
POLICE
PROTECT & SERVE
054

Die Proteste gegen rassistische Polizeiarbeit haben zu neuen Untersuchungen bei großen Technologieunternehmen wie Facebook, das von Werbekunden wegen Hassreden gegen PoC boykottiert wird, und Amazon, die zur Unterstützung der Polizeiüberwachung aufgerufen hat, geführt. Aber Microsoft, das weitgehend der Kritik entgangen ist, steckt knietief in Diensten für die Strafverfolgung und fördert ein Ökosystem von Unternehmen, die der Polizei Software über Microsofts Cloud und andere Plattformen zur Verfügung stellen. Die ganze Geschichte dieser Verbindungen zeigt, wie der Technologiesektor immer mehr in intime, andauernde Beziehungen zu den Polizeidienststellen verstrickt ist.

Microsofts Verbindungen zu den Strafverfolgungsbehörden wurden von der Firma verschleiert, deren öffentliche Reaktion auf den Skandal nach dem Mord an George Floyd sich auf Gesichtserkennungssoftware konzentriert hat. Dies lenkt die Aufmerksamkeit von Microsofts eigener Massenüberwachungsplattform für Polizist:innen ab, dem Domain Awareness System, das für die New Yorker Polizei gebaut und später auf Atlanta, Brasilien und Singapur ausgeweitet wurde.
Es verschleiert auch, dass Microsoft sich mit einer Vielzahl von Anbietern von Polizeiüberwachungsgeräten zusammengeschlossen hat, die ihre Produkte auf einer „Government Cloud“ betreiben, die von der Azure-Abteilung des Unternehmens geliefert wird, und dass Microsoft Plattformen zur Vernetzung von Polizeieinsätzen, einschließlich Drohnen, Robotern und anderen Geräten, vorantreibt.

Mit Partnerschaft, Unterstützung und kritischer Infrastruktur, die von Microsoft zur Verfügung gestellt wird, bietet eine Schattenindustrie aus kleineren Unternehmen den Strafverfolgungsbehörden eine Massenüberwachung. Genetec bietet Cloud-basierte Überwachungskamerasysteme und große Datenanalysen für die Massenüberwachung in großen US-Städten an. Veritone bietet den Strafverfolgungsbehörden Gesichtserkennungsdienste an. Und eine breite Palette von Partnern liefert Hightech-Polizeiausrüstung für die Microsoft Advanced Patrol Platform, die Polizeiautos in alles überwachende Überwachungspatrouillen verwandelt. All dies wird zusammen mit Microsoft durchgeführt und auf der Azure Government Cloud gehostet.

Letzten Monat haben hunderte von Microsoft-Angestellten ihren CEO, Satya Nadella, gebeten, Verträge mit den Strafverfolgungsbehörden zu kündigen, Black Lives Matter zu unterstützen und die Finanzmittelkürzung der Polizei zu befürworten. Als Reaktion darauf ignorierte Microsoft die Beschwerde und verbot stattdessen den Verkauf seiner eigenen Gesichtserkennungssoftware an die Polizei in den Vereinigten Staaten und lenkte den Fokus von Microsofts anderen Beiträgen zur Polizeiüberwachung ab. Die Strategie funktionierte: Sowohl die Presse als auch die Aktivist:innen lobten den Schritt, was Microsofts besagte Position als moralischer Führer im Bereich der Technologie stärkte.

Dennoch ist es nicht klar, wie lange Microsoft einer größeren Überprüfung entgehen wird. Die Polizeiarbeit wird zunehmend mit aktiver Mitarbeit von Technologieunternehmen durchgeführt, und Microsoft ist zusammen mit Amazon und anderen Cloud-Anbietern einer der Hauptakteure in diesem Bereich.

Da Partnerschaften und Dienste, die Drittanbieter in der Azure-Cloud beherbergen, nicht öffentlich bekannt gegeben werden müssen, ist es unmöglich, das volle Ausmaß von Microsofts Beteiligung im Bereich der Polizeiarbeit oder den Status der öffentlich angekündigten Dienste Dritter zu kennen, möglicherweise einschließlich einiger der unten genannten, bereits angekündigten Beziehungen.

