2017/38 Lifestyle

https://jungle.world/artikel/2017/38/your-face

Biometrische Verfahren nehmen Einzug in den Alltag

In your face

Von **Enno Park**

Beim neuen iPhone soll die Gesichtserkennung das Passwort ersetzen. Welche Möglichkeiten und Risiken diese Technologie birgt, zeigen ganz andere Beispiele.

Knöpfe sind unsexy. Für ein möglichst futuristisches Design arbeitet das kalifornische Technologieunternehmen Apple schon lange daran, die Anzahl der Knöpfe an seinen Geräten möglichst weit zu reduzieren. Bisher blieb beim iPhone neben den Lautstärketasten und dem Ausschalter noch der »Homebutton« übrig, der unten in der Mitte sitzt. Da muss draufdrücken, wer das Telefon in die Hand nimmt und etwas damit machen will. Diesen Knopf aus Gründen der Eleganz wegzurationalisieren, damit das ganze Telefon ein einziges großes Display ist, stellte Apple vor ein Problem: In den Homebutton ist bei bisherigen Modellen der Fingerabdrucksensor integriert, mit dem ein Nutzer das Telefon entsperren kann.

Ein Ersatz für Fingerabdrücke musste her und das Unternehmen entschied sich für Gesichtserkennung. Das ist schon auf den ersten Blick eine unheimlich schlechte Idee. Gesichtserkennung zum Entsperren von Smartphones gibt es bei Android-Geräten schon seit Jahren und alle Experten raten unisono davon ab, diese Funktion zu verwenden, weil sie notorisch unsicher ist. Bei einfachen Systemen reicht es oft schon aus, ein Foto vor die Kamera zu halten, um es zu überlisten. Allerdings hat sich Apple einiges ausgedacht, um die Gesichtserkennung sicherer zu machen: Das neue Smartphone benutzt eine Infrarotkamera und mehrere Sensoren, um einen kompletten 3D-Scan des Gesichts zu erstellen. Übrigens auch keine ganz neue Technik: Das Grundprinzip ähnelt dem von Microsoft, das auf ähnlichem Wege die Personen in einem Raum scannt, um Computerspiele mit echten Bewegungen zu steuern.

Wie sicher ist Face ID?

Natürlich ist die 3D-Gesichtserkennung eine Herausforderung für Hacker. Die hatten bereits bei der Einführung des Fingerabdrucksensors nur Tage gebraucht, um diesen zu umgehen. Denn Kopien von Fingerabdrücken lassen sich mit Tesafilm und etwas Leim im Handumdrehen erstellen. Die neue Gesichtserkennung zu überlisten, sollte da schon schwieriger sein. Wer sich vor dem Telefon als dessen Besitzer ausgeben möchte, muss eine naturgetreue dreidimensionale Nachbildung von dessen Kopf davor halten. Solche Angriffsversuche soll das Smartphone erkennen und den Zugang verweigern. Wie sicher das in der Praxis sein wird, muss sich noch zeigen. Genauso wie ein normales Schloss für die Haustür in der Regel ausreicht, aber Profis nicht abhalten wird, sind Fingerabdruck-Scan oder 3D-Gesichtserkennung für den Alltag

ausreichend. Sehr vorsichtige Zeitgenossen oder solche, denen wirklich Gangster oder Ermittlungsbehörden auf den Fersen sind, bleiben aber besser beim Passwort.

> Während man sich in den USA weigern kann, ein Passwort zu verraten, kommt man nicht darum herum, Fingerabdrücke abzugeben oder sich fotografieren zu lassen.

