer Regierung, die das Gesetz verachtet, das sie geschworen hat, zu wahren, rasch expandieren* (Mai-Juni 2014).“

Die Bibel beschreibt diese Zeit als einen „bitteren Jammer“, eine Bedrängnis für die modernen Nationen Israels: Großbritannien und Amerika. Sie waren „bis auf den letzten Mann dahin und [es war] kein Helfer in Israel.“ (2. Könige 14, 26).

Wenn die Regierung in Ihrem Haus und in Ihrer Tasche sitzt, ist es schwierig, eine freie Gesellschaft aufrechtzuhalten. Und die Gefahren des Missbrauchs durch Regierungen im In- und Ausland sind enorm.

Die radikale Linke arbeitet daran, Amerika von einer konstitutionellen Republik zu verändern, und sie nutzt die Macht, die eine solche Überwachung bietet, als Waffe. Wie das Buch *Amerika unter Beschuss* zeigt, warnt die Bibel, dass Gott Selbst Amerika vor dieser Art von Tyrannei retten muss.

Aber die Bibel warnt auch davor, dass Amerika, wenn wir uns nicht ändern, wieder in die Tyrannei zurückfallen wird – diesmal vom Ausland aufgezwungen. Ohne Amerikas Engagement für die Freiheit erheben sich andere Länder. Ihnen wird prophezeit, dass sie ihre Herrschaft mit Gewalt durchsetzen werden und sich diese Art von Technologie leicht zunutze machen könnten.

Doch wie Herr Flurry schrieb, ist Gott ein Gott der Freiheit. All dies ist Teil Seines Plans, der Welt Freiheit zu bringen – Freiheit von Tyrannei und Freiheit von den schmerzhaften Abhängigkeiten und Sünden, die diese Welt in ihren Bann halten.