Philip E. Agre

Az arcunk nem vonalkód: érvek a nyilvános helyeken elhelyezett automatikus arcfelismerő berendezések használata ellen

Ha rendelkezésünkre áll egy személy digitalizált arcképe, az arcfelismerési szoftver összehasonlítja azt egy adatbázissal, amelyben más arcképek vannak. Ha a tárolt képek bármelyike elég szorosan egyezik vele, akkor a találatról a rendszer jelentést tesz a tulajdonosának. Az automatikus arcfelismeréssel kapcsolatos kutatások már évtizedek óta folynak, de az 1990-es években felgyorsultak, és az eredmények jelenleg lépnek a gyakorlati felhasználhatóság stádiumába: az arcfelismerő rendszereket világszerte kezdik nagy mértékben alkalmazni.

Az automatikus arcfelismerési rendszerek bizonyos alkalmazásai viszonylag nem kifogásolhatók. Sokféle létesítménynek jó oka van arra, hogy meggyőződjön mindenkinek a kilétéről, aki besétál az ajtaján, például a fegyverekhez, pénzhez, bűnügyi bizonyítékokhoz, nukleáris anyagokhoz vagy biológiailag veszélyes anyagokhoz való hozzáférés szabályozása érdekében. Amikor egy állampolgárt valamilyen alapos gyanúval letartóztatnak, a rendőrség részéről ésszerű eljárás az automatikus arcfelismerés alkalmazása az adott személyről készült pillanatfelvétel összehasonlítására olyan más személyekről készült és a rendőrségi nyilvántartásban tárolt képek adatbázisával, akiket korábban már letartóztattak. A technológia ilyen fajta használata igazolható a nyilvánosság előtt, ha kellő ellenőrzéssel biztosítják, hogy csakis a megfelelő célokra használják a technológiát.

A nyilvános helyeken elhelyezett arcfelismerő rendszerek azonban komoly aggodalomra adnak okot. Ez a téma igen nagy nyilvánosságot kapott a közelmúltban, amikor kiderült, hogy azoknak a szurkolóknak az arcképeit, akik részt vettek egy *Super Bowl*[*] bajnoki mérkőzésen, tudtuk nélkül összehasonlították a feltételezett bűnözők adatbázisával, továbbá Tampa városában arcfelismerő rendszert helyeztek üzembe az *Ybor City* nevű éjszakai szórakozónegyedben. Az arcfelismerés jelenlegi és javasolt alkalmazásai azonban – ahogyan a cikk végén felsorolt források részletesen megmutatják – ennél jóval szélesebb körre terjednek ki.

[*] A bajnoki döntőnek számító amerikai *Super Bowl* a világ legnézettebb egynapos sporteseménye. – *A ford*.

Most van itt az ideje annak, hogy mérlegeljük a nyilvános helyeken alkalmazott arcfelismerés elfogadhatóságát, még mielőtt teljesen bevett gyakorlattá válik és még komolyabban kezdi sérteni az emberek érdekeit.

A probléma korántsem korlátozódik azokra a szórványos esetekre, amelyekről eddig beszámolók jelentek meg. Ahogy a rendszer működését megalapozó információs és kommunikációs technikai eszközök (digitális kamerák, kép-adatbázisok, képfeldolgozó és adatátviteli rendszerek) teljesítménye a következő két évtized során drámaian növekedni, az áruk pedig radikálisan csökkenni fog, az arcfelismerés szintén drámai mértékben olcsóbb lesz, még akkor is, ha nem következik be nagyobb előrehaladás az olyan technológiák terén, mint például a képfeldolgozás, ami döntő fontosságú az arcok felismerésében. A gyakorlat jogi korlátozásai az Egyesült Államokban minimálisak. (Európában az adatvédelmi törvények erre is vonatkoznak, és biztosítják legalább a figyelmeztetés és a korrekció alapvető jogait.) Az azonosított arcképek adatbázisai máris nagy számban léteznek (például a vezetői engedélyek vagy az alkalmazottak számára készített személyazonossági kártyák esetében), és nem lesz nehéz új arckép-adatbázisokat létrehozni azoknak az embereknek a tudomásával és jóváhagyásával vagy akár anélkül, akiknek az arcképét rögzítették. (A képeknek ellenőrzött feltételek között kell készülniük, a legtöbb állampolgár azonban rendszeresen megfordul olyan kamerákkal figyelt és monitorokkal ellenőrzött helyeken, mint amilyenek például az üzletek és bizonyos irodák.) Szinte bizonyos tehát, hogy az automatikus arcfelismerés alkalmazása robbanásszerűen terjedni fog, és – hacsak nem lépünk akcióba most – hamarosan szinte mindenütt találkozni fogunk vele.

Meggyőződésem, hogy az automatikus arcfelismerés alkalmazását a nyilvános helyeken – köztük a nagyközönség számára nyitott, kereskedelmi funkciójú terekben, például a bevásárló központokban – törvényileg be kellene tiltani. A veszélyek nagyobbak, mint a hasznok. A szükséges törvényeket azonban a közvélemény szervezett fellépésének nagy erejű nyomása nélkül nem fogják meghozni. Ez a cikk érveket szolgáltat e cél érdekében az automatikus arcfelismerés nyilvános helyeken való bevezetése ellen, és válaszokat kínál a mellette szóló leggyakoribb érvekkel szemben.

Érvek az automatikus arcfelismerés nyilvános helyeken való alkalmazása ellen

–

– A visszaélések lehetőségei csillagászati méretűek. A mindenütt megjelenő arcfelismerés felhasználható az emberek nyomon követésére, bárhová is mennek. A különféle szervezetek által működtetett rendszerek könnyen hálózatba köthetők, hogy együttműködjenek az emberek különféle helyek között történő mozgásának nyomon követésében, akár ismerik az adott egyén személyazonosságát, akár nem, és minden azonosító jelet, amit ismernek, megoszthatnak egymással. Ezt a nyomkövetési információt sokféle célra fel lehet használni. A lehetőségek skálájának egyik végén az információ kiszivárogtatható például bűnözők számára, akik meg kívánják ismerni egy lehetséges áldozat utazási szokásait. Az információ rutinszerűen kiszivárog mindenféle adatbázisból, és nincs okunk azt feltételezni, hogy a nyomkövetési adatbázisok bármiben is különbözni fognak a többitől. A nyomkövetési információ – még ennél is alattomosabb módon – felhasználható a társadalom fölötti ellenőrzés gyakorlására is. Az emberek a jövőben kisebb valószínűséggel fognak részt venni olyan közösségi megmozdulásokban, amelyek bizonyos hatalmi érdekek ellen irányulnak, ha tudják, hogy személyazonosságukat meg fogják állapítani, és tudomására hozzák bárkinek, aki azt meg akarja ismerni.

–

– Az arcfelismerési rendszerekből származó információ könnyen kombinálható más technológiák útján megszerzett információkkal. A számos „biometrikus” azonosítási technológia közül az arcfelismeréshez van szükség a legkevesebb együttműködésre a megfigyelt egyén részéről. Az automatikus ujjlenyomat-leolvasáshoz – ezzel ellentétben – szükség van arra, hogy az ember valamelyik ujját rányomja egy gépre. (Alkalmasint lehetővé fog válni az emberek azonosítása DNS-t tartalmazó sejtjeikkel is, amelyeket jártukban-keltükben maguk után hagynak, ez a technológia azonban még messze van attól, hogy mindenütt elterjedhessen.) Azoknak a szervezeteknek, amelyeknek jó okuk van az emberek azonosítására, azt a technológiát kellene alkalmazniuk, amely a legkevesebb eleve benne rejlő lehetőséget nyújtja a visszaélésre, ám nagyon kevés azonosítási technológia nyújt több visszaélési lehetőséget, mint az arcfelismerés. Az arcfelismerési rendszerekből származó információk feldolgozása továbbá könnyen kombinálható az úgynevezett lokációs technológiákkal is (ilyen például a mobiltelefonoknál alkalmazott *E-911* jelű lokációs nyomkövetés), ami tovább növeli a visszaélések veszélyét.

–

– A technológia aligha tévedhetetlen. A potenciális árnyoldalak közé tartoznak a téves azonosítások, például amikor valakit „láttak” egy olyan utcában, amelyet gyakran látogatnak

kábítószer-árusok. Egy ilyen jelentés olyan „tényeket” produkál, amelyeket az egyénnek tisztáznia kell. Ám a képek felvételének és azonosításának feltételei a legtöbb nyilvános helyen távolról sem ideálisak. Az árnyékok, a takarások, a visszaverődések és a többszörös, ellenőrizhetetlen fényforrások mind-mind növelik a téves azonosítás kockázatát. Mivel az arcképek adatbázisai egyre nagyobbra nőnek, az azokban tárolt képeknek való téves megfeleltetés esélyei is arányosan növekednek.