Microsoft: Vom polizeilichen Geheimdienst zur Azure Cloud

Nach dem 11. September 2001 leistete Microsoft wichtige Beiträge zu zentralisierten Geheimdienstzentren für die Strafverfolgungsbehörden. Um 2009 herum begann das Unternehmen mit der Arbeit an einer Überwachungsplattform für das NYPD, dem so genannten Domain Awareness System (DAS), das 2012 der Öffentlichkeit vorgestellt wurde. Das System wurde unter der Leitung von Microsoft zusammen mit NYPD-Beamt:innen aufgebaut.

Das DAS integriert unterschiedliche Informationsquellen, um drei Kernfunktionen zu erfüllen: Echtzeit-Alarmierung, Ermittlungen und polizeiliche Analysen.

Durch das DAS beobachtet das NYPD die persönlichen Bewegungen der gesamten Stadt. In seiner Anfangszeit nahm das System Informationen von Überwachungskameras, Umweltsensoren (um Strahlung und gefährliche Chemikalien aufzuspüren) und automatischen Nummernschild-Lesegeräten (ALPR) auf. Bis 2010 begann es damit, geokodierte NYPD-Aufzeichnungen von Beschwerden, Verhaftungen, 911-Anrufen und Haftbefehlen hinzuzufügen, „um den Sensordaten einen Kontext zu geben“. Danach kamen Videoanalyse, automatische Mustererkennung, vorausschauende Polizeiarbeit und eine mobile Anwendung für Polizist:innen hinzu.

Bis 2016 hatte das System zwei Milliarden Nummernschildbilder von ALPR-Kameras aufgenommen (drei Millionen Lesevorgänge pro Tag, fünf Jahre lang archiviert), 15 Millionen Beschwerden, mehr als 33 Milliarden öffentliche Aufzeichnungen, über 9000 NYPD- und privat betriebene Kamerafeeds,

Videos von über 20.000 Körperkameras und mehr. Um dem Ganzen einen Sinn zu geben, suchen die Analysealgorithmen relevante Daten heraus, auch für die vorausschauende Polizeiarbeit.

Während das DAS einige Aufmerksamkeit von der Presse erhalten hat – und unter Aktivist:innen ziemlich bekannt ist – gibt es mehr über die Geschichte der Microsoft-Polizeidienste.

Im Laufe der Jahre hat Microsoft sein Geschäft durch die Ausweitung seiner Cloud-Dienste ausgebaut. Eines seiner Angebote, Azure Government, bietet dediziertes Daten-Hosting in ausschließlich inländischen Cloud-Centern, so dass die Daten das Host-Land nie physisch verlassen. In den USA hat Microsoft mehrere Azure Government Cloud Center für die Nutzung durch lokale, staatliche und bundesstaatliche Organisationen aufgebaut.

Den meisten Leuten ist nicht bekannt, dass Microsoft eine Abteilung für „Öffentliche Sicherheit und Justiz“ mit Mitarbeiter:innen hat, die früher in der Strafverfolgung gearbeitet haben. Dies ist das wahre Herzstück der Polizeidienste der Firma, auch wenn sie seit Jahren fernab der öffentlichen Meinung operiert.

Microsofts polizeiliche Überwachungsdienste sind oft undurchsichtig, da die Firma wenig eigene Produkte für die Polizei verkauft. Stattdessen bietet es eine Reihe allgemeiner Azure-Cloud-Dienste an, wie zum Beispiel maschinelles Lernen und prädiktive Analysewerkzeuge wie Power BI (Business Intelligence) und kognitive Dienste, die von Strafverfolgungsbehörden und Überwachungsanbietern genutzt werden können, um ihre eigene Software oder Lösungen zu entwickeln.

