1

Podaci kao nusproizvod računarstva

Računari stalno proizvode podatke. To je njihov ulaz i izlaz, ali je i nusproizvod svega što rade. U normalnom toku rada, kompjuteri kontinuirano dokumentuju ono što rade. Oni osećaju i beleže više nego što ste svesni.

Na primer, program za obradu teksta vodi evidenciju o onome što ste napisali, uključujući nacrte i promene. Kada pritisnete „save", program za obradu teksta snima novu verziju, ali vaš računar ne briše stare verzije sve dok joj ne treba prostor na disku za nešto drugo. Program za obradu teksta automatski čuva dokument sve češće; Microsoft Word čuva moje dokumente svakih 20 minuta. Word takođe vodi evidenciju o tome ko je kreirao dokument, a često i o tome ko je još radio na njemu.

Povežite se sa Internetom i podaci koje proizvodite umnožavaju se: zapisi veb lokacija koje posećujete, oglase koje kliknete, reči koje kucate. Vaš računar, lokacije koje posećujete i računari u mreži proizvode podatke. Pretraživač šalje podatke veb lokacijama o tome koji softver imate, kada je instaliran, koje su vam funkcije omogućene i tako dalje. U mnogim slučajevima, ovi podaci su dovoljni za jedinstvenu identifikaciju vašeg računara.

Sve češće komuniciramo sa porodicom, prijateljima, saradnicima i običnim poznanicima preko računara, koristeći e-poštu, tekstualne poruke, Facebook, Twitter, Instagram, SnapChat, WhatsApp, i sve ostalo što je trenutno aktuelno. Podaci su nusproizvod ove visokotehnološke socijalizacije. Ovi sistemi ne prenose samo podatke; oni takođe kreiraju zapise podataka o vašim interakcijama sa drugima.

Šetajući se napolju, možda ne mislite da proizvodite podatke, ali nije tako. Vaš mobilni telefon konstantno izračunava svoju lokaciju na osnovu najbližeg repetitora. Nije da vaš provajder posebno brine o tome gde se vi nalazite, ali treba da zna gde je vaš mobilni telefon da usmerava telefonske pozive prema vama.

Naravno, ako zaista koristite taj telefon, proizvodite više podataka: birane brojeve i primljene pozive, poslate i primljene tekstualne poruke, trajanje poziva i tako dalje. Ako je to pametni telefon, on je i računar i sve vaše aplikacije proizvode podatke kada ih koristite, a ponekad čak i kada ih ne koristite. Vaš telefon verovatno ima GPS prijemnik, koji daje još preciznije informacije o lokaciji od same lokacije repetitora. GPS prijemnik u vašem pametnom telefonu locira vas na udaljenosti od 5-10 metara a repetitor na oko 700 metara.

Kupite nešto u prodavnici, i stvorićete još podataka. Kasa je kompjuter i stvara zapis o tome šta ste kupili i vreme i datum kada ste ga kupili. Ti podaci ulaze u kompjuterski sistem trgovca. Ako niste platili gotovinom, podaci o vašoj kreditnoj ili debitnoj kartici su vezani za tu kupovinu. Ti podaci se takođe šalju kompaniji za izdavanje kreditnih kartica, a neke od njih dobijate u mesečnom izveštaju.

Može postojati video kamera u prodavnici, instalirana za snimanje dokaza u slučaju krađe ili prevare. Druga kamera vas snima kada koristite bankomat. Napolju je više kamera, nadgledaju zgrade, trotoare, puteve i druge javne prostore.

Uđite u automobil i stvorićete još više podataka. Moderni automobili puni su kompjutera, proizvodeći podatke o vašoj brzini, koliko jako pritiskate pedale, u kom položaju je upravljač, i još mnogo toga. Većina stvari se automatski snima, što je korisno za otkrivanje šta se desilo tokom nesreće. U svakoj gumi postoji čak i kompjuter, koji prikuplja podatke o pritisku. Odvezite svoj automobil kod automehaničara, a prva stvar koju će mehaničar da uradi je da pristupi svim tim podacima da dijagnostikuje bilo kakve probleme. Samovozeći automobil može da stvori gigabajt podataka u sekundi.