–

– Az arcfelismerés majdnem hasznavehetetlen az olyan fajta alkalmazások esetében, amelyeket a szeptember tizenegyedikei New York-i és washingtoni támadások óta a legszélesebb körben vitatnak, vagyis a terroristák azonosítására valamely tömegben. Mint Bruce Schneier rámutat, ennek okai statisztikai természetűek. Erős túlzással tételezzük fel, hogy egy arcfelismerő rendszer 99,99 százalékig pontos. Más szóval, ha egy jó minőségű fénykép az arcunkról nem szerepel a „terroristafigyelő lista” adatbázisában, akkor 99,99 százalék a valószínűsége annak, hogy a szoftver nem produkál megfelelést, ha a valós életben találkozik az arcunkkal. Tegyük fel továbbá, hogy tízmillió közül egy légi utasnak van meg az arcképe az adatbázisban. Ekkor a 99,99 százalékos megbízhatóság valószínűleg jól hangzik, ugyanis ez annyit jelent, hogy tízezer esetből egyetlen egyszer fordul elő hiba. Tízmillió utas átfésülésekor azonban a tízezerből egy hibalehetőség már ezer hibát jelent, és csak egyetlen egy korrekt megfeleltetés fogja kiszűrni egy valódi terrorista képét. Más szóval, 1000 megfeleltetés közül 999 téves lesz, és minden egyes ilyen téves azonosítás időt és erőfeszítést igényel, amit biztonságunk más módon való megvédésére fordíthatnának. Talán lehet úgy is érvelni, hogy egyetlen megakadályozott repülőgép-eltérítés megéri az ezer téves riasztás kockázatát. Mihelyt azonban a közelmúltbeli támadások okozta kezdeti sokk alábbhagy, a hibás „találatok” óriási százalékaránya úgy fogja kondicionálni a biztonsági dolgozókat, hogy minden pozitív azonosítás esetében eleve tévedést tételezzenek fel. Az arcfelismerő rendszerek implementációjának és fenntartásának óriási költségei mind kárba vesznek. Tény, hogy a terroristák felismerése valamilyen tömegben olyan, mint a „tű a szénakazalban” problémája, az automatikus arcfelismerés pedig korántsem olyan minőségű technológia, ami alkalmas lenne a „tű a szénakazalban” problémák megoldására. A repülőgép-eltérítés sokféleképpen megakadályozható, és a forrásokat olyan intézkedésekre kellene fordítani, amelyek nagyobb valószínűséggel működni fognak.

–

– Számos társadalmi intézményt az a tényleges helyzet tart el, hogy az arcokhoz emberi beavatkozás nélkül nehéz neveket hozzáilleszteni. Ha az emberek azonosíthatók lennének pusztán azáltal, hogy megnéznek egy kirakatot vagy megebédelnek egy étteremben, ez óriási változást okozna társadalmunknak az ember személyéről kialakult felfogásában. Az emberek azt hallanák, hogy idegenek nevükön szólítják őket. A leendő vásárlók, akik besétálnak egy üzletbe, azt láthatnák, hogy hitelkártyájuk számlaegyenlegét más fontos információkkal együtt már elő is hívták és az eladó személyzet rendelkezésére bocsátották, még mielőtt egyáltalán érdeklődnének valamilyen áru felől. Az ilyen fajta információ idő előtti feltárása – még a magánszférába való behatolástól eltekintve is – befolyásolhatná a vásárló alkupozícióját.

–

– A nyilvánosság igen keveset tud azoknak a kameráknak a képességeiről, amelyek sok országban már szinte mindenütt megtalálhatók. Az emberek rendszerint nincsenek tudatában például annak, hogy a felvett képek infravörös tartománya mire használható. Még az „arcfelismerés” kifejezés sem mutatja, hogy a rendszer milyen könnyen ki tudja emelni az arckifejezéseket. Tetten érhetők tehát a „személyazonosságon” kívül olyan adatok is, amelyek az adott személy lelkiállapotát is tükrözik. Még ha a nagy nyilvánosságot minden évben megfelelően tájékoztatnák is a legújabb kamerák teljesítményéről, a szoftverek és az adatmegosztó rendszerek egyetlen év alatt is szinte észrevehetetlenül tökéletesebbé válhatnak.

–

– A legtöbb nyilvános helyen igen nehéz hatásosan jelezni a kamerák jelenlétét és képességeit, és még nehezebben lehet megszerezni ehhez az emberek tudatos hozzájárulását. Az áthaladás számos nyilvános helyen, például a kormányhivatalok vagy a centralizált közlekedési létesítmények helyiségein aligha választás lehetősége bárki számára, aki a modern világban kíván élni. Még a privát szektorban is egyre fokozódik a kiskereskedelmi vállalkozások (például az élelmiszer-üzletek) koncentrálódása, úgyhogy a fogyasztóknak kevés választási lehetőségük van, és kénytelenek alávetni magukat a domináns kereskedelmi vállalat felügyeleti gyakorlatának.

–

– Ha az arcfelismerési technológiák alkalmazásának olyan országok az úttörői, ahol a polgári szabadságjogok viszonylag erősek, még valószínűbb, hogy ezeket a technológiákat olyan országokban is alkalmazni fogják, ahol ezek a jogok alig léteznek. A fejlődés jelenlegi sebessége mellett húsz éven belül megvalósítható lesz a kínai kormány számára, hogy

arcfelismeréssel kövesse nyomon minden egyes személy nyilvános helyeken történő mozgását az egész országban.

Válaszok a nyilvános helyeken alkalmazott automatikus arcfelismerés mellett hangoztatott érvekre

> *„A civilizált világot terroristák támadták meg. Meg kell védenünk magunkat. Hadiállapot van, és le kell mondanunk bizonyos polgári szabadságjogokról abból a célból, hogy megvédjük magunkat a veszélyek ellen.”*

Minden bizonnyal sok területen meg kell erősítenünk biztonságunkat. Ezt mondogattam magamnak évekig. Itt a biztonság és a polgári szabadságjogok automatikus társítása az, ami megtévesztő. A biztonság sokféle olyan módon is javítható, amelyek nincsenek kihatással a polgári szabadságjogokra, ilyen például a reptéri alkalmazottak használatára szolgáló azonosítási rendszerek racionalizálása vagy az utaskísérők harcművészeti képzése. A biztonság növelhető olyan módokon is, amelyek nagymértékben erősítik a magánszférát, például azáltal, hogy megakadályozzák a személyazonosításra szolgáló adatok ellopását vagy a *Microsoft* termékeket jól megszerkesztett szoftverekkel helyettesítik. A biztonság növelésére irányuló számos új javaslatnak – a meglévő gyakorlatokhoz, például az utasok bőröndjének megfelelő alaposságú átkutatásához képest – minimális hatása van a magánszférára. A biztonság és a polgári szabadságjogok közötti „alku” tehát túl van értékelve, és számomra meglepő az a gyorsaság, amellyel a szabadság sok védelmezője a terroristatámadás következtében lemondott mindenféle erőfeszítésről társadalmunk központi értékeinek védelmében.

Ha túllépünk az automatikus képzettársításokon, világosan gondolkodhatunk az előttünk álló választási lehetőségekről. Újra kell terveznünk biztonsági berendezkedésünket, úgy, hogy mind a biztonságot, mind a polgári szabadságjogokat meg tudjuk védeni. Kétségesnek tűnik, hogy ha mi választhatunk, akkor a választható számos biztonsági intézkedés közül azokat fogjuk választani, amelyek – mint például a nyilvános helyeken alkalmazott automatikus arcfelismerés – csillagászati méretű veszélyeket hordoznak a privát szférára nézve. Az ilyen technológiák mellett szóló bármilyen érveléshez legalábbis igen nyomós bizonyítékok felsorakoztatására lenne szükség.

„Az arcfelismerés alkalmazása mellett világos és lényegre törő érvek szólnak. A terroristák közül kettőt kerestek, akiknek megvoltak a fényképei. Az arcfelismerő rendszerek a repülőtereken elkapták volna őket."

Nem vagyok benne biztos, csakugyan tudjuk-e, hogy a hatóságok birtokában levő képek elég jók voltak az arcfelismeréshez még annak a csekély számú gyanúsítottnak a kiszűrésére is, akik állítólag szerepeltek a terrorista-figyelő listán. Még ha adottnak is vesszük azonban ezt a feltételt, nem sok következik belőle. Először is az a tény, hogy a hatóságok a 19 gépeltérítő közül mindössze kettőre gyanakodtak, arra emlékeztet bennünket, hogy az automatikus arcfelismerés mindaddig nem képes azonosítani egy arcot, amíg az nincs az adatbázisban. A legtöbb gépeltérítő nem szerepelt a terrorista-gyanús személyek listáin, és még ha ezeket a bizonyos gépeltérítőket meg is akadályozták volna abban, hogy felszálljanak a repülőgépekre, a másik tizenhét felszállt volna.