Microsofts überwachungsbasierter IoT-Patrouillenwagen

Ein reichhaltiges Angebot von Microsofts Cloud-basierten Angeboten wird mit einem Konzept namens „The Connected Officer“ präsentiert. Microsoft situiert dieses Konzept als Teil des Internet der Dinge, oder IoT (Internet of Things), in dem Gadgets mit Online-Servern verbunden und dadurch nützlicher gemacht werden. Der „Connected Officer“, so hat es Microsoft geschrieben, wird „das IoT zur Überwachung bringen“.

Mit dem Internet der Dinge werden physische Objekte mit eindeutigen Kennungen versehen und übertragen Daten automatisiert über Netzwerke. Zieht ein:e Polizeibeamt:in zum Beispiel eine Waffe aus dem Holster, kann eine Benachrichtigung über das Netzwerk verschickt werden, um andere Polizeibeamt:innen zu warnen, wenn Gefahr droht. Echtzeit-Verbrechenszentren könnten die Beamt:innen dann auf einer Karte lokalisieren und die Situation von einem Kommando- und Kontrollzentrum aus überwachen.

Nach diesem Konzept wird eine Vielzahl von Überwachungs- und IoT-Sensordaten auf einen „heißen Pfad“ für den schnellen Einsatz in Kommandozentralen und auf einen „kalten Pfad“ geschickt, um später von Geheimdienstanalytiker:innen auf der Suche nach Mustern verwendet zu werden. Die Daten werden durch Microsofts Azure Stream Analytics gestreamt, auf der Azure-Cloud gespeichert und durch Microsoft Analyselösungen wie Power BI erweitert – und bieten eine Reihe von Punkten, an denen Microsoft Geld verdienen kann.

Während der „Connected Officer“ eine konzeptionelle Übung war, ist die echte Patrouillenlösung des Unternehmens die Microsoft Advanced Patrol Platform, oder MAPP. MAPP ist eine IoT-Plattform für Polizeistreifenfahrzeuge, die Überwachungssensoren und Datenbankeinträge auf der Azure-Cloud integriert, einschließlich „Dispatch-Informationen, Fahranweisungen, Verdächtigengeschichte, einem sprachaktivierten Nummernschildleser, einer Vermisstenliste,

standortbezogenen Verbrechensbulletins, Schichtberichten und mehr“.

Das MAPP-Fahrzeug ist mit Ausrüstung von Drittanbietern ausgestattet, die für die Strafverfolgungsbehörden Überwachungsdaten in die Azure-Cloud streamen. Auf dem Dach montiert, überträgt eine hochauflösende 360-Grad-Kamera Live-Videos an Azure und den Laptop im Inneren des Fahrzeugs, wobei der Zugriff auch über ein Mobiltelefon oder einen entfernten Computer möglich ist. Das Fahrzeug ist außerdem mit einem automatischen Nummernschild-Lesegerät ausgestattet, das 5000 Nummernschilder pro Minute lesen kann – egal ob das Auto steht oder unterwegs ist – und diese mit einer Datenbank in Azure abgleichen kann, die von Genetecs Nummernschild-Lesegerät AutoVu betrieben wird.

Eine Drohne, die vom Microsoft-Partner Aeryon Labs, dem SkyRanger, zur Verfügung gestellt wird, patrouilliert den Himmel und liefert Echtzeit-Streaming-Videos. (Aeryon Labs ist jetzt Teil des Überwachungsgiganten FLIR Systems.) Die Drohnen können der integrierten Datenplattform Luftbilder zur Verfügung stellen, die es den Beamt:innen erlauben, laufende Situationen in Echtzeit zu beurteilen oder forensische Beweise von einem Tatort zu sammeln.

Auch Polizeiroboter sind Teil der MAPP-Plattform. Produkte von ReconRobotics, zum Beispiel „integriert[e] mit Microsofts Programm ‚Streifenwagen der Zukunft'“ im Jahr 2016. Microsoft sagt, dass ReconRobotics sein MAPP-Fahrzeug mit einem „kleinen, leichten, aber leistungsstarken Roboter“ ausstattet, der „von Streifenpolizist:innen einfach eingesetzt und ferngesteuert werden kann, um Entscheidungsträgern Informationen in Echtzeit zu liefern“.