Snimite fotografiju i ponovo ste proizveli podatke. Ugrađeni u digitalne fotografije su informacije kao što su datum, vreme i lokacija, da, mnogi foto-aparati beleže GPS lokaciju prilikom fotografisanja; generičke informacije o foto-apartu, objektivu i postavkama; i ID broj foto-aparta. Ako učitate fotografiju na veb, te informacije su često u datoteci.

Nije uvek bilo ovako. U eri štampe, radija i televizije, dobili smo informacije, ali nisu se beležili dodatni podaci o događaju. Sada primamo vesti i zabavu preko interneta. Govorili smo sa ljudima licem u lice, a zatim telefonom; sada razgovaramo preko teksta ili e-pošte. Kupovali smo stvari za gotovinu u prodavnici; sada koristimo kreditne kartice. Mi smo plaćali kovanicama na naplatnoj stanici, u metrou, ili parking satu. Sada koristimo automatske platne sisteme, koji su povezani sa registarskim brojem automobila i kreditnom karticom. Taksi se plaćao samo gotovinom. Onda smo počeli da plaćamo kreditnom karticom. Sada koristimo pametne telefone za pristup umreženim taksi sistemima kao što su Uber, Lift, Car:Go, koji evidentiraju transakcije, plus lokacije našeg ulaska i izlaska iz taksija. Uz nekoliko izuzetaka, kompjuteri su sada svuda gde se bavimo trgovinom, i na većini mesta gde izlazimo sa prijateljima.

Prošle godine, kada se mi se frižider pokvario, majstor je zamenio kompjuter koji ga kontroliše. Shvatio sam da sam

razmišljao o frižideru: to nije frižider sa kompjuterom, to je računar koji hladi hranu. Samo tako, sve se pretvara u kompjuter. Vaš telefon je računar koji poziva. Vaš automobil je kompjuter sa točkovima i motorom. Vaša pećnica je kompjuter koji peče lazanje. Foto-aparat je računar koji snima slike. Čak su i naši kućni ljubimci redovno čipovani; moja mačka je praktično kompjuter koji spava na suncu ceo dan.

Računari se ugrađuju u sve više i više vrsta proizvoda koji se povezuju na Internet. Kompanija pod imenom Nest, koju je Google kupio u 2014. za više od 3 milijarde dolara, proizvodi termostat koji podržava Internet. Pametni termostat se prilagođava vašim obrascima ponašanja i odgovara na ono što se dešava na električnoj mreži. Ali da bi sve to uradio, on beleži više od vaše potrošnje energije: takođe prati i beleži temperaturu, vlažnost, svetlost vašeg doma i bilo koji pokret u blizini. Možete da kupite pametan frižider koji prati datume isteka hrane, i pametni klima uređaj koji može da nauči vaše želje i poboljša energetsku efikasnost. Ali to nije sve: Nest sada prodaje pametni detektor dima i ugljen-monoksida i planira čitavu liniju dodatnih kućnih senzora. Mnoge druge kompanije rade na širokom spektru pametnih uređaja. Sve ovo će biti neophodno ako želimo da izgradimo pametnu električnu mrežu, koja će da smanji potrošnju energije i efekat staklene bašte.

Počinjemo da prikupljamo i analiziramo podatke o našem telu radi poboljšanja našeg zdravlja i dobrobiti. Ako nosite uređaj za praćenje kondicije kao što je Fitbit ili Javbone, on prikuplja informacije o vašim pokretima u budnom stanju i za vreme sna i koristi ih za analizu vaših navika vežbanja i spavanja. Može da odredi kada imaš seksualne odnose. Dajte uređaju više informacija o sebi, koliko ste teški, šta jedete, i možete da saznate još više. Naravno, svi ovi podaci koje delite nalaze se i na mreži.

Mnogi medicinski uređaji počinju da koriste Internet, prikupljaju i izveštavaju o različitim biometrijskim podacima.

Već postoje uređaji koji neprestano mere naše vitalne tačke, raspoloženje i aktivnost našeg mozga. To nisu samo specijalizovani uređaji; trenutni pametni telefoni imaju prilično osetljive senzore pokreta. Kako cena sekvenciranja DNK nastavlja da opada, sve više nas se prijavljuje da generišemo i analiziramo naše sopstvene genetske podatke. Kompanije kao što je 23andMe se nadaju da će koristiti genomske podatke svojih klijenata kako bi pronašli gene povezane s bolešću, što dovodi do novih i visoko profitabilnih terapija. Oni takođe pričaju o personalizovanom marketingu, a osiguravajuće kompanije će jednog dana moći da kupe njihove podatke radi donošenja poslovnih odluka.