Ennél is fontosabb, hogy a biztonsági eljárások a bostoni repülőtéren és másutt is sok szempontból olyan gyenge hatékonyságúak voltak, hogy igen sokféle lehetséges tökéletesítésük megakadályozhatta volna a gép-eltérítéseket. Ha elolvassuk azt a *White Paper*-t, amelyet az arcfelismerési rendszereket gyártó vezető vállalat, a *Visionics* adott ki a repülőgép-eltérítésekről, világossá válik, hogy az arcfelismerést valójában az azonosítási rendszerekben meglévő hiányosságok pótlásához ajánlják. A terrorista-figyelő listák tartalmazzák a terroristák neveit, így tehát az automatikus arcfelismerés csupán azokban az esetekben szükséges, amikor a kormány rendelkezik a terroristák jó minőségű arcképeivel, de nem tudja a nevüket (ami nem túlságosan gyakran fordul elő), vagy amikor a terroristák olyan nevekre kiállított hamis személyazonossági iratokat használnak, amelyek nem ismertek a hatóságok előtt. Úgy tűnik, hogy a mostani támadásokban néhány terrorista ártatlan emberek személyazonosságát lopta el. Ennek a problémának a legjobb megoldása a jelenlegi azonosítási eljárások (például a legalább tizenöt éve széles körben reklámozott állami *DMV*-k[*]) mélységesen romboló hatású gyöngeségeinek kiküszöbölése. Ha ezek a mostani támadások nem motiválnak bennünket azonosítási rendszereink hibáinak kijavítására, akkor csakugyan elvesztünk. De ha csakugyan kijavítjuk őket, akkor az automatikus arcfelismerés szerepe a többi biztonsági intézkedés kontextusában egészen marginálissá válik.

[*] A DMV (Department of MotorVehicles) rövidítés a gépjármű-nyilvántartási rendszerre utal. – *A ford*.

A polgári szabadságjogok szempontjából – a fentiek szem előtt tartásával – különbséget kellene tennünk az arcfelismerés különféle alkalmazásai között, amelyek elrendezhetők egy skála mentén. A skála egyik végén foglalnak helyet a nyilvános helyeken alkalmazott megoldások, például a tömeg pásztázása az üzletekben vagy a városi utcákon. Ezek azok, amelyeknek a betiltását javaslom. A skála másik végén elhelyezkedő megoldások erősen kötődnek a törvényes alkalmazás jogszerű folyamataihoz: ilyen például egy letartóztatott személy rendőrségi nyilvántartásba vett fényképének egybevetése olyan emberek képeivel, akiket a múltban letartóztattak. Amikor az automatikus arcfelismerés valamilyen alkalmazását fontolgatjuk, a várható hasznokat össze kell vetni a polgári szabadságjogokat érintő veszélyekkel. A repülőtéri biztonság fokozására javasolt alkalmazások a skála különböző pontjain helyezkednek el. A tömeg pásztázása egy repülőtéri terminálon a skála „nyilvános" vége felé esik, míg a beszálló utasok fényképes személyazonossági dokumentumainak ellenőrzése, ami oly módon történik, hogy a benne levő fényképet összehasonlítják azzal a fényképpel, amely az adatbázisban ehhez a kártyához tartozik, a skálának a „jogszerű eljárásokat" tartalmazó vége felé lesznek. Az arcok nyilvános helyeken való pásztázásának veszélyei (például az egyének potenciálisan semmihez sem köthető kategóriáinak nyomon követése) nem állnak fenn a skála „jogszerű eljárásokat" tartalmazó végén levő alkalmazások esetében. Fontos tehát, hogy a javasolt rendszereket ne csak a biztonságra apelláló elvont jelszavakat, hanem az alkalmazás konkrét körülményeit is figyelembe véve értékeljük.

> *„Az adatbázisunkban szereplő személyek valamennyien körözött bűnözők. Nem tárolunk egyetlen képet sem, amit a kameráink rögzítenek, kivéve abban az esetben, ha megfelelnek valamelyik képnek az adatbázisból. Így kizárólag a bűnözőknek lehet okuk bármilyen panaszra."*

Ezzel az érvvel kapcsolatban számos probléma merül fel.

(1) Bíznunk kell az Önök állításában, hogy csupán körözött bűnözők képeit tárolják az adatbázisban, és el kell hinnünk azt is, hogy kivétel nélkül törlik azokat a képeket, amelyek nem egyeznek meg semmivel sem az adatbázisban.
(2) Önök saját maguk sem tudják igazán, hogy vajon az adatbázisban szereplő valamennyi személy csakugyan bűnöző-e. Az ilyen adatbázisok minőségellenőrzése távolról sem tökéletes, mint ahogyan ez kiderült például a „bűnözőknek" arról az adatbázisáról, amelyet a

választói névjegyzékek megtisztogatására használtak fel néhány floridai választókörzetben a 2000. évi választások alkalmából.

(3) Azok az erők, amelyek az egyre fokozódó felügyelet sikamlós lejtőjén egyre lejjebb taszítanak bennünket, még akkor is nyomasztóak, ha az adatbázisban valóban kizárólag bűnözők szerepelnek. Ha egy ilyen rendszer létrejön és működik, miért nem bővítjük ki a listákat azokkal az állítólagos bajkeverőkkel, akiket a múltban kizártak az üzleti vállalkozásokból, de sohasem ítéltek el bűncselekményekért? Azután hozzátehetnénk azokat a büntetett előéletű személyeket is, akik már letöltötték a büntetésüket, majd azokat, akiket olyan kisebb szabálysértésekért ítéltek el, mint például az üzleti lopás. Ezután következhetnének azok, akiket bírói ítélet kötelez arra, hogy tartsák távol magukat bizonyos helyektől, továbbá a börtönök foglyai, a feltételesen szabadlábra helyezett foglyok, az utcai bandák tagjai, a katonák és azok az emberek, akiket bírói idézéssel köteleznek olyan kisebb szabálysértések következményeinek vállalására, mint például a kifizetetlen parkolási kihágásokért járó büntetések. Bővíthetnénk a listákat a külföldiekkel, akik lejárt vízummal tartózkodnak az országban, általában minden külföldivel, és az olyan emberekkel, akiknek valaha valamilyen idegrendszeri megbetegedésük volt. Nem kellene kihagyni azokat sem, akikre perdöntő tanúként igényt tartanak, továbbá az eltűnt személyeket, azokat a gyermekeket, akikért a szüleik aggódnak, az idős embereket, akikért a gyermekeik aggódnak, a szülőket, akik gyermekeik tartásdíjával elmaradásban vannak, valamint azoknak a vállalatoknak az alkalmazottait, amelyeknél arcfelismerő rendszer működik. Nem maradhatnának ki azután a gazdag emberek, akik félnek, hogy elrabolják őket, és az alkoholisták sem, akik nem akarják, hogy a kocsmákban meglássák őket, és végül következnének azok a személyek, akik szerződés aláírásával beleegyezésüket adták ahhoz, hogy nyomon kövessék őket. Amikor pedig mindezeket az embereket már feltettük a listára, innen már csak egy kis lépés lenne sok további kategória hozzáadása is.

> *„A nyilvános helyek nyilvánosak. Ha valaki történetesen észrevesz bennünket, amikor a parkban sétálunk, semmi alapunk nem lehet a panaszkodásra, ha úgy döntenek, hogy elmondják valaki másnak, hogy mi hol jártunk. Mindannyian ezt tesszük. Nem támasztható semmiféle ésszerű elvárás a magánszféra fenntartására valamely nyilvános helyen, és a szólásszabadság joga mindenki számára lehetővé teszi, hogy tényszerű információt közöljön arról, hogy merre jártunk.”*

Annak az embernek, aki észrevesz bennünket a parkban, számolnia kell azzal, hogy valaki őt is éppúgy észreveszi. A kamerák azonban névtelenek, és könnyű őket elrejteni. Még fontosabb a lépték kérdése. A legtöbb ember megérti azt az erkölcsi különbséget, ami a között a két eset között fennáll, hogy valaki esetleg megfigyel minket a parkban, illetve egy ezzel megbízott nyomozó követ bennünket mindenhová, ahova megyünk. A második esetben összegyűjtött információ nyilvánvalóan veszélyesebb. Sőt mi több, az erkölcs és a törvény egyaránt mindig is elismerte a privát szféra sokféle fajtáját a nyilvánosság előtt is. A sajtó például a legtöbb emberről nem közölhet olyan személyesen érzékeny szituációkban felvett képeket, amelyeknek nincs legitim hírértékük. Udvariatlanságnak számít nyilvános helyen belehallgatózni mások beszélgetésébe. A legszélesebb körben elterjedt arcfelismerés-alkalmazások egyértelműen a skála erkölcsi szempontból legproblematikusabb végén találhatók. Annak az esélye, hogy valaki észrevesz bennünket, különbözik attól a bizonyosságtól, hogy nyomon követnek.