Ein weiterer Partner von Microsoft, SuperDroid Robots, hat ebenfalls angekündigt, das Microsoft MAPP-Fahrzeug mit zwei kompakten ferngesteuerten Überwachungsrobotern auszustatten, dem MLT „Jack Russell“ und dem LT2-F „Bloodhound“, wobei letzterer Treppen und Hindernisse überwinden kann.

Obwohl es ein Microsoft-Abzeichen auf der Motorhaube und an der Tür trägt, steht das physische Fahrzeug, das die Firma zur Werbung für MAPP verwendet, nicht zum Verkauf durch Microsoft, und man wird wahrscheinlich keine Autos mit dem Microsoft-Label herumfahren sehen. Vielmehr stellt Microsoft MAPP als Plattform zur Verfügung, über die bestehende Polizeiautos in IoT-Überwachungsfahrzeuge umgewandelt werden können: „Es geht wirklich darum, all diese Daten in die Cloud stellen zu können, diese Daten mit ihren Daten belegen zu können und anfangen zu können, relevante Informationen daraus zu machen“, so Microsoft.

Das Auto soll zum Nervenzentrum der Strafverfolgung werden. Die Informationen, die in der Azure-Cloud gesammelt und gespeichert werden, sollen den Beamt:innen helfen, „schlechte Akteur:innen zu identifizieren“ und „die Beamt:innen auf die Umgebung aufmerksam zu machen, die um sie herum vorgeht“. In Zukunft sollen mit maschinellem Lernen und KI mit dem Mustervergleich begonnen werden können, wobei MAPP-Fahrzeuge Daten liefern, die dabei helfen, „schlechte Akteur:innen“ zu finden.

Letzten Oktober kündigte die südafrikanische Polizei an, dass Microsoft eine Partnerschaft mit der Stadt Durban für die smarte Überwachung im 21. Jahrhundert eingegangen ist. Durbans Version der MAPP-Lösung beinhaltet ein 360-Grad-ALPR zum Scannen von Nummernschildern und eine Gesichtserkennungskamera der chinesischen Videoüberwachungsfirma Hikvision für den Einsatz bei stehendem Fahrzeug (z.B. geparkt bei einer Veranstaltung).

Laut dem südafrikanischen Nachrichtensender ITWeb wird die U-Bahn-Polizei die MAPP-Lösung „zur Abschreckung krimineller Aktivitäten auf der Grundlage der Datenanalyse durch vorausschauende Modellierung und Algorithmen des maschinellen Lernens“ einsetzen. Das

Fahrzeug wurde bereits in Kapstadt ausgerollt, wo Microsoft kürzlich ein neues Azure-Rechenzentrum eröffnet hat – eine Erweiterung des digitalen Kolonialismus.

Ähnlich wie die USA, sieht sich Südafrika der Geißel der Polizeibrutalität gegenüber, die People of Color unverhältnismäßig stark trifft. Das Land hatte seinen eigenen George Floyd-Moment während des kürzlichen Covid-19-Lockdowns, als das Militär und die Polizei den 40-jährigen Collins Khosa in der armen Alexandra-Stadtgemeinde brutal zusammenschlugen, was zu seinem Tod führte – wegen einem Becher Bier.

Die MAPP-Lösung wird für eine „Null-Toleranz"-Polizeiarbeit verwendet werden. Zum Beispiel sagte der Metro-Polizeisprecher von Durban, Parboo Sewpersad, dass die Einführung darauf abzielt, „Vermüllung, Trinken beim Fahren, sowie Trinken beim Gehen" während der Sommerfeierlichkeiten zu bestrafen.

Es ist schwer zu bestimmen, wo das MAPP-Fahrzeug sonst noch eingesetzt werden darf. Der Rollout in Südafrika lässt vermuten, dass Microsoft Afrika als einen Ort sieht, an dem man mit seinen polizeilichen Überwachungstechnologien experimentieren kann.