Možda je ekstremno u trendu samogenerisanje ličnih podataka. Već možete da instalirate aplikacije koje će zabeležiti vaše aktivnosti na pametnom telefonu, kao što su razgovori sa prijateljima, igranje igara, gledanje filmova i tako dalje. Ali to je samo bleda senka onoga šta će postati beleženje životnih podataka. Ubuduće će sadržati video zapis. Google Glass je prvi nosivi uređaj koji ima ovaj potencijal, ali ni drugi ne zaostaju.

Ovo su primeri interneta stvari. Ekološki senzori će detektovati nivoe zagađenja. Pametni sistemi inventara i kontrole će smanjiti otpad i uštedeti novac. Računari povezani sa Internetom će biti u svemu: pametni gradovi, pametne četkice za zube, pametne sijalice, pametni pločnici, pametne flašice za pilule, pametna odeća, zašto da ne? Procene su da trenutno postoji 10 milijardi uređaja povezanih na Internet. To je već više od broja ljudi na planeti, video sam predviđanja da će ona doseći 30 milijardi do 2020. godine. Ono što znamo je da će svi da generišu podatke, puno podataka. Stvari oko nas postaće oči i uši Interneta.

Implikacije privatnosti svih ovih veza su duboke. Svi ti pametni uređaji će smanjiti emisiju gasova sa efektom staklene bašte, i takođe će da prenose podatke o tome kako se ljudi kreću unutar svojih kuća i kako provode vreme.

3

Analiziranje naših podataka

Godine 2012, *New York Times* je objavio priču o tome kako korporacije analiziraju naše podatke za potrebe oglašavanja. U članku je otkriveno da korporacija Target može da utvrdi način na koji žene kupuju za vreme svoje trudnoće i da koristi te informacije da bi trudnicama slale oglase i kupone za proizvode u vezi beba. U članku je bila i anegdotu o čoveku iz Minneapolisa koji se požalio korporaciji zato što je slala kupone u vezi beba njegovoj kćerki tinejdžerki, da bi kasnije čovek otkrio da je korporacija bila u pravu.

Opšta praksa prikupljanja i čuvanja svih vrsta podataka naziva se „veliki podaci" (engl. *big data*), a naučni postupak i inženjering izdvajanja korisnih informacija iz nje nazivaju se „rudarenje podataka" (engl. *data mining*). Kompanije rudare po svojim podacima da bi forukisrale svoje reklamne kampanje. Barak Obama se iz istog razloga bavio rudarenjem podataka za potrebe svojih predsedničkih kampanja za 2008. i 2012. godinu. Auto kompanije rudare podatke iz vašeg automobila kako bi dizajniralie bolje automobile; opštine prikupljaju i rudare po podacima od senzora na putevima kako bi razumelie uslove vožnje. Naši genetski podaci su izrudareni

za razne vrste medicinskih istraživanja. Kompanije kao što su Facebook i Twitter rudare po našim podacima u reklamne svrhe i omogućavaju akademskim ustanovama da ih koriste za istraživanje društva.

Većina rudarenja je zapravo sekundarna upotreba podataka. To jest, to nije razlog zbog kog su podaci prikupljeni. U stvari, to je osnovna vrednost velikih podataka: sačuvajte sve što možete i jednog dana ćete imate neku korist od svega toga.

Veliki skupovi podataka imaju vrednost, delom iz zaključaka koji mogu da se izvedu od njih. Neki od njih su očigledni. Ako imate podatke o nečijem detaljnom kretanju tokom godine, možete da zaključite koji su njegovi omiljeni restorani. Ako imate spisak ljudi koje poziva i kojima šalje e-poštu, možete da zaključite ko su njegovi prijatelji. Ako imate spisak internet stranica koje posećuje, ili možda spisak knjiga koje je kupio, možete da zaključite kakvi su njegovi interesi.