A magánszféra „ésszerűen elvárható" tiszteletben tartásának követelménye az USA Legfelsőbb Bíróságának egyik döntéséből származik. Ezt a kifejezést széles körben bírálták, használhatatlannak nevezve, egyszerűen azért, mert a magánszféra fenntarthatóságára vonatkozó „ésszerű elvárások" valamely szituációban azonnal megszűnhetnek, mihelyt valaki az adott helyzetben rutinszerűen elkezd behatolni a magánszférába. A probléma az „elvárás" (*expectation*) szó gyakran kihasznált kétértelműségében van, ami egyrészt előrejelzést jelenthet (a nélkül a logikai következmény nélkül, hogy a világnak erkölcsileg meg *kellene* felelnie az elvárásnak), másrészt normát is (a nélkül a logikai következmény nélkül, hogy a világ ténylegesen meg *fog* felelni annak). A nyilvános helyeken alkalmazott automatikus arcfelismerés betiltása mellett érvelve az ember nem egyfajta általános, mindenre kiterjedő jog, a „nyilvános helyeken is fenntartható magánszférához való jog" mellett száll síkra, ami ésszerűtlen és gyakorlatilag kivihetetlen lenne, hanem azért a jogért, hogy védelmet élvezhessen a magánszférába technológiai eszközökkel való behatolás bizonyos típusai ellen. Ebben az esetben – egyrészt az eszközök folyamatos működése és standardizált teljesítménye, másrészt a legitim célok hiánya és a gyorsan csökkenő költségek miatt – kulcsfontosságú a technikai közvetítés.

A szólásszabadság jogára utaló érv hibás, mivel a javasolt tiltás nem az információ továbbítására vonatkozik, hanem az elektronikusan rögzített információk bizonyos fajtáinak létrehozására. Ugyanennek az információnak a továbbadásához való jog megmarad, ha az információt más módon szerzik meg.

„A nyilvános helyeken elhelyezett kamerák jelenlétének megfelelő tudatosítása könnyen megoldható. Európában sok nyilvános helyen találhatók ilyen feliratok: 'Ezt a térséget zártláncú televíziós rendszerrel figyelik'. Mi a probléma?"

Az a kifejezés, hogy „ezt a térséget zártláncú televíziós rendszerrel figyelik", nem megfelelő mértékig tudatosítja a közönségben, hogy a kamerák mire képesek, és még jóval kevebbet árul el arról, hogy mi fog történni azokkal a képekkel, amelyeket rögzítenek. Mivel a kamerák és azok képességei egyre változatosabbá válnak, az effajta figyelmeztetéseknek egyre részletesebbé, vagy pedig egyre semmitmondóbbá kell válniuk. Hasonló a helyzet a potenciális másodlagos felhasználók egyre bővülő körét tekintve is.

„Az automatikus arcfelismerés nemcsak rossz célokra szolgálhat. Pozitív felhasználásai is vannak. A technikai eszközök miniatürizálódásának köszönhetően például elhelyezhetünk egy készüléket akár a szemüvegünkben is, hogy emlékeztessen bennünket az emberek nevére, amikor találkozunk velük. Kétségtelen, hogy leleményes társadalmunk más pozitív használati módokkal is elő fog állni. Ne bélyegezzük meg elhamarkodottan a technológiát, csupán az elnyomás eszközét látva benne."

A technológiának valóban vannak pozitív felhasználási módjai. A bevezetésben megemlítettem néhányat azok közül a pozitív alkalmazások közül, amelyek nem foglalják magukban az emberek hozzájárulásuk nélküli megfigyelését a nyilvános helyeken. A fentiekre vonatkozó ellenérvek a következők: (1) a nyilvános helyeken a veszélyek nagyobbak, mint a pozitív lehetőségek, (2) még a pozitív felhasználások is általában együtt járnak az emberek beleegyezésük nélkül történő megfigyelésével, és (3) azok a pozitív alkalmazások, amelyekhez megvan az emberek hozzájárulása, szinte mindig ugyanolyan jól megoldhatók olyan más technológiák alkalmazásával is, amelyekkel nehezebb visszaélni.

„A technológiát nem lehet betiltani. A technológia mindenképpen használatba fog kerülni."

Ez az érv mindenféle törvénnyel szemben állna, ha lenne értelme egyáltalán. A gyilkosság tiltása nem azt jelenti, hogy nem követnek el egyetlen gyilkosságot sem. A társadalom – azáltal, hogy törvényeket fogad el a gyilkosság ellen – a jóról és a rosszról alkotott véleményét juttatja kifejezésre és elrettentő akadályt hoz létre; azokat pedig, akik gyilkosságot követnek el, eltávolítja az utcákról. Így kevésbé valószínű, hogy a gyilkosok újból gyilkosságot követnek el, és a gyilkosság általában sokkal nehezebbé és költségesebbé

válik. Az automatikus arcfelismerés a nyilvános helyeken nem olyan rossz, mint a gyilkosság, de az analógia világos: betiltása azt fejezné ki, hogy a közvélemény helyteleníti, és nehezebbé teszi a megvalósítását, mint amilyen egyébként lenne.

„A valódi megoldást az jelenti, ha gondoskodunk róla, hogy mindenki ki legyen téve a megfigyelésnek. Mihelyt a társadalom teljesen átlátszóvá válik, a hatalom birtokosai nem fogják tudni többé az elnyomás szolgálatába állítani a technológiát, mivel elnyomó törekvéseik is felügyelet alatt fognak állni."

Ez a forgatókönyv egyrészt irreális, másrészt erkölcstelen. A hatalom birtokosai definíciószerűen éppen azok, akik a leginkább képesek kitérni a felügyelet elől, és így a felügyeletnek még a lehető legnagyobb mértékű, járványszerű kiterjesztése esetén is ők lennének az utolsók, akik alávetik magukat az ellenőrzésnek. A totális felügyeleti rendszer önmagában is szélsőséges elnyomást jelentene, és mivel ennek a lakosság óriási része ellenállna, csupán szélsőséges elnyomás útján lehetne megvalósítani. Az az ígéret, hogy az elnyomást a hatalmasok ellen lehet majd fordítani, élénken emlékeztet az uralkodó osztályok elnyomására a francia, az orosz és a kínai forradalmakban. Magam is a demokrácia és az egyenlőség híve vagyok, de az is világos számomra, hogy ezeknek az értékeknek az előbbre viteléhez az általános elnyomás a legrosszabb út.

> *„Az automatikus arcfelismerés gátat vet a bűnözésnek. A rendőrség igényt tart rá. Egyes fárasztó és monoton rutinfeladataik automatizálása lehetővé tenné számukra, hogy korlátozott forrásaikat hatékonyabban használhassák fel, és ha ez megakadályozza akár csak egyetlen gyermek meggyilkolását, akkor támogatni kell."*

A szabad társadalom olyan társadalom, amelyben bizonyos korlátok szabják meg, hogy a rendőrség mit tehet meg. Ha szabad társadalom akarunk maradni, akkor döntést kell hoznunk ezekről a korlátokról. Ha egyszer üzembe helyeztek egy új felügyeleti technológiát, szinte lehetetlen megakadályozni, hogy azt – egyre lejjebb csúszva a síkos lejtőn – egyre szélesebb körű ellenőrzésre használják fel. Ezt világossá teszi többek között az autópályákon automatizált eszközökkel folyó díjbeszedés példája. Tisztán átlátható jogi védelem hiányában már kezdettől fogva fel kell tételeznünk, hogy minden technológiát, ami személyes információk megszerzésére szolgál, a törvények betartatására is fel fognak használni, mégpedig nem csupán olyan esetekben, ahol közvetlenül életek forognak kockán. A visszaélések lehetőségét tehát figyelembe kell vennünk, amikor döntést hozunk arról, hogy a technológiát egyáltalán alkalmazni akarjuk-e. Ezt előrebocsátván, aligha tekinthető

bizonyítottnak, hogy az arcfelismerés megakadályozza a bűnözést, amikor egy olyan világban vezetik be, amely máris sokféle bűnüldözési technológiával rendelkezik. A rendőrség rendelkezésére álló bűnfeltárási technológiák az utóbbi években óriási fejlődésen mentek keresztül, és még ha olyan esettel is találkozunk, ahol valamely bűnügyet egy adott technológia segítségével oldottak meg, ebből semmi esetre sem következik, hogy az ügyet nem lehetett volna ugyanolyan jól megoldani valami más technológia felhasználásával. Továbbá, még ha az arcfelismerés növeli is azoknak a bűnügyeknek a számát, amelyek megelőzhetők vagy megoldhatók, ezt az eredményt az arcfelismerés által lehetővé tett visszaélések révén elkövetett további bűnesetek számával összehasonlítva kell mérlegelni.

> *„Szolgáltam a hadseregben és a rendőrségnél is, és ha Önök is láttak volna néhány olyan dolgot, mint amiket én láttam, akkor meggondolnák magukat."*

Nem tudhatjuk, hogy az illető, aki ezt mondja, vajon mit látott. Azt viszont – mivel az újságok naponta felhívják rá a figyelmet – mindenki tudja, hogy minden nap gonosz bűntetteket követnek el. Ezzel az érvvel kapcsolatban az igazi probléma az, hogy a legtöbb, általam itt számba vett más érvhez hasonlóan – felhasználható arra, hogy abszolút hatalmat adjon a hadsereg és a rendőrség kezébe. Ha azonban ez bekövetkezne, akkor értelemszerűen nem lennénk többé szabad társadalom. Elvileg megalapozott érvekre van szükségünk ahhoz, hogy világosan lássuk a kormányzat helyét a szabad társadalomban, és az általam javasolt ellenérvek éppen ezt a célt szolgálják.

> *„Miért vannak Önök a törvények erélyes végrehajtása ellen? Az Önök, valamint a családjuk és vagyonuk biztonságát semmi más nem védi, csakis az erős végrehajtó szervezetek. A törvények betartatása nélkül az Önök vagyontárgyait pillanatokon belül ellopnák."*

A törvényszegések hatékony büntető szankciókkal sújtása mellett lehet érvelni, mint ahogyan ellene is, ám ez egyfajta kettősség leegyszerűsítését jelenti. A társadalomnak ugyanúgy kellene viszonyulnia a rendőrséghez, mint ahogyan a hadsereghez: természetesen szükségünk van rá, de ha kultúránk központi szervező elvévé válik, akkor bajba kerülünk. Veszélyes dolog létrehozni valamilyen bürokratikus kormányzati apparátust, ebben az esetben rendőrséget, és azt mondani: „Az Önök egyetlen feladata a bűnözés visszaszorítása, és erre a célra megadunk Önöknek bármit, amit csak kérnek". Ez lényegében az elnyomó központi

hatalmi rendszer kialakításának a receptje, ami hosszú távon a rendőrség számára sem jelent jobbat, mint bárki másnak. A demokrácia nem a szélsőségek közötti választást, hanem bizonyos egyensúlyok gondos kialakítását jelenti, és a legjobb ellenérv itt egyszerűen az, hogy egy bizonyos partikuláris technológia - esetünkben a nyilvános helyeken felhasznált automatikus arcfelismerés – olyan nagy mértékű kiegyensúlyozatlanságot hoz létre, amit a demokrácia már nem képes tolerálni.

„Az Önök érvelése a megfélemlítés taktikáját követi. Ahelyett, hogy síkos lejtőkről szóló forgatókönyvekkel ijesztgetik az embereket, miért nem csatlakoznak inkább ahhoz a konstruktív munkához, amivel meghatározhatjuk, hogy az adott rendszereket hogyan használhatjuk felelősségteljesen?"

A nyilvános helyeken alkalmazott automatikus arcfelismerési technológia mellett szóló érvek szintén „megfélemlítési taktikát" jelentenek annyiban, hogy a terrorizmustól való félelmünkre apellálnak. Bizonyos félelmek azonban jogosak, és ésszerű, ha beszélünk róluk. A terrorizmus indokolt félelmet kelt, de ugyanezt teheti egy olyan kormányzat által való elnyomás is, amely túl nagy hatalmat kapott. A történelem bőséggel szolgál példákkal mindkét esetre. Nagyon sok irányadó eset előfordult már, amelyek azt a feltételezést támasztják alá, hogy az automatikus arcfelismerést – mihelyt bevezetik és intézményesítik – egyre bővülő és egyre sokasodó célokra fogják felhasználni. A síkos lejtők metaforájával jelzett aggodalom nem puszta spekuláció, hanem azokkal a számtalan lehetőséggel összefüggő, nagyon is reális politikai stratégiákkal számol, amelyekre az automatikus arcfelismerés felhasználható. Az én javaslatom itt *ténylegesen* azt célozza, hogy működjünk közre abban a konstruktív munkában, ami döntéshez vezet az automatikus arcfelismerés felelősségteljes használatának kérdésében. Ez a technológia ugyanis olyan körülmények között használható fel felelősségteljesen, ahol az érintett egyéneket megfelelően ellátták a szükséges védekezési eszközökkel, és [éppen ezért] a nyilvános helyeken nem használható felelősségteljesen. Teljes mértékben tisztában vagyok azzal, hogy az automatikus arcfelismerés betiltása a nyilvános helyeken a szó szoros értelmében igen nagy lépés. A tiltás oka azonban egyszerű: azok a veszélyek, amelyeket az automatikus arcfelismerés a polgári szabadságjogokra nézve magával von, gyakorlatilag önmagukban is egész osztályt alkotnak.

> *„A szabadság nem lehet abszolút. Indokolt és elfogadható, hogy a kormány a közjó érdekében bizonyos elfogadható mértékig megnyirbálja a szabadságot."*

Minden bizonnyal így van. A kérdés csupán az, hogy a szabadság milyen megkurtításai járnak olyan haszonnal, ami megéri a kockázatot. A válasz itt egyszerűen az, hogy a nyilvános helyeken alkalmazott automatikus arcfelismerés nem állja ki ezt a próbát.

> *„A technológia nem hoz létre semmi újat. Ha a kormány követni akar valakit, amerre jár, civil ruhás detektíveket alkalmazhat erre. A technológia olcsóbbá teheti az emberek követését, de semmi olyat sem tesz lehetővé, ami azelőtt nem volt lehetséges."*

Ez igaz a legtöbb információs és kommunikációs technológiára, amelyeket az emberek olyan erők felerősítésére használnak, amelyek már korábban is léteztek a társadalomban. Az automatikus arcfelismerés ellen szóló érv nem az, hogy a technológia valami olyasmit teremt, ami minőségileg új, hanem az, hogy a demokrácia által eltűrhető szinten túlmenően felerősíti a ma is meglevő veszélyeket, például a politikai elnyomás fenyegetését.

> *„Miről beszélnek Önök? Az arcunk máris vonalkód. Mindenkinek az arca egyedi, és az emberek az arcunk alapján ismernek fel bennünket. Mindössze ennyit tesz a technológia is."*

Nos, ha azt állítjuk, hogy az arcunk nem vonalkód, ez elsősorban és mindenekelőtt nyilvánvalóan erkölcsi állásfoglalás. Az arcunkat nem lenne szabad vonalkódként *kezelni*. Ám az arcunk – ami a tényeket illeti – valóban nem vonalkód. Amikor valaki látja az arcunkat, ez nem ugyanaz, mint ha egy gép leolvas egy vonalkódot, mert az a személy, aki látja az arcunkat, nem tudja egykönnyen közölni valamely harmadik féllel, hogy az az arc, amit látott, milyen. Pontosan ezért van a rendőrségnek szüksége szakképzett kérdezőbiztosokra és speciális művészi technikák használatára a bűnözők arcképének a szemtanúk vallomása alapján történő megrajzolásához. Másrészt viszont egy automatikus arcfelismerő berendezés arcunknak egy olyan digitális ábrázolását készíti el, ami könnyen továbbítható, raktározható, továbbá összehasonlítható és társítható más információkkal is. Így tehát a technológia többet tesz, mint amit az emberek megtehetnek. Ha több különböző ember meglát bennünket több különböző helyen, nem tudják összekötni egymással az általuk érzékelt látványokat, hacsak nem tudják mindannyian a nevünket, vagy nem mutatják meg nekik a fényképünket, vagy a megjelenésünk valamilyen módon nem különböztethető meg igen markánsan másokétól. A különböző látványok egybevetéséhez még ilyenkor is jelentős erőfeszítésre van szükség. A gépek képesek ipari mennyiségben memorizálni emberek személyazonosságát, amit mi

magunk speciális képzés nélkül nem tudunk megtenni, továbbá igen nagy távolságokat áthidalva is képesek adatokat összegyűjteni és összeilleszteni, sokkal gyorsabban és hatékonyabban, mint az emberek. Az emberi és a gépi arcfelismerés közötti különbségek olyan nagy mértékűek, hogy ezek nem kezelhetők felcserélhető módon.

> *„Azok a veszélyek, amelyeket Ön vizionál, mind spekulatív természetűek. Ez a technológia nem ártott senkinek, és annak bizonyítása nélkül, hogy valóban veszélyes lenne, nem lehet halálra ítélni."*

Az arcfelismerést lehetővé tevő technológia drámai fejlődése aligha nevezhető spekulatívnak. Tudjuk, hogy milyen technológiák állnak további fejlesztés alatt a laboratóriumokban, és körülbelül azt is tudjuk, hogy mennyi időbe fog kerülni, amíg ezek is eljutnak a piacra. Ennélfogva indokolt a költségek történeti alakulási tendenciájának extrapolálása a belátható jövőre. A technológia képességei, amelyeket a következő néhány évtizedben fog felmutatni, aligha lehetnek kétségesek.

Nem sok kétségünk lehet továbbá a visszaélési lehetőségeket illetően sem. Nagy bőségben állnak rendelkezésünkre különféle példák más technológiák köréből, és a felelősség terhe valójában azokra hárul, akik úgy gondolják, hogy a nyilvános helyeken alkalmazott automatikus arcfelismerés ezekhez képest kivételt fog képezni. Az adatbázisok szivárogni fognak, a technológiák ugyanis mindig ki vannak téve üzemzavaroknak. Az információt másodlagos célokra is fel fogják használni. A törvények végrehajtásához alkalmazni fognak eredetileg más célokra tervezett technológiákat, a viszonylag szabad társadalmakban elért technológiai áttöréseket elnyomó rendszerek is használatba fogják venni, és az emberek életére bomlasztó hatást fognak gyakorolni az adatok minőségellenőrzésével kapcsolatos problémák. Nem arról van szó, hogy a nyilvános helyeken alkalmazott automatikus arcfelismerés a társadalmat egyik napról a másikra – vagy egyáltalán – átváltoztatná olyanná, amit Orwell írt le az „1984"-ben. Az automatikus arcfelismerésből származó károk lassanként fognak kibontakozni, mivel a technológiát nem azonnal és nem egyidejűleg vezetik be mindenütt, és mert az intézmények lassan változnak. A veszély azonban elég nagy, és ezt a történelem és a logika egyaránt eléggé alátámasztja ahhoz, hogy – amennyiben anyagi valósággá válik – meglehetősen nehéz lesz visszavonulót fújni, tehát minden okunk megvan arra, hogy most cselekedjünk.

„Amikor egy automatikus arcfelismerési rendszer valamilyen megfeleltetést produkál, ezt nem valamely bíró, esküdtszék vagy ítéletvégrehajtó teszi. Ha a nevünk valahol hibásan jelenik meg, ugyanolyan módon tisztázhatjuk magunkat, mint bármely más téves azonosítás esetében. Az automatikus arcfelismerés bizonyára nem tökéletes, de sokkal pontosabb, mint az emberi lények által végzett azonosítás, tehát érthetetlen, hogy miért akarják betiltani."

Az arcfelismerési rendszerek – ahogy a működésüket megalapozó technológiák költségei exponenciálisan csökkennek – igen könnyen mindenütt megjelenhetnek. Amikor ez megtörténik, a téves azonosítás lehetőségei is mindenütt adottak lesznek. Az emberek, illetve gépek által történő azonosítás valójában egyébként sem hasonlítható össze, mivel azok a feltételek, amelyek között a rendőrség az emberektől, illetve a gépektől megkapja bizonyos személyek azonosítását, teljesen eltérőek. Az emberek nem könnyen programozhatók arra, hogy felismerjenek nagyszámú olyan emberi arcot, amelyeket még sohasem láttak. A technológia elismerése és megbecsülése a pontosságán alapul, tehát amikor egy gép téves megfeleltetést produkál, ez jelentős bizalom-vesztéssel jár, ám egy személy által végzett téves azonosítás sokkal kisebb csorbát ejt az illető jó hírnevén. A hamis találatok lehetősége önmagában semmi esetre sem volna elegendő érv az automatikus arcfelismerés nyilvános helyeken való alkalmazása ellen. Más, erős érvekkel kombinálva azonban az ellene szóló döntő bizonyítékok részét képezi.

„A privát szféra fenntartása akadályozza a piac hatékony működését. Ha egy vállalat többet tud rólunk, személyre szabottan nyújthatja számunkra pontosan azt, amire szükségünk van. Ha megkérdezzük az embereket, hogy az ijesztő arcfelismerési rendszereket be kellene-e tiltani, akkor természetesen azt fogják mondani, hogy igen. Ám ez rossz kérdés. A jó kérdés az, hogy az emberek vajon hajlamosak-e információt kiadni saját magukról valami értékes dologért cserébe, és erre a legtöbb ember hajlandó lenne."

Ez úgynevezett *non sequitur* (nem következetes) érvelés. A privát szféra védelmére kevés olyan javaslat született, amelyek megakadályoznák az embereket abban, hogy önkéntesen információt szolgáltassanak saját magukról olyan vállalatoknak, amelyekkel üzletet kívánnak kötni. A probléma akkor keletkezik, amikor az információt az egyén tudta nélkül továbbítják, oly módon, ami könnyen zavart vagy kárt okozhatna, ha ismertté válna. Az automatikus

arcfelismerést az különbözteti meg sok más ugyanolyan jó azonosítási technológiától, hogy a megfigyelt emberek engedélye nélkül használható (és ennélfogva anélkül is, hogy az érintettek bármilyen egyezséget kötöttek volna valamilyen csereakcióra). Éppen ezért kellene betiltani.

> *„A magánszféra fenntartása melletti elkötelezettség bomlasztó és gyengítő hatású. A demokrácia megkívánja tőlünk, hogy közösségi emberek legyünk. A széleskörű titkolózás egészségtelen."*

A magánszféra fenntartása nem egyenlő a titkolózással, hanem csak azt jelenti, hogy az egyén ésszerű mértékig maga dönthesse el, hogy mely információkat tesz közzé magáról, és melyeket nem. Minden tisztességes társadalmi rend megkívánja, hogy mindenkinek joga legyen ehhez. Még ha bizonyos egyének úgy is döntenek, hogy akár patologikus módon titkolózni akarnak, nem kényszeríthetjük őket arra, hogy megváltozzanak, mert ez semmit sem javítana a helyzeten, és egyébként is – a kényszer lényegéből fakadóan – helytelen volna. A közösségi ember személyiségének értékét illetően pedig olyan technológiák fejlesztését kellene ösztönöznünk, amelyek megadják az embereknek a lehetőséget ahhoz, hogy ott, akkor és úgy jelenjenek meg a nyilvánosság előtt, ahogyan akarnak.

> *„Mit kell Önöknek takargatniuk?"*

Ezt a célzatos kérdést felhasználják szinte minden olyan kísérlet ellenében, ami a személyes privát szféra védelmére irányul, és a válasz minden esetben ugyanaz. Az embereknek nagyon sok olyan elfogadható okuk van bizonyos más személyek megakadályozására abban, hogy bizonyos információkat megszerezzenek róluk, mint például a személyes biztonság. A demokrácia csak akkor működik, ha a különféle csoportoknak lehetőségük van arra, hogy politikai stratégiáikat a kormányzattól és minden más létező, de általuk esetleg ellenzett érdekcsoporttól függetlenül dolgozhassák ki és hajthassák végre. Ez magában foglalja többek között az olyan emberek identitásának a titokban tartását is, akik esetleg valamely nyilvános helyen haladhatnak át, hogy egy privát politikai megbeszélésre összegyűljenek. Normális használata esetén. A „mit kell Önöknek takargatniuk?" kérdés antiszociálisként bélyegez meg mindenféle személyes autonómiát. Ez viszont – mivel tekintélyelvű követelmény – nem kaphat helyet a szabad társadalomban.

Ajánlott források

A magánszféra feletti őrködéssel szemben hangoztatott helytelen érvekre több válasz található az alábbi honlapon:
http://dlis.gseis.ucla.edu/people/pagre/arguments.html

Az arcfelismeréssel kapcsolatos viták a terrorista támadások után
A nyilvános helyeken alkalmazott arcfelismerési rendszerek használatát propagáló források
http://www.nytimes.com/2001/12/06/national/06SURV.html?pagewanted=print
http://www.washingtontechnology.com/news/16_15/state/17338-1.html
http://www.washingtonpost.com/wp-dyn/articles/A53844-2001Oct25.html
http://www.washingtonpost.com/wp-dyn/articles/A14273-2001Sep23.html
http://www.nytimes.com/2001/09/19/nyregion/19TECH.html
http://www.nytimes.com/2001/09/16/nyregion/16SECU.html?pagewanted=all
http://www.nytimes.com/2001/09/15/national/15CIVI.html
http://news.cnet.com/news/0-1003-200-7141717.html
A repülőtereken alkalmazott biometriai módszerek: hogyan kell és hogyan nem lehet megállítani Mahommed Attát és barátait. (Biometrics in Airports: How To, and How Not to, Stop Mahommed Atta and Friends).
http://www.anu.edu.au/people/Roger.Clarke/DV/BioAirports.html
Biometria: Szembenézve a terrorizmussal. (Biometrics: Facing Up to Terrorism).
http://www.rand.org/publications/IP/IP218/
Biometria: Egy pillantás az arcfelismerésre (Biometrics: A Look at Facial Recognition).
http://www.rand.org/publications/DB/DB396/
High-tech azonosítási lehetőségek kiaknázása az útlevelekben és vízumokban. (Passports and Visas to Add High-Tech Identity Features).
http://www.nytimes.com/2003/08/24/national/24IDEN.html?pagewanted=print
Az állhatatos és következetes biztonsági ellenőrzés megvalósítása csalóka cél a repülőtereken. (Consistent Security Is Elusive Airport Goal).
http://www.washingtonpost.com/wp-dyn/articles/A13786-2002Feb15.html
Az Európai Bizottság javaslata a biometriai azonosító jegyek meghatározására (European Commission's Proposal on Biometric Identifiers).

http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=IP/03/1289|0|RAPID&lg=EN&display=

A Viisage vállalat igazgatója belföldi biztonsági állást foglal el (Viisage Director Takes Homeland Security Post).

http://www.corporate-ir.net/ireye/ir_site.zhtml?ticker=VISG&script=410&layout=0&item_id=330130

Kétkedő kommentárok a terrorcselekmények megakadályozása terén alkalmazott arcfelismerés használatát illetően

http://www.wired.com/news/culture/0,1284,56878,00.html

http://www.reason.com/0210/fe.dk.face.shtml

http://www.wired.com/news/print/0,1294,54423,00.html

http://www.theregister.co.uk/content/55/25400.html

http://www.nytimes.com/2002/01/20/business/yourmoney/20PROF.html?pagewanted=print

http://www.nytimes.com/2002/01/15/science/physical/15FACE.html

http://www.zdnet.com/zdnn/stories/news/0,4586,5101223,00.html

http://www.pbs.org/cringely/pulpit/pulpit20011220.html

http://ComputerBytesMan.com/facescan/presentation/index.htm

http://www.nytimes.com/2001/10/07/magazine/07SURVEILLANCE.html?pagewanted=all

Az arcfelismeréssel kapcsolatos újságcikkek

Tökéletesedő arcfelismerési technológiák. (Face-Recognition Technology Improves (March 2003))

http://www.nytimes.com/2003/03/14/technology/14FACE.html

Az arcfelismerésen alapuló azonosítási rendszerek növekvő aggodalmat keltenek a privát szféra biztonságával kapcsolatban. (Facial ID Systems Raising Concerns About Privacy (August 2001))

http://washingtonpost.com/wp-dyn/articles/A12629-2001Jul31.html

Mosolyogjon, az üzlet kamerája felveszi az arcát! (Smile, You're on In-Store Camera (August 2002))

http://www.wired.com/news/print/0,1294,54078,00.html

Az arcfelismerési technológia új oldala: áldozatok azonosítása (New Side to Face-Recognition Technology: Identifying Victims (June 2002)).

http://www.nytimes.com/2002/01/15/science/physical/15FACE.html

Munkában az arcunk felismerését támogató dollárok (Your Face-Scan Dollars at Work (August 2001)).
http://www.wired.com/news/technology/0,1282,46018,00.html
Az arcfelismerési technológia gombostűre tűzi az embereket (Facial-Recognition Tech Has People Pegged (July 2001)).
http://www.cnn.com/2001/TECH/ptech/07/17/face.time.idg/
Az arcfelismerő berendezések belső énünkre fordítják a kamerákat (Face Scanners Turn Lens on Selves (July 2001)).
http://wired.com/news/privacy/0,1848,45687,00.html
Cikk a biometriai ipar reklámkezdeményezéséről (Article about a biometric industry public relations initiative (September 2001)).
http://www.wired.com/news/print/0,1294,46539,00.html
Hogyan találják meg az arcokat az arcfelismerési szoftverek? (How Facial Recognition Software Finds Faces (July 2001)).
http://abcnews.go.com/sections/scitech/CuttingEdge/cuttingedge010706.html
Rendőrségi szervek munkálkodnak a 3D arcfelismerési technológiák fejlesztésén (Law Enforcement Agencies Working on 3D Face Recognition Technology (September 1999)).
http://asia.cnn.com/TECH/computing/9909/24/3d.face.recognition.idg/
Az arcfelismerési technológia a Nagy Testvértől való félelmet gerjeszti (Face-Recognition Technology Raises Fears of Big Brother (February 2000)).
http://www.deseretnews.com/dn/view/0,1249,150015975,00.html
Mosolyogjon, kamera van jelen! (Smile, You're on Scan Camera (March 2001)).
http://www.wired.com/news/technology/0,1282,42317,00.html
Arcfelismerés mobiltelefonokon keresztül (Face Recognition Via Cell Phones (March 2002)).
http://www.internetnews.com/infra/print.php/999361

Egyéb hálózati források, amelyek háttér-információt nyújtanak az arcfelismerési technológiákról és azoknak a privát szférát sértő felhasználási lehetőségeiről
Az elektronikus privát szféra információs központjának arcfelismerési honlapja (Electronic Privacy Information Center Face Recognition Page).
http://www.epic.org/privacy/facerecognition/
A koalíció 2001. december 24.-ét „az alanyi jogok világnapjává” nyilvánította (Coalition Declares December 24, 2001 to Be "World Subjectrights Day"). http://wearcam.org/wsd.htm

Kereskedők arcfelismerési tesztje, 2002 (Facial Recognition Vendor Test 2002). http://www.frvt.org/FRVT2002/default.htm

Kereskedők arcfelismerési tesztje, 2000. (Facial Recognition Vendor Test 2000). http://www.dodcounterdrug.com/facialrecognition/DLs/FRVT_2000.pdf

http://www.dodcounterdrug.com/facialrecognition/FRVT2000/frvt2000.htm

Válogatott arcfelismerési fejlesztési programok (Selected Facial Scan Projects). http://www.facial-scan.com/selected_facial_scan_projects1.htm

Az USA kormányának honlapja a biometriai technológiák (köztük az arcfelismerés) témakörében. (US government site for biometric technology (including face recognition). http://www.biometrics.org/

Nézzünk szembe az igazsággal: új eszköz megnyilvánulásaink elemzésére (Facing the Truth: A New Tool to Analyze Our Expressions). http://www.hhmi.org/bulletin/may2001/faces/

Az arcfelismerési berendezéseket gyártó két domináns vállalat

http://www.visionics.com/faceit/

http://www.viisage.com/

A Viisage vállalat sok arca (The Many Faces of Viisage).

http://www.notbored.org/viisage.html

Egyéb vállalatok

http://www.visionspheretech.com/menu.htm

http://www.cognitec-ag.de/

http://www.c-vis.com/htdocs/english/facesnap/

http://www.neurodynamics.com/

http://www.imagistechnologies.com/

http://www.spiritcorp.com/face_rec.html

http://www.bioid.com/

http://www.keyware.com/

http://www.bionetrix.com/

Az arcfelismeréssel kapcsolatos műszaki kutatási programokkal foglalkozó honlapok

Arcfelismerés, észlelés és nyomon követés (Face Recognition and Detection).

http://home.t-online.de/home/Robert.Frischholz/face.htm

Felső arcmimikára alapozott, teljesen automatizált felismerés (Fully Automatic Upper Facial Action Recognition).

ftp://whitechapel.media.mit.edu/pub/tech-reports/TR-571.pdf

A DoD drogellenes program arcfelismerési technológiai programja (DoD Counterdrug Program Face Recognition Technology Program).

http://www.dodcounterdrug.com/facialrecognition/Feret/feret.htm

http://www.itl.nist.gov/iad/humanid/feret/feret_master.html

Miniatürizált hordozható arc-azonosítási technológia mindent átható számítástechnikai környezetben (Handheld Face Identification Technology in a Pervasive Computing Environment).

http://www.ai.mit.edu/projects/cbcl/publications/ps/pervasive-2002.pdf

Ruhán viselhető arcfelismerési és nyomon követési berendezések (Wearable Face Recognition and Detection).

http://www.gvu.gatech.edu/ccg/projects/face/

Arcok azonosítása videófelvételekről (Identification of Faces From Video).

http://staff.psy.gla.ac.uk/~mike/videoproj.html

Arcfelismerési algoritmusok értékelése (Evaluation of Face Recognition Algorithms).

http://www.cs.colostate.edu/evalfacerec/

Diasorozat az MIT emberi és gépi arcfelismeréssel foglalkozó kurzusának anyagából.

http://web.mit.edu/9.670/www/

A gesztusfelismerés honlapja (kapcsolódó technológiák) (Gesture Recognition Home Page (related technology)).

http://www.cybernet.com/~ccohen/

A különféle helyeken alkalmazott arcfelismerési rendszerekkel kapcsolatos vitákkal foglalkozó cikkek, megközelítőleg fordított időrendi sorrendben

***Borders* üzletek**

A *Borders* szóvivője először úgy nyilatkozott, hogy az arcfelismerés alkalmazására vonatkozó „valamennyi tervet felfüggesztette”, …

http://www.computerworld.com/storyba/0,4125,NAV47_STO63359,00.html

… majd tagadta, hogy valaha is volt ilyen szándéka.

http://www.politechbot.com/p-02447.html

A *Borders* azt tervezi, hogy arcfelismerést alkalmaz az üzleti tolvajok leleplezésére.

http://www.sundayherald.com/18007/

Kaszinók

Az OPP rejtett kamerákat használ a kaszinókban („a rendőrség titokban megfigyeli a vendégek arcát Ontario állam valamennyi kaszinójában”).
http://www.efc.ca/pages/media/2001/2001-01-16-a-torontostar.html

Boston

A repülőtéri terrorista-ellenes rendszerek meghibásodási tesztjei (Airport Anti-Terror Systems Flub Tests).
http://usatoday.printthis.clickability.com/pt/cpt?action=cpt&expire=&urlID=7387802&fb=Y&partnerID=1664

Az arcfelismerés kudarcot vall a bostoni repülőtéren (Face Recognition Fails in Boston Airport).
http://www.theregister.co.uk/content/55/26298.html

Logan ellenőrizni fogja az arcfelismerési adatbankok biztonságát (Logan Will Test Face-Data Security).
http://www.boston.com/dailyglobe2/298/metro/Logan_will_test_face_data_security+.shtml

Virginia Beach, Virginia

Virginia Beach közterületein arcfelismerő kamerákat helyeznek el (Virginia Beach Installs Face-Recognition Cameras).
http://www.washingtonpost.com/wp-dyn/articles/A19946-2002Jul3.html

Oakland, California

Oaklandi repülőtér: „Mosolyogjon a kamerába!” (Oakland Airport: "Smile for the Camera")
http://www.usatoday.com/life/cyber/tech/2001/10/18/airport-camera.htm

Huntington Beach, California

A Hungtinton Beach-i rendőrség az *Imagis* és az *ORION* vállalatokat bízta meg biometriai berendezések installációjával (Imagis and ORION Chosen to Install Biometrics by Huntington Beach Police).
http://cipherwar.com/news/01/imagis_big_brother.htm

Providence, Rhode Island

A repülőtér vezetője újra megfontolja, hogy zöld utat adjon-e az arcfelismerési technológiáknak (Airport Chief Reconsiders Face Recognition Technology for Green).

http://www.projo.com/cgi-bin/story.pl/news/06877271.htm

Ausztrália

SmartGate arcfelismerési rendszer kipróbálása a Sydney repülőtéren (SmartGate: A Face Recognition Trial at Sydney Airport).

http://www.anu.edu.au/people/Roger.Clarke/DV/SmartGate.html

Az utasokat titokban filmre veszik egy terrorista-ellenes kísérlet során (Passengers Secretly Filmed in Anti-Terror Trial).

http://www.smh.com.au/articles/2003/01/04/1041566268528.html

Colorado

Colorado állam kormányzója az arcfelismerési technológiával való visszaélések ellen (Colorado Governor Doesn't Want Face Recognition Technology Abused).

http://www.thedenverchannel.com/den/entertainment/stories/technology-87985620010719-070716.html

Colorado államban nem fognak arcfelismerési technológiákat alkalmazni a jogosítványok ellenőrzésére (Colorado Won't Use Facial Recognition Technology on Licenses).

http://www.thedenverchannel.com/den/entertainment/stories/technology-86955020010712-110740.html

Minnesota

Bevezetik a biztonsági arcfelismerést a repülőtéren? (Security Face-Scanning Coming to Airport?)

http://www.channel4000.com/msp/news/stories/news-131098520020319-070306.html

New York

Kamerák a terroristák arcának felismerésére a Szabadság szobor látogatói között (Cameras to Seek Faces of Terror In Visitors to the Statue of Liberty).

http://www.nytimes.com/2002/05/25/nyregion/25CAME.html

Missouri

Atomreaktor: mutasd az arcod! (Nuke Reactor: Show Me Your Face).

http://www.wired.com/news/print/0,1294,54423,00.html

Super Bowl (bajnokok ligája)

Az arcfelismerési adatbázisok kevés gyanúsítottal produkálnak megfeleltetést (Face Scans Match Few Suspects).

http://www.sptimes.com/News/021601/TampaBay/Face_scans_match_few_.shtml

Az ACLU ellenzi a high-tech megfigyelési eszközök alkalmazását Super Bowl mérkőzéseken (ACLU Protests High-Tech *Super Bowl* Surveillance).

http://www.usatoday.com/life/cyber/tech/2001-02-02-super-bowl-surveillance.htm

Felügyelet a *Super Bowl* mérkőzéseken: itt vannak a biometriai eszközök (*Super Bowl* Surveillance: Facing Up to Biometrics).

http://www.rand.org/publications/IP/IP209/IP209.pdf

A szövetségi ügynökök biometriai eszközöket használnak a *Super Bowl* mérkőzések szurkolóinak szűrésére (Feds Use Biometrics Against Super Bowl Fans).

http://www.theregister.co.uk/content/6/16561.html

Kamerákkal figyelték a szurkolókat – bűnözők vannak közöttük? (Cameras Scanned Fans for Criminals)

http://www.sptimes.com/News/013101/TampaBay/Cameras_scanned_fans_.shtml

Jacksonville, Florida

A rendőrségi spicli-kamerákkal kapcsolatos harc még folyik (Police Snooper Camera Fight Still Alive).

http://www.jacksonville.com/tu-online/stories/083101/met_7161286.html

Tampa, Florida

A tampai rendőrség eltávolítja az arcfelismerési rendszert (Tampa Police Eliminate Facial-Recognition System).

http://www.palmbeachpost.com/news/content/news/0820camera.html

Arcfelismerési technológia: bizonyítottan vásári komédia (Face Recognition Technology a Proven Farce).

http://www.theregister.co.uk/content/6/23559.html

Az arcok letapogatása Tampában (Facial Frisking in Tampa).

http://www.privacyfoundation.org/commentary/tipsheet.asp?id=46&action=0

A „Nagy Testvér” kamerák bűnözőket keresnek ("Big Brother" Cameras on Watch for Criminals).

http://www.usatoday.com/life/cyber/tech/2001-08-02-big-brother-cameras.htm

„Úgy éreztem magam tőlük, mint egy bűnöző” ("They made me feel like a criminal").
http://www.sptimes.com/News/080801/TampaBay/_They_made_me_feel_li.shtml
Polgári jogok, vagy csak savanyú a szőlő? (Civil Rights or Just Sour Grapes?)
http://www.sptimes.com/News/080301/TampaBay/Civil_rights_or_just_.shtml
Klikk. BEEP! Megvan az arc (Click. BEEP! Face Captured).
http://www.sptimes.com/News/071901/Floridian/Click_BEEP_Face_captu.shtml
Tampa felkészül a tüzetes vizsgálatokra (Tampa Gets Ready For Its Closeup).
http://www.time.com/time/nation/article/0,8599,167846,00.html
Álarcos tiltakozók fellépése az arcfelismerés ellen (Masked Protesters Fight Face Scans).
http://www.sptimes.com/News/071501/TampaBay/Masked_protesters_fig.shtml
Tampa arcfelismerési rendszert helyez üzembe egy utcán (Tampa Puts Face-Recognition System on Public Street).
http://www.usatoday.com/life/cyber/tech/2001-07-13-tampa-surveillance.htm
Tampában bűnözőket keresve rögzítik az arcokat a tömegekben (Tampa Scans the Faces in Its Crowds for Criminals).
http://www.nytimes.com/2001/07/04/technology/04VIDE.html
Közérdekű rádióriport a vitákról
http://www.npr.org/ramfiles/atc/20010702.atc.14.rmm
Az ybori rendőrség kamerái fejlett kém-technológiai eszközzé válnak (Ybor Police Cameras Go Spy-Tech).
http://www.sptimes.com/News/063001/TampaBay/Ybor_police_cameras_g.shtml

Palm Beach, Florida

A Palm Beach-i repülőtéren nem fognak arcfelismerési technológiát alkalmazni (Palm Beach Airport Won't Use Face-Scan Technology).
http://www.local6.com/orlpn/news/stories/news-148124920020526-160533.html
Az arcfelismerő rendszercsomag meghibásodott egy floridai repülőtéren (Face Recognition Kit Fails in Florida Airport).
http://www.theregister.co.uk/content/55/25444.html

Nagy-Britannia

Agytröszt sürgeti az arcfelismerés alkalmazását tömegesen látogatott helyeken (Think Tank Urges Face-Scanning of the Masses).
http://www.theregister.co.uk/content/6/20966.html

Arcfelismerési technológia az Egyesült Királyságban:

http://www.urban75.com/Action/cctv.html

http://www.sourceuk.net/articles/a00624.html

Izland

Izland bizalommal fordul az arcfelismerés felé (Iceland Places Trust in Face-Scanning).

http://news.bbc.co.uk/hi/english/sci/tech/newsid_1780000/1780150.stm

Az izlandi Keflavik repülőtér Visionics' FaceIt szoftverrel korszerűsíti zárt láncú televíziós rendszerét (Iceland's Keflavik Airport Upgrades CCTV System with Visionics' FaceIt)

http://ir.shareholder.com/vsnx/ReleaseDetail.cfm?ReleaseID=45325

Philip E. Agre

Amerikai informatikus, adatvédelmi szakértő. 1998 óta a Kaliforniai Egyetem Los Angeles-i kampuszának professzora. Ph.D. fokozatát 1989-ben informatikából szerezte a mesterséges intelligencia témakörében. Tanított többek között a Chicagói Egyetemen, a Sussexi Egyetemen és a San Diego-i Egyetemen. Számos tanulmánya jelent meg, több könyv szerzője és szerkesztője. Jelenlegi kutatási területe az informatikai rendszerek szervezeti változásai, ezen belül is kiemelt témája az informatikai rendszereknek a privát szférára gyakorolt hatása. Az *Electronic Privacy Information Center* tanácsadó testületének tagja. A „*Red Rock Eater News Service*" című hírlevél szerkesztője.