Microsoft: Versorgung von Überwachungskameras und Polizeispionage in der Stadt

Neben der Vernetzung von Polizeifahrzeugen bietet die Videoüberwachung eine weitere lukrative Einnahmequelle für Microsoft, da sie mit Datenpaketen beladen wird, die zu übertragen, zu speichern und zu verarbeiten sind – und mit jedem Schritt Gebühren einbringt.

Beim Aufbau eines Überwachungsnetzwerks voller Kameras verwenden Städte und Unternehmen in der Regel ein Videoverwaltungssystem (Video Management System, VMS), um Dinge wie die Anzeige mehrerer Kamera-Feeds auf einer Videowand oder die Möglichkeit, das Filmmaterial zu durchsuchen, zu tun. Ein führender VMS-Anbieter, Genetec, bietet das Kern-VMS integriert in Microsofts Domain Awareness System an. Seit über 20 Jahren ein enger Partner von Microsoft, arbeiten die beiden Unternehmen zusammen an der Integration von Überwachungsdiensten auf der Azure-Cloud.

Einige der bekanntesten städtischen Polizeikräfte benutzen Genetec und Microsoft für die Videoüberwachung und -analyse.

Durch eine öffentlich-private Partnerschaft namens „Operation Shield" ist Atlantas Kameranetzwerk von 17 Kameras in der Innenstadt auf ein weites Netz von 10.600 Kameras angewachsen, von denen die Beamt:innen hoffen, dass sie bald alle Stadtquadranten abdecken werden.

In Chicago decken 35.000 Kameras die Stadt mit einem Plug-in-Überwachungsnetzwerk ab. Das Back-End nutzt derzeit Genetec Stratocast und Genetecs Federation Service, der den Zugang zu den Kameras über ein föderales Netzwerk von Überwachungs-Kameras verwaltet – ein Netzwerk von Kameranetzwerken sozusagen.

Im Jahr 2017 hat Genetec ihre Citigraf-Plattform speziell für das Chicago Police Department – die zweitgrößte Polizei des Landes – gebaut, um die riesigen Datenmengen des Departments zu verstehen. Citigraf wird von Microsoft Azure betrieben und nimmt Informationen von Überwachungssensoren und Datenbankeinträgen auf. Mit Hilfe von Echtzeit- und historischen Daten führt es Berechnungen, Visualisierungen, Alarme und andere Aufgaben durch, um ein „tiefes Situationsbewusstsein" für das CPD zu schaffen. Microsoft arbeitet mit Genetec zusammen, um eine

„Korrelationsmaschine“ aufzubauen, die den Sinn der Überwachungsdaten erkennen lässt.

Die Stadt Detroit benutzt Genetec Stratocast und Microsoft Azure, um ihr umstrittenes Project Green Light anzutreiben. Das Projekt, das 2016 zusammen mit einem neuen Echtzeit-Verbrechenszentrum gestartet wurde, ermöglicht es lokalen Unternehmen – oder anderen teilnehmenden Einrichtungen, wie Kirchen und öffentlichen Gebäuden – Videokameras auf ihrem Gelände zu installieren und die Überwachungsdaten an die Polizei von Detroit zu übertragen. Die Teilnehmenden können ein „grünes Licht“ neben den Kameras platzieren, um die Öffentlichkeit – die zu 80 Prozent aus Schwarzen besteht – zu warnen, dass „ihr von der Polizei beobachtet werdet“.

2015, so das Detroit Police Department, „wird der Tag kommen, an dem die Polizei überall Zugang zu Kameras haben wird, die es der Polizei erlauben, praktisch in jedem Bereich der Stadt zu patrouillieren, ohne auch nur einen Fuß zu setzen“.

Die Ausweitung der polizeilichen Überwachung in Detroit ging schnell voran. Heute hat das Projekt Green Light etwa 2800 Kameras an über 700 Orten installiert, und zwei kleinere Echtzeit-Verbrechenszentren kommen hinzu, eine Entwicklung, die in Städten wie Chicago im Trend liegt.