Neki zaključci su suptilniji. Spisak kupljenih namirnica neke osobe može ukazati na njenu etničku pripadnost. Ili starost i pol, i verovatno religisko opredeljenje. Ili medicinsku istoriju i sklonost ka alkoholu. Ljudi u marketingu su stalno u potrezi za obrascima koji ukazuju da će neko napraviti veći trošak, kao što je venčanje, odlazak na odmor, kupovina kuće, rođenje deteta i tako dalje. Policija u raznim zemljama koristi ove obrasce kao dokaze, bilo na sudu ili u tajnosti. Facebook može da proceni nečiju rasu, ličnost, seksualnu orijentaciju, političku ideologiju, stanje veze sa partnerom i upotrebu droga samo na osnovu pritska na Like dugme. Kompanija zna da ćete da se verite pre nego što ste to objavili, ili da je neko homeskusualac i pre nego što okolina sazna, a njegove poruke mogu to da otkriju drugim ljudima bez njegovog znanja ili dozvole. U zavisnosti od zemlje u kojoj živi, to bi mogla da bude sramota ili gubitak glave.

Postoji mnogo grešaka u zaključivanjima, a to svi mi koji smo videli internet oglase koji su nam slabo zanimljivi, možemo da potvrdimo. Ali kada su oglasi pogodili šta nas

intresuje, mogu da budu jezivi i često nam se ne sviđaju. Jedna je stvar kada vidite na televiziji oglase za čepiće za hemoroida ili oglas za agenciju za bračno posredovanje, gde znamo da svi vide te oglase. Ali kada znamo da su oglasi posebno ciljani na nas, na osnovu onoga što smo objavili ili označavali sa Like na internetu, tada oglašavanje može da bude mnogo invazivnije. Ovo nam stvara protivrečnu situaciju: podaci koje smo spremni da delimo mogu da nas dovedu do zaključka da ne želimo da ih delimo. Mnoge žene sa zadovoljstvom kažu šta ih interesuje da kupe na popustu i žele da budu obaveštavane o novim proizvodima koje bi možda želele da kupe, ali većina njih ne želi da kompanija shvati da su trudne. Takođe ne želimo velike krađe podataka i prevare koje neizbežno prate ove velike baze podataka.

Kada pomislimo na računare koji koriste sve naše podatke da bi napravili zaključke, mi imamo veoma humani način razmišljanja o tome. Zamišljamo kako bismo podacima dali smisao i preneli takav proces na kompjutere. Ali to nije tako. Računari i ljudi imaju različite snage, slabosti i ograničenja. Računari ne mogu apstraktno da razmišljaju kao ljudi, ali mogu da obrade ogromne količine podataka sve brže i brže. (Ako razmišljate o tome, to znači da su računari bolji u radu sa metapodacima nego što su u obradi snimljenih razgovora) Računari se stalno poboljšavaju. Računarska snaga se još uvek udvostručuje svakih osamnaest meseci, dok je veličina mozga naše vrste i dalje ista. Računari su već daleko bolji od ljudi pri obradi kvantitativnih podataka i nastaviće da se poboljšavaju.

Upravo sada, rudarenje podataka je akutelna tehnologija, a oko nje je mnogo oduševljenja i oportunizma. Još nije sasvim jasno koje će vrste istraživanja da budu moguće, ili koji je pravi potencijal svega toga. Ono što je jasno je da tehnologija rudarenja podataka postaje sve moćnija i omogućava posmatračima da izvuku sve više iznenađujućih zaključaka iz velikih skupova podataka.

10
Privatnost

Najčešća zabluda o privatnosti je ta da je u pitanju nešto što bi trebalo da se sakrije. „Ako ne radite bilo šta loše, onda nemate šta da krijete“, kaže izreka, sa očiglednom implikacijom da je privatnost potrebna samo zločincima.

Ako malo razmislite, to nema smisla. Ne radimo ništa loše kada vodimo ljubav, odlazimo u kupatilo ili pevamo pod tušem. Ne radimo ništa pogrešno kada tražimo posao a da to ne kažemo našem trenutnom poslodavcu. Ne radimo ništa pogrešno kada tražimo skrovita mesta za razmišljanje ili razgovor, kada odlučimo da ne razgovaramo o nečem emocionalnom ili ličnom, kada koristimo koverte za poštu ili kada se poveravamo prijatelju i nikome drugom.

