IN5 T5 Tiedosta tulee pelottavaa

Salaisuuksia, joita emme edes ymmärrä paljastavamme

Jaammeko tietämättämme enemmän tietoa itsestämme kun käytämme erilaisia sovelluksia ja verkkosivustoja? Käyttämällä algoritmeja ja data-analyysiä, pienet palaset tietoa voidaan koota yhteen, jotta saadaan tietää enemmän meistä, kuin olemme koskaan halunneet paljastaa.

Joskus, vaikka ihmisillä on hyvät aikomukset ja selkeä lupa, data-analyysi voi tuoda esiin outoja eettisiä kysymyksiä. Viime aikoina hallitus on esimerkiksi pyytänyt perhelääkäreitä tuottamaan listan ihmisistä, joiden he arvelevat todennäköisesti kuolevan seuraavan vuoden aikana. Sinänsä tämä on hyvä idea: järjestelmään ilmestyy merkki, joka muistuttaa lääkäriä keskustelemaan seuraavassa potilastapaamisessa ”elämän lopun” suunnittelusta. Päivätyössäni käytän paljon aikaa terveysdatan mielenkiintoisten käyttötapojen parissa. Pomoni ehdotti, että voisimme tarkastella potilastietojen automaattista analysointia, jotta voisimme heti tunnistaa pian kuolevat ihmiset. Tämäkin on hyvä idea.

Mutta lisää yksi viimeinen ainesosa, niin johtopäätös ei olekaan niin selvä. Olemme siirtymässä aikaan, joka meidän pitäisi ottaa avosylin vastaan — jolloin potilailla on vihdoin pääsy omiin täydellisin potilastietoihinsa verkossa. Yhtäkkiä meillä on uusi ongelma. Eräänä päivänä kirjaudut potilastietoihisi, ja tiedostossasi on uusi merkintä: ”Todennäköisesti kuolee seuraavan vuoden aikana.” Käytämme paljon aikaa opettamalla lääketieteen opiskelijoita olemaan taitavia kertomaan huonoja uutisia. Potilastietoihisi rastittu ruutu ei ole empaattista viestintää. Piilottaisimmeko laatikon? Onko se eettistä? Vai ovatko ”johdetut muuttujat” kuten nämä, terveysrekisterissä jotain, mitä lääkäreiden pitäisi jakaa kuten mitä tahansa muuta? Tämän suhteen eri ihmisillä on taas erilaisia ajattelutapoja.

Sitten on tieto, jota et tiennyt vuotavasi. Jokaisella Wi-Fi-laitteella on ainutlaatuinen MAC-osoite, jota lähetetään jatkuvasti niin kauan kuin langaton verkko on kytketty päälle. Se on tylsä tekninen seikka WLANin toimintatavassa, etkä oikeasti välittäisi vaikka joku näkisi MAC-osoitteesi radioaalloilla kun kävelet heidän reitittimensä ohi. Mutta jälleen, kysymys ei ole yhden tiedon vuotamisesta, vaan pikemminkin kyvystä yhdistää asiat ketjuksi. Monet kaupat ja kauppakeskukset esimerkiksi käyttävät nyt useita WLAN-antureita, valvovat yhteyksien voimakkuutta, kolmiomittavat sijaintisi ja seuraavat, miten kävelet liikkeessä.

Yhdistämällä signaalin turvavideoon he saavat tietää, miltä näytät. Jos annat sähköpostiosoitteen, jotta voit käyttää ilmaista Wi-Fi-verkkoa, heillä on sekin.

Joissain suhteissa tämä ei eroa online-jälleenmyyjästä, kuten Amazon, joka seuraa liikkumistasi verkkosivuillaan. Erona ehkä on se, että tuntuu karmivammalta tulla seuratuksi, kun kävelee fyysisessä tilassa. Ehkä et välitä. Tai ehkä et tiennyt. Mutta ratkaisevasti: epäilen, että kaikki tuntemasi ihmiset eivät ole samaa mieltä siitä, mikä tässä on oikein tai väärin, saati mikä on ilmiselvää tai yllättävää, karmivaa tai ystävällistä.

On myös mielenkiintoista nähdä, miten ihmisten rajat siirtyvät. Minulle esimerkiksi myymäläseuranta oli OK, mutta ajatteluni muuttui, kun tajusin, että minua jäljitetään paljon laajemmissa tiloissa. Esimerkiksi Turnstyle ulottuu yli koko Toronton — kaupungin, jota rakastan — jäljittäen yksilöitä, kun he siirtyvät kaupungin yhdestä osasta toiseen. Yrityksille tämä on loistavaa tiedustelutietoa: jos lounasaikaan kahvila-asiakkaat käyvät töiden jälkeen myös Whole Foods -kaupassa lähellä kotia, salaatteja kannattaa tarjota enemmän. Yksilön kannalta alankin yhtäkkiä ajatella: voitteko lopettaa seuraamisen, kiitos? Puolet Turnstylen infrastruktuurista on Kanadan ulkopuolella. He tietävät, missä maassa olen. Tämä ylittää oman, henkilökohtaisen karmivuuden kynnykseni. Ehkä luulet, että liioittelen tässä asiaa.

On olemassa erityinen oppikirja, jonka on kirjoittanut Cambridgen yliopiston tietoturvan professori Ross Anderson. Sen nimi on Turvasuunnittelu, ja huolimatta siitä, että se on yli 1 000 sivua pitkä luku-urakka, se on yksi vuosikymmenen luettavimmista populaaritieteellisistä teoksista. Ensinnäkin Anderson esittää turvallisuuden perustotuudet. Voisithan tietenkin tehdä talostasi uskomattoman turvallisen asentamalla vahvistetut metalliset ikkunaluukut jokaisen ikkunan päälle ja 10 lukkoa yhteen vahvistettuun etuoveen; mutta veisi hyvin kauan päästä sisään ja ulos, tai nähdä auringonpaiste aamulla.

Digitaalinen tietoturvan suhteen on sama juttu: me kaikki teemme kompromisseja turvallisuuden ja mukavuuden välillä, mutta vanhanaikaisen fyysisen tilan turvallisuuden ja tämän päivän turvallisuuden välillä on ratkaiseva ero. Voit potkia ovea ja tuntea sen painon. Voit heiluttaa lukkoa ja ihmetellä avaimen yksityiskohtia.Mutta kun kahlaat läpi Andersonin kirjan esimerkit — oppia salasanojen mekaniikasta, yksinkertaisista sähköisistä autotallin ovenavaimista ja sitten pankeista, salauksesta, potilastiedoista ja muusta — sinulle vähitellen valkenee

todellisuus, että tänään lähes kaikki turvallisuutta vaativa on tehty digitaalisesti. Silti suurimmalle osalle meistä tämä koko maailma on läpinäkymätön, kuten sarja mustia laatikoita, joihin uskomme rahamme, yksityisyytemme ja kaiken muun, jonka voimme toivoa olevan turvassa lukittuna. Meillä ei ole selkeää näköyhteyttä tähän maailmaan, ja meillä on vain vähän järkeviä käsityksiä siitä, mikä on turvallista ja mikä hataraa — puhumattakaan siitä, mikä on eettistä ja mikä on pelottavaa. Meille jää sokea, tietämätön, väärä luottamus; sillä välin, kaikkialla ympärillämme, jopa huomaamattamme, tehdään valintoja.