Nach der Ermordung von George Floyd haben Aktivist:innen in Detroit ihre Bemühungen wieder aufgeladen, das Projekt Green Light im Kampf gegen die Polizeiüberwachung abzuschaffen, das von lokalen Befürworter:innen der Gemeinde als rassistisch eingestuft wird. In diesem Jahr wurden zwei Schwarze, Robert Julian-Borchak Williams und Michael Oliver, zu Unrecht verhaftet, nachdem sie durch die Gesichtserkennungstechnologie des DPD falsch identifiziert wurden.

Nakia Wallace, eine Mitorganisatorin von Detroit Will Breathe, erzählte, dass Project Green Light Menschen „vorkriminalisiert“ und „der Polizei das Recht gibt, dich im Auge zu behalten, wenn sie denken, dass du schuldig bist“ und „Schwarze und Braune Gemeinschaften belästigt“. Das „Zusammenschalten von Kameras“ über weite Gebiete hinweg ist „Hyper-Überwachung“ und „muss gestoppt werden“, fügte sie hinzu.

Die „Funktion, der das [DPD] dient“, sagte Wallace, ist „der Schutz von Eigentum und die Vorherrschaft der Weißen“. „Sie sind hypermilitarisiert, und selbst im Zuge dessen sterben immer noch Menschen in der Stadt“, weil „sie kein Interesse an der Lebensgrundlage der Bürger:innen von Detroit haben“. Anstatt zu militarisieren, müssen wir „aufhören, so zu tun, als ob die armen Schwarzen von Natur aus kriminell wären, und anfangen, nach sozialen Diensten und Dingen zu suchen, die die Menschen davon abhalten, in ein kriminelles Leben zu gehen“.

In einem Blogbeitrag aus dem Jahr 2017 prahlte Microsoft mit der Partnerschaft mit Genetec für den DPD und erklärte, dass das Projekt Green Light „ein großartiges Beispiel dafür ist, wie Städte mit den heutigen Technologien die öffentliche Sicherheit, die Lebensqualität der Bürger:innen und das Wirtschaftswachstum verbessern können“.

Microsoft und die Gesichtserkennungstechnologie

Während Microsoft die Geheimdienstzentren und Überwachungsnetzwerke im Verborgenen betreibt, hat sich die Firma öffentlich auf Gesichtserkennungsvorschriften konzentriert. Am 11. Juni schloss sich Microsoft Amazon und IBM an und sagte, dass es seine Gesichtserkennungstechnologie nicht an die Polizei verkaufen wird, solange es keine Regelungen gibt.

Dies ist ein PR-Gag, der in mehrfacher Hinsicht verwirrt, wie Microsofts Beziehung zur Polizei

technisch und ethisch funktioniert.

Erstens, während die Presse gelegentlich Microsofts Domain Awareness System kritisiert, konzentriert sich die meiste Aufmerksamkeit für die Microsoft-Polizeiarbeit auf die Gesichtserkennung. Dies ist ein Irrtum: Microsoft stellt Software zur Verfügung, um eine Vielzahl von Polizeitechnologien zu betreiben, die Zivilrechte und Freiheiten untergraben – auch ohne Gesichtserkennung.

Zweitens ist die Gesichtserkennung ein bemerkenswertes Merkmal vieler Videoüberwachungssysteme und Echtzeit-Verbrechenszentren, die Microsoft betreibt. Die Städte New York, Atlanta, Chicago und Detroit gehören zu den Städten, die die Dienste von Microsoft nutzen, um die für die Gesichtserkennung verwendeten visuellen Überwachungsdaten zu sammeln, zu speichern und zu verarbeiten. Microsoft-Dienste sind ein fester Bestandteil vieler polizeilicher Überwachungssysteme zur Gesichtserkennung.

Drittens wurde mindestens eine Gesichtserkennungsfirma, Veritone, aus dem Gespräch ausgeschlossen. Das südkalifornische Unternehmen für künstliche Intelligenz, ein Partner von Microsoft, bietet eine Cloud-basierte Software namens IDentify an, die auf Microsofts Cloud läuft und den Strafverfolgungsbehörden hilft, die Gesichter potenzieller Verdächtiger zu markieren.

In einem Webinar hat Veritone kürzlich erklärt, wie IDentify die Daten nutzt, über die die Polizei bereits verfügt, wie zum Beispiel Verhaftungsunterlagen. Wenn eine Person entdeckt wird und es keine bekannte Übereinstimmung gibt, kann die IDentify-Software ein Profil von Verdächtigen erstellen, indem sie eine „Person von Interesse-Datenbank“ erstellt, die „es dir ermöglicht, unbekannte Gesichter einfach in dieser Datenbank zu speichern und diese Gesichter im Laufe der Zeit kontinuierlich zu überwachen“.

Veritone behauptet, Dienste an „etwa 150 Orten“ anzubieten, nennt aber nicht, welche davon IDentify benutzen. Veritone hat 2019 einen Pilotversuch mit der Polizei von Anaheim gestartet.

Microsoft listet Veritone IDentify als ein Produkt zur Gesichtserkennung für Strafverfolgungsbehörden in seinem App-Repository online auf. Das Werbevideo auf der Microsoft-Website wirbt für die Fähigkeit von IDentify:

„… deine Datenbanken mit bekannten Täter:innen und Personen von Interesse mit Videobeweisen zu vergleichen, um schnell und automatisch Verdächtige für Ermittlungen zu identifizieren. Einfach Beweise von Überwachungssystemen, Körperkameras und mehr hochzuladen. … Aber das Beste ist, du bist nicht an deinen Schreibtisch gekettet! Mach ein Foto und identifiziere Verdächtige, während du auf Streife bist, um Aussagen zu überprüfen und laufende Ermittlungen zu sichern.“

Microsoft und die Irreführung

Trotz gegenteiliger Behauptungen bietet Microsoft durch Partnerschaften und Dienstleistungen für Firmen wie Veritone und Genetec und durch sein Domain Awareness System Gesichtserkennungsdienste für die Strafverfolgung an.

Microsofts Strategie der Öffentlichkeitsarbeit zielt darauf ab, die Öffentlichkeit in die Irre zu führen, indem die Aufmerksamkeit von seinen weitreichenden Dienstleistungen für die Polizei abgelenkt wird. Stattdessen drängt Microsoft-Präsident und Leiter der Rechtsabteilung Brad Smith die Öffentlichkeit dazu, sich auf die Regulierung der Gesichtserkennung und die Frage von Microsofts

eigener Gesichtserkennungssoftware zu konzentrieren, als ob ihre anderen Software- und Serviceangebote, Partnerschaften, Konzepte und Marketing nicht integraler Bestandteil eines ganzen Ökosystems von Gesichtserkennungs- und Massenüberwachungssystemen sind, die von kleineren Firmen angeboten werden.

Microsoft und seine Befürworter:innen könnten behaupten, dass es sich bei Azure um einen „neutralen“ Cloud-Anbieter handelt und es liegt an anderen Firmen und Polizeidienststellen zu entscheiden, wie sie Microsoft-Software nutzen. Dennoch arbeiten diese Firmen mit Microsoft zusammen und Microsoft wird dafür bezahlt, ihre Massenüberwachungs- und Gesichtserkennungsdienste auf der Azure-Cloud laufen zu lassen – Dienste, die People of Color unverhältnismäßig stark betreffen.

Wenn diese Microsoft-Clients Dienste für den Sexhandel in der Azure-Cloud anbieten würden, würde Microsoft sicherlich ihre Konten schließen. Und weil die Strafverfolgungsbehörden Überwachungstechnologien mit Steuergeldern kaufen, bezahlt die Öffentlichkeit Microsoft tatsächlich für ihre eigene Polizeiüberwachung.

Quelle: The Intercept