Štaviše, čak i oni koji to tvrde ne veruju u privatnost. U intervjuu iz 2009. godine, direktor Googla Eric Schmidt je to izrekao ovako: „Ako postoji nešto za šta ne želite da iko sazna, možda to uopšte ne bi trebalo da radite.“ Ali 2005. godine, Schmidt je zabranio zaposlenima da razgovaraju sa novinarima sa CNET-a, jer je reporter u jednom članku otkrio lične detalje o Schmidtu. Mark Zuckerberg osnivač Facebooka izjavio je 2010. godine da privatnost više nije „društvena norma“,

ali je kupio četiri kuće za svoj dom u Palo Altu kako bi osigurao sopstvenu privatnost.

Postoje neke tajne koje otkrijemo *samo nekome* i verujemo da će ostati sakrivene iako smo ih otkrili toj osobi. Ljubavnicima i prijateljima pišemo intimna pisma, razgovaramo sa lekarima o stvarima koje ne bismo nikome rekli, i govorimo stvari na poslovnim sastancima koje ne bismo govorili u javnosti. Koristimo pseudonime da odvojimo naše privatno ja od javnog, ili da bismo isprobali nešto novo.

Izvršni direktor Facebooka Mark Zuckerberg pokazao je izvanrednu naivnost kada je izjavio: „Imate jedan identitet. Dani kada imate jednu sliku za svoje kolege ili saradnike a drugu sliku za ostale ljude koje poznajete, verovatno se brzo privode kraju. Imati dva identiteta za sebe je primer nedostatka integriteta. "

Nismo isti za sve koje znamo i upoznamo. Ponašamo se drugačije kada smo sa porodicom, prijateljima, kolegama i tako dalje. Imamo različite manire kod kuće i u restoranu. Deci pričamo drugačije priče nego što pričamo našim prijateljima sa kojima pijemo. Nije nužno da lažemo, mada ponekad i to činimo. Činjenica je da mi otkrivamo različite aspekte naše ličnosti različitim ljudima. To je nešto što je ljudsko. Privatnost je ono što nam omogućava da postupamo na odgovarajući način u bilo kom okruženju u kom se nađemo. U privatnosti naše kuće ili spavaće sobe možemo da se opustimo na način koji ne možemo kada je neko drugi u blizini.

Privatnost je inherentno ljudsko pravo i uslov da se ljudsko stanje održava dostojanstveno i poštovano. Reč je o izboru i moći da upravljate s tim kako se predstavljate svetu. Internet etnograf danah boyd kaže ovako: „Privatnost ne samo da zavisi od agencije, nego biti u mogućnosti ostvarivanja privatnosti je odraz same agencije. "

Kad izgubimo privatnost, gubimo i kontrolu nad tim kako se predstavljamo. Gubimo kontrolu kada nešto što kažemo na

jednoj grupi Facebooka, slučajno bude podeljeno na drugoj grupi, a potpuno gubimo kontrolu kada vlada prikupi naše podatke. „Kako je on to saznao?“ pitamo se. Kako sam izgubio kontrolu nad onim ko sme da zna o mom traumatičnom detinjstvu, sklonosti ka lošem humoru ili o odmoru u Dominikanskoj republici? Možda znate taj osećaj: osetili ste ga kada vas je sopstvena majka označila za prijatelja na Facebooku ili na bilo kom drugom mestu društvenog umrežavanja na kojoj ste nekada bili samo vi i vaši prijatelji. Kršenje privatnosti je invazija.

Postoji snažna psihološka osnova privatnosti. Biolog Peter Watts ističe da je želja za privatnošću urođena: sisari, posebno, ne reaguju dobro na nadzor. Smatramo to fizičkom pretnjom, jer su životinje u prirodi pod prismotrom predatora. Zbog nadzora se osećamo kao plen, baš kao što one koje nas nadgledaju smatramo predatorima.

Psiholozi, sociolozi, filozofi, romanopisci i tehnolozi, svi su pisali o efektima stalnog nadzora, ili čak samo percepcije stalnog nadzora. Studije pokazuju da smo manje zdravi i fizički i emocionalno. Imamo osećaj niskog samopoštovanja, depresije i anksioznosti. Nadzor nam oduzima dostojanstvo. On preti našoj ličnosti kao pojedincima. To je dehumanizujuća taktika koja se koristi u zatvorima i logorima širom sveta.

Nisu sve povrede privatnosti jednake. Kontekst je bitan. Postoji razