EFF'S SURVEILLANCE SELF-DEFENSE

SIMU ZA MKONONI: UFUATILIAJI WA MAHALI

https://ssd.eff.org/en/about-surveillance-self-defense

ELECTRONIC FRONTIER FOUNDATION

LOCALIZATION LAB

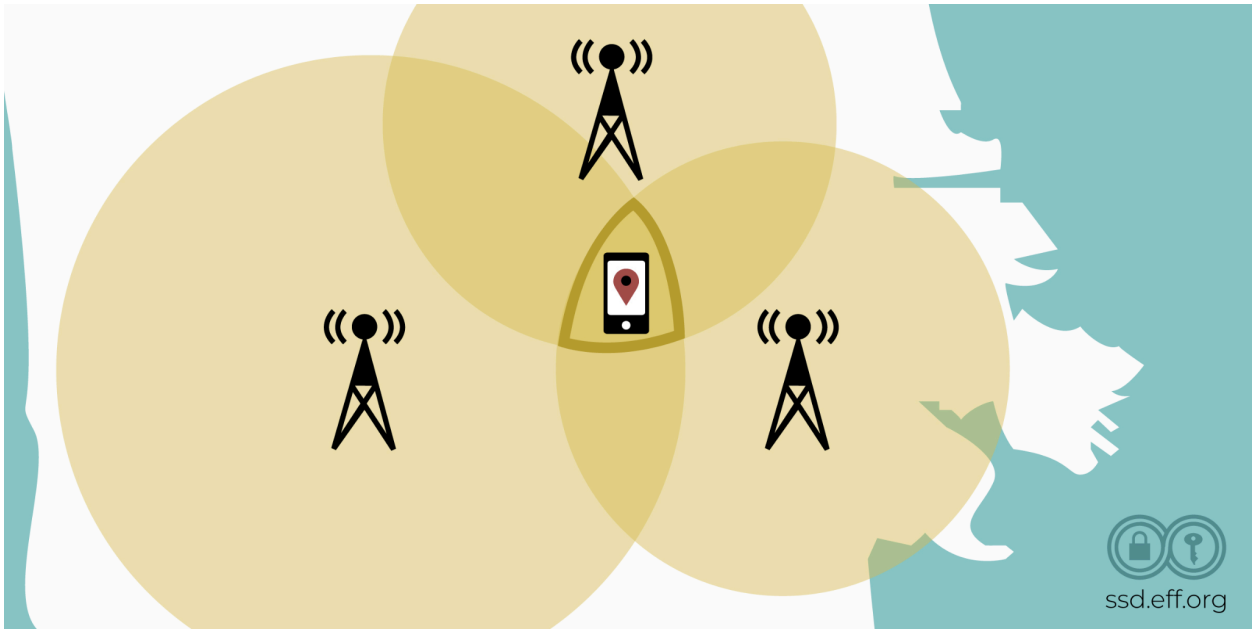
Ufuatiliaji wa Mahali

Tishio kubwa zaidi la ufaragha kutoka kwa simu za mkononi—lakini ambalo mara nyingi halionekani kabisa—ni jinsi zinavyoonyesha mahali ulipo siku nzima (na usiku wote) kupitia mawimbi zinazotoa. Kuna angalau njia nne ambazo eneo la simu ya mtu binafsi linaweza kufuatiliwa na wengine.

- Ufuatiliaji wa Mawimbi ya Simu kutoka kwa Minara
- Ufuatiliaji wa Mawimbi ya Simu kutoka kwa Viigaji vya Tovuti ya Simu
- Ufuatiliaji wa Wi-Fi na Bluetooth
- Uvujaji wa Taarifa za Mahali kutoka kwa Programu na Kuvinjari kwenye Wavuti

Ufuatiliaji wa Mawimbi ya Simu - Minara

Katika mitandao yote ya kisasa ya rununu, mwendeshaji anaweza kujua mahali simu ya mteja fulani iko wakati wowote simu imewashwa na kusajiliwa na mtandao. Uwezo wa kufanya hivi unatokana na jinsi mtandao wa simu unavyoundwa na kwa kawaida hujulikana kama kupata sehemu isiyojulikana kwa kutumia pembe kutoka kwa sehemu zinazojulikana .