Was das Marketing betrifft, könnte die neue Technologie ein Problem haben, jedenfalls aus deutscher Perspektive. Hierzulande wird gerade über Verhaltens- und Gesichtserkennung per Videoüberwachung gestritten wie etwa beim Pilotversuch am Berliner S-Bahnhof Südkreuz. Dass das überhaupt nichts mit der Gesichtserkennung auf dem neuen iPhone zu tun hat, hindert einige Kolumnisten nicht daran, beides munter durcheinanderzuwerfen. Apple beteuert, die Daten würden nirgends hochgeladen und auf dem Telefon verbleiben. Nach eigenen Angaben hat auch Apple selbst keinen Zugriff auf die biometrischen Daten. Bereits in der Vergangenheit weigerte sich der Smartphone-Hersteller, beim Entsperren von Telefonen mit dem FBI oder anderen Ermittlungsbehörden zu kooperieren. Anders als Google, das wenig am Verkauf von Android-Telefonen verdient und sein Geld mit den Daten macht, die die Kunden bei der Nutzung ihres Telefons über sich preisgeben, verkauft Apple in erster Linie Lifestyle-Gadgets. Und die - gehören trotz einiger berechtigter Kritik im Hinblick auf den Datenschutz derzeit zu den Besseren auf dem Markt.

Dennoch wird auch die Apple-Version der Gesichtserkennung von Experten kritisiert – aus einer ganzen Reihe von Gründen. So gelten biometrische Verfahren grundsätzlich als nicht besonders gut geeignet, um ein Passwort zu ersetzen. Denn ein Passwort lässt sich geheim halten, während wir unsere Gesichter ständig mit uns herumtragen und der Öffentlichkeit zeigen. Ähnliches gilt für Fingerabdrücke oder genetische Profile. In vielen Ländern ist das auch ein handfester juristischer Unterschied: Während man sich zum Beispiel in den USA weigern kann, ein Passwort zu verraten, kommt man nicht darum herum, Fingerabdrücke abzugeben oder sich fotografieren zu lassen.

Während Apple die Daten wahrscheinlich wirklich nur auf dem Telefon selbst speichert, ist das bei anderen Systemen nicht gesagt. Mittlerweile geht Gesichtserkennung auch über das reine Identifizieren von Personen hinaus. Künstliche Intelligenzen (KI) können mit mehr oder weniger hoher Treffergenauigkeit Krankheiten oder die sexuelle Orientierung aus den Fotos herauslesen. Zwar sind viele solcher Experimente statistisch und methodisch eher fragwürdig, könnten aber versehen mit dem Label »Künstliche Intelligenz« zu einer Renaissance des Schädelvermessens führen wie vor 200 Jahren, als Wissenschaftler glaubten, aus den Ausformungen des Kopfes allerlei Charaktermerkmale herauslesen zu können.

Zudem bleibt unklar, in welchem Ausmaß andere Apps, die auf dem Telefon installiert sind, auf die Gesichtsdaten zugreifen können. So hat Apple im wohl absurdesten Moment der Firmengeschichte ein animiertes Emoji in Form einer Fäkalie präsentiert, die sich entsprechend der Mimik seines Besitzers bewegt. Und Zugriff auf die Gesichtsdaten haben offenbar nicht nur Apples »Animojis«, sondern auch Apps von Drittanbietern wie Snapchat, etwa um virtuelle Masken in Gesichter einzublenden.

Bezahlen per Blick

Neben solchen Datenschutzerwägungen sprechen noch andere Gründe gegen jede noch so ausgefuchste Gesichtserkennung. Während ein gutes Passwort kaum zu knacken ist und man einen Fingerabdruck erstmal fälschen oder Gewalt anwenden muss, damit jemand gegen seinen Willen seinen Finger auf den Sensor legt, reicht es in Zukunft, dass ein Dieb seinem Opfer noch schnell das Telefon vors Gesicht hält, bevor er sich damit aus dem Staub macht. Besonders problematisch wird es aber, wenn Ermittlungsbehörden sich für den Inhalt eines Telefons interessieren. Immerhin gibt es hierfür die Möglichkeit, durch fünfmaliges Drücken des Ausschaltknopfes die Gesichtserkennung (wie übrigens auch den Fingerabdrucksensor bei älteren Geräten) zu deaktivieren. Jedenfalls wenn man schnell genug ist.

Ein Sicherheitsproblem gibt es auch beim Bezahldienst Apple Pay. Statt per Passwort, soll der Bezahlvorgang künftig ebenfalls mit einem Blick ins Smartphone autorisiert werden. Man braucht nicht besonders viel Phantasie, um sich auszumalen, welche Gaunereien so möglich werden.