Njia moja ambayo kampuni ya huduma za mawasiliano inaweza kutumia kufanya hivyo ni kuangalia nguvu ya mawimbi ambayo minara tofauti hupata kutoka kwa simu ya mkononi ya mteja fulani na kisha kuhesabu mahali ambapo simu hiyo inapaswa kuwa ili kufikia matokeo hayo. Hii hufanywa kwa vipimo vya Pembe ambayo Mawimbi Yanafikia Antena au AoA. Usahihi ambao kampuni ya huduma za mawasiliano inaweza kufahamu eneo la mteja hutofautiana kulingana na mambo mengi, ikiwa ni pamoja na teknolojia ambayo kampuni hiyo ya huduma za mawasiliano hutumia na ni minara mingapi ya seli iliyonayo katika eneo. Kwa kawaida, kwa angalau minara 3 ya seli kampuni ya huduma za mawasiliano inaweza kuwa na usahihi wa hadi ¾ ya maili au kilomita 1. Kwa simu za mkononi za kisasa na mbinu ya kijiometri inayotumiwa kuamua eneo kwa kupima umbali wake kutoka kwa angalau sehemu tatu zinazojulikana ya mitandao pia hutumiwa. Hasa, hutumiwa ambapo kipengele cha "locationInfo-r10" kinatumika. Kipengele hiki hurejesha ripoti ambayo ina viwianishi kamili vya GPS vya simu hiyo.

Hakuna njia ya kujificha kutokana na aina hii ya ufuatiliaji mradi tu simu yako ya mkononi imewashwa, ina kadi ya SIM iliyosajiliwa na inatuma mawimbi kwa mtandao wa kampuni ya huduma za mawasiliano. Ingawa kwa kawaida ni kampuni ya huduma za mawasiliano pekee inayoweza kutekeleza ufuatiliaji wa aina hii, serikali inaweza kulazimisha kampuni hiyo ya huduma za mawasiliano kushiriki data ya eneo kuhusu mtumiaji (katika muda halisi au kama rekodi ya kihistoria). Mnamo 2010, mtetezi wa ufaragha wa Ujerumani anayeitwa Malte Spitz alitumia sheria za ufaragha kufanya kampuni yako ya huduma za mawasiliano kuwasilisha rekodi ilizokuwa nazo kuhusu rekodi zake; alichagua kuzichapisha kama nyenzo ya kielimu ili watu wengine waelewe jinsi kampuni za huduma za mawasiliano zinaweza kufuatilia watumiaji kwa njia hii. (Unaweza kutembelea hapa ili kuona kile kampuni hiyo ya huduma za mawasiliano ilikuwa inajua kumhusu.) Uwezekano wa serikali kufikia aina hii ya data si wa kinadharia: tayari inatumiwa sana na walinda usalama katika nchi kama Marekani.

Aina nyingine inayohusiana ya ombi la serikali inaitwa kuomba data yote kuhusu mnara; katika hali hii, serikali huomba kampuni ya huduma za mawasiliano orodha ya vifaa vyote vya simu ya mkononi ambavyo vilikuwepo katika eneo fulani kwa wakati fulani. Hii inaweza kutumika kuchunguza uhalifu, au kujua ni nani aliyekuwepo kwenye maandamano fulani.

- Inasemekana kuwa, serikali ya Ukraine ilitumia njia hii kwa madhumuni haya mnamo 2014, kupata orodha ya watu wote ambao simu zao za mkononi zilikuwepo kwenye maandamano dhidi ya serikali.
- Katika kesi ya Carpenter dhidi ya Marekani, Mahakama Kuu iliamua kwamba kupata taarifa za kihistoria za eneo la simu ya mkononi (CSLI) zenye maeneo halisi ya simu za mkononi bila kibali kunakiuka Marekebisho ya Nne.

Watoa huduma pia hubadilishana data kuhusu eneo ambalo kifaa kinaunganishwa kwa sasa. Data hii mara nyingi huwa si sahihi kwa kiasi fulani kuliko data ya kufuatilia ambayo hujumlisha uchunguzi wa minara mingi, lakini bado inaweza kutumika kama msingi wa huduma zinazofuatilia kifaa mahususi—ikiwa ni pamoja na huduma za kibiashara ambazo huomba rekodi hizi ili kupata mahali simu mahususi inaunganishwa kwa sasa kwenye mtandao wa simu na kufanya matokeo haya yapatikane kwa wateja wa serikali au wa kibinafsi. (Gazeti la *Washington Post* liliripoti jinsi taarifa hizi za ufuatiliaji zinapatikana kwa urahisi.) Tofauti na mbinu za awali za ufuatiliaji, ufuatiliaji huu hauhusishi kulazimisha watoa huduma kuwasilisha data ya mtumiaji; badala yake, mbinu hii hutumia data ya eneo ambayo inapatikana kwa misingi ya kibiashara.

Ufuatiliaji wa Mawimbi ya Simu - Viigaji vya Tovuti ya Simu

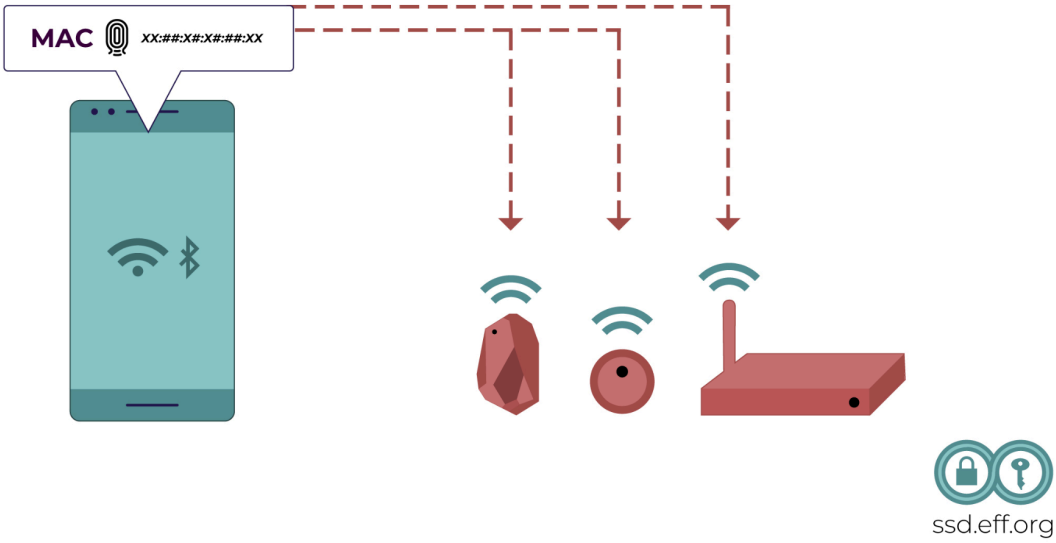
Serikali au shirika lingine lililobobea kitaalamu linaweza pia kukusanya data ya eneo moja kwa moja, kama vile kiigaji cha tovuti ya simu ya mkononi (mnara bandia unaoweza kubebeka wa simu unaoiga mnara halisi, ili "kunasa" simu za mkononi za watumiaji fulani na kugundua simu zao za mkononi. uwepo wao na/au kupeleleza mawasiliano yao, pia wakati mwingine huitwa Kinasa IMSI au Stingray). IMSI inarejelea Nambari ya Kitambulisho cha Kimataifa ya Msajili wa Simu ambayo hutambua kadi ya SIM ya mteja fulani, ingawa Kinasa IMSI kinaweza kulenga kifaa fulani kwa kutumia sifa zingine za kifaa hicho pia.

Kinasa IMSI kinahitaji kupelekwa katika eneo fulani ili kupata au kufuatilia vifaa katika eneo hilo. Kumbuka kuwa uingiliaji wa trafiki wa IMSI kwa utekelezaji wa sheria unapaswa kufikia masharti ili kupata kibali. Hata hivyo, CSS "haramu", (ambayo haijaanzishwa na wasimamizi wa sheria) itakuwa ikifanya kazi nje ya vigezo hivyo vya kisheria.

Kwa sasa hakuna ulinzi wa kuaminika dhidi ya vinasa IMSI vyote. (Baadhi ya programu zinadai kutambua uwepo wao, lakini utambuzi huu si kamilifu.) Kwenye vifaa vinavyoiruhusu, inaweza kusaidia kuzima uwezo wa kutumia 2G (ili kifaa hicho kiweze kuunganishwa kwenye mitandao ya 3G na 4G pekee) na kuzima utumiaji wa mitandao ukiwa nje ya eneo lako ikiwa hutarajii kusafiri nje ya eneo la huduma la mtoa huduma wa eneo lako. Zaidi ya hayo, inaweza kusaidia kutumia ujumbe uliosimbwa kwa njia fiche kama vile Mawimbi, WhatsApp au iMessage ili kuhakikisha kuwa maudhui ya mawasiliano yako hayawezi kuingiliwa. Hatua hizi zinaweza kulinda dhidi ya aina fulani za vinasa IMSI.

Ufuatiliaji wa Wi-Fi na Bluetooth

Simu mahiri za kisasa zina visambazaji vingine vya redio pamoja na kiolesura cha mtandao wa simu. Kawaida pia zina usaidizi wa Wi-Fi na Bluetooth. Ishara hizi husambazwa kwa nguvu ndogo kuliko mawimbi ya simu ya mkononi na kwa kawaida zinaweza kupokelewa tu ndani ya masafa mafupi (kama vile ndani ya chumba kimoja au jengo moja), ingawa mtu anayetumia antena ya kiwango cha juu anaweza kutambua mawimbi haya kutoka umbali mrefu usiotarajiwa; katika maandamano ya 2007, mtaalam nchini Venezuela alipokea ishara ya Wi-Fi kwa umbali wa kilomita 382 au maili 237, chini ya hali ya vijijini na uingiliaji mdogo wa redio. Hata hivyo, hali hii ya safu kama hiyo haiwezekani. Aina hizi mbili za mawimbi yasiyotumia waya ni pamoja na nambari ya kipekee ya kifaa, inayoitwa anwani ya MAC, ambayo inaweza kuonekana na mtu yeyote anayeweza kupokea mawimbi hayo.



Wakati wowote Wi-Fi imewashwa, simu mahiri ya kawaida itatuma "maombi ya uchunguzi" ya mara kwa mara ambayo inajumuisha anwani ya MAC na itawaruhusu watu wengine walio karibu kutambua kuwa kifaa hiki mahususi kipo. Vifaa vya Bluetooth hufanya vivyo hivyo. Vitambuzi hivi vimekuwa zana muhimu kwa vifuatiliaji tu katika maduka ya reja reja na maduka ya kahawa ili kukusanya data kuhusu jinsi vifaa na watu wanavyosafiri ulimwenguni. Hata hivyo, kwenye masasisho ya hivi majuzi kwenye iOS na Android, anwani ya MAC iliyojumuishwa katika maombi ya uchunguzi hunasibishwa kwa chaguo-msingi kiprogramu, hali ambayo hufanya ufuatiliaji wa aina hii kuwa mgumu. Kwa kuwa uwekaji nasibu wa MAC unatokana na programu, inaweza kushindwa na anwani chaguo-msingi ya MAC ina uwezo wa kuvuja. Zaidi ya hayo, baadhi ya vifaa vya Android huenda visitekeleze ubahatishaji wa MAC ipasavyo (upakuaji wa PDF).

Ingawa simu za kisasa kwa kawaida hunasibisha anwani zinazoshiriki katika maombi ya uchunguzi, simu nyingi bado hushiriki anwani thabiti ya MAC na mitandao ambayo zinajiunga nayo, kama vile kushiriki muunganisho na vipokeasauti vya maskioni visivyotumia waya. Hii inamaanisha kuwa kampuni za huduma za mawasiliano zinaweza kutambua vifaa mahususi baada ya muda na kueleza kama wewe ni mtu yule yule uliyejiunga na mtandao huo hapo awali (hata kama hutaandika jina lako au anwani ya barua pepe popote au kuingia kwenye huduma zozote) .

Mifumo kadhaa ya uendeshaji inaelekea kuwa na anwani za MAC zilizonasibishwa kibahati nasibu kwenye WiFi. Hili ni suala tata, kwa kuwa mifumo mingi ina hitaji halali la anwani thabiti ya MAC. Kwa mfano, ukiingia

katika mtandao wa hoteli, mtandao huo hufuatilia uidhinishaji wako kupitia anwani yako ya MAC; unapopata anwani mpya ya MAC, mtandao huo huona kifaa chako kama kifaa kipya. iOS 14 ina mipangilio kwa kila mtandao, "Anwani za binafsi za MAC."

Uvujaji wa Taarifa za Mahali Kutoka kwa Programu na Kuvinjari kwenye Wavuti

Simu razini za kisasa hutoa njia kwa simu kubaini mahali ilipo, mara nyingi hutumia GPS na wakati mwingine kutumia huduma nyingine zinazotolewa na kampuni za eneo (ambazo kwa kawaida huomba kampuni kukisia mahali simu ilipo kulingana na orodha ya minara ya simu na/au mitandao ya Wi-Fi ambayo simu inaweza kuona kutoka mahali ilipo). Maelezo haya huwekwa kwenye kipengele ambacho Apple na Google huita "Huduma za Mahali". Programu zinaweza kuomba maelezo ya eneo hili kwa simu na kuyatumia kutoa huduma zinazolingana na eneo, kama vile ramani zinazoonyesha eneo lako kwenye ramani. Muundo wa hivi majuzi zaidi wa ruhusa umesasishwa ili programu ziombe kutumia eneo. Hata hivyo, baadhi ya programu zinaweza kuwa na nguvu zaidi kuliko zingine zinazoomba kutumia GPS au muunganisho wa Huduma za Mahali.

Baadhi ya programu hizi zitasambaza eneo lako kupitia mtandao kwa mtoa huduma, ambaye, kwa upande wake, hutoa njia kwa ajili ya programu na wahusika wengine ambao wanaweza kushiriki nao kukufuatilia. (Huenda wasanidi programu hawakuhamasishwa na hamu ya kufuatilia watumiaji, lakini bado wana uwezo wa kufanya hivyo na wanaweza kufichua maelezo ya eneo

kuhusu watumiaji wao kwa serikali au uvunjaji wa data.) Baadhi ya simu razini itakupa aina fulani ya udhibiti ikiwa programu zinaweza kujua eneo lako halisi; mazoezi mazuri ya ufaragha ni kujaribu kuzuia ni programu zipi zinaweza kuona maelezo haya na kuhakikisha kuwa eneo lako linashirikiwa pekee na programu unazoamini na ambazo zina sababu nzuri ya kujua mahali ulipo.

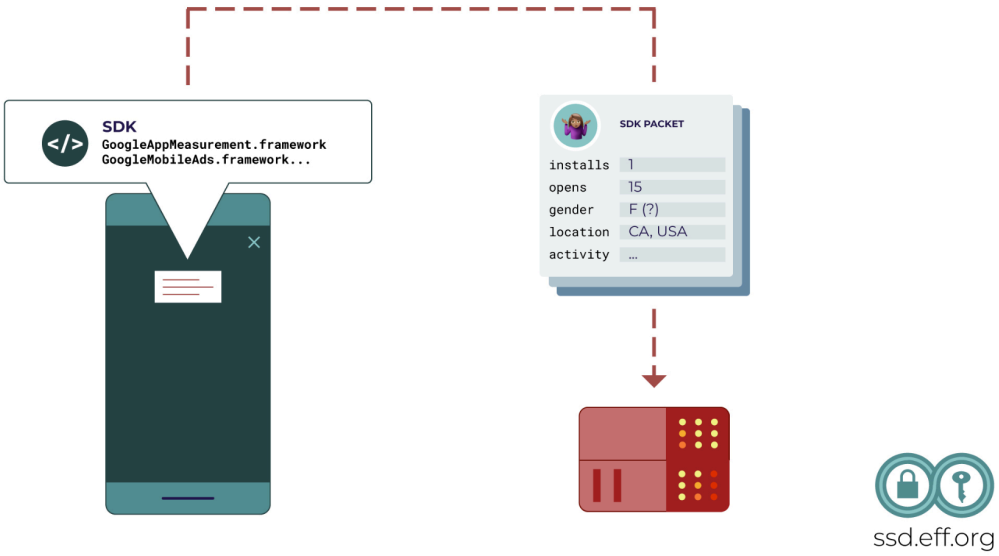
Katika kila hali, ufuatiliaji wa eneo si tu kuhusu kutafuta mahali mtu alipo kwa sasa, kama vile katika eneo la kusisimua la kukimbizana kwa filamu ambapo mawakala wanafuata mtu mitaani. Inaweza pia kuwa kuhusu kujibu maswali kuhusu shughuli za kihistoria za watu na pia kuhusu imani zao, kushiriki katika matukio na mahusiano ya kibinafsi. Kwa mfano, ufuatiliaji wa eneo unaweza kutumika ili kujua kama watu fulani wako kwenye uhusiano wa kimapenzi, kujua ni nani aliyehudhuria mkutano fulani au ni nani alikuwa kwenye maandamano fulani, au kujaribu kutambua chanzo cha siri cha mwandishi wa habari.

Gazeti la *Washington Post* liliripoti mnamo Desemba 2013 kwenye zana za ufuatiliaji wa eneo la NSA ambazo hukusanya kiasi kikubwa cha taarifa "kuhusu mahali simu za mkononi zilipo duniani kote," hasa kutoka kwa miundombinu ya makampuni ya simu ili kuangalia ni minara gani simu mahususi zinaunganishwa nayo wakati simu hizo zimeunganishwa kwenye minara hiyo. Zana inayoitwa CO-TRAVELER hutumia data hii kutafuta uhusiano kati ya mienendo ya watu tofauti (ili kubaini ni vifaa vipi vya watu vinaonekana kusafiri pamoja, na pia ikiwa mtu mmoja anaonekana kumfuata mwingine).

Ukusanyaji wa Data ya Tabia na Vitambulisho vya Utangazaji vya Simu

Kando na data ya eneo iliyokusanywa na baadhi ya programu na tovuti, programu nyingi hushiriki taarifa kuhusu mwingiliano wa kimsingi zaidi, kama vile usakinishaji wa programu, kufungua, matumizi na shughuli nyinginezo. Taarifa hizi mara nyingi hushirikiwa na kampuni nyingi za wahusika wengine katika mfumo ikolojia wa utangazaji unaowezeshwa na zabuni ya wakati halisi (RTB). Licha ya hali ya kawaida ya vidokezo vya data binafsi, kwa jumla data hii ya tabia bado inaweza kufichua maelezo mengi.

Kampuni za teknolojia ya utangazaji huwashawishi wasanidi programu kusakinisha vipande vya msimbo katika hati za kifurushi cha ukuzaji programu (SDK) ili kuonyesha matangazo katika programu zao. Sehemu hizi za msimbo hukusanya data kuhusu jinsi kila mtumiaji anavyoingiliana na programu hiyo, kisha kushiriki data hiyo na kampuni nyingine ya ufuatiliaji. Kifuatiliaji kinaweza kushiriki tena maelezo hayo na watangazaji wengine kadhaa, watoa huduma wa utangazaji na mawakala wa data katika mnada wa RTB wa milisekunde.



Data hii hukuwa na maana kutokana na kitambulisho cha utangazaji wa simu ya mkononi, au MAID, nambari ya kipekee ya nasibu ambayo hutambulisha kifaa kimoja. Kila kundi la taarifa zilizoshirikiwa wakati wa mnada wa RTB kawaida huhusishwa na MAID. Watangazaji na mawakala wa data wanaweza kukusanya pamoja data iliyokusanywa kutoka kwa programu nyingi tofauti kwa kutumia MAID na kwa hivyo kuunda wasifu wa jinsi kila mtumiaji anayetambuliwa na MAID anavyofanya. MAIDs wenyewe hawaambatanishi habari kuhusu utambulisho halisi wa mtumiaji. Hata hivyo, mara nyingi si jambo ndogo kwa wakala wa data au watangazaji kuhusisha MAID na utambulisho halisi, kwa mfano kwa kukusanya jina au barua pepe kutoka ndani ya programu.

Vitambulisho vya tangazo la kifaa cha mkononi vimeundwa katika Android na iOS, pamoja na vifaa vingine kadhaa kama vile viweko vya michezo, kompyuta kibao na vifaa vya kupokea mawimbi vya runinga. Kwenye Android, kila programu na kila programu nyingine iliyosakinishwa katika programu hizo, zinaweza kufikia MAID kwa chaguo-msingi. Zaidi ya hayo, hakuna njia ya kuzima MAID kwenye kifaa cha Android kamwe: mtumiaji anaweza tu "kuweka upya" kitambulisho na kukibadilisha na nambari mpya ya nasibu. Katika toleo jipya zaidi la iOS, programu hatimaye zinahitaji kuomba ruhusa kabla ya kukusanya na kutumia kitambulisho cha tangazo la simu ya mkononi. Hata hivyo, bado haijulikani ikiwa watumiaji wanatambua ni washirika wangapi wanaweza kuhusika wanapokubali kuruhusu programu inayoonekana kutokuwa na hatari kufikia taarifa zao.

Data ya tabia iliyokusanywa kutoka kwa programu za simu hutumiwa kimsingi na makampuni ya utangazaji na mawakala wa data, kwa kawaida kufanya ulengaji wa kitabia kwa matangazo ya kibiashara au ya kisiasa. Lakini serikali zimejulikana kutumia ufuatiliaji unaofanywa na kampuni za kibinafsi.

Maelezo zaidi kuhusu ufuatiliaji wa kivinjari: Je, Kuweka Kitambulisho cha Kipekee ni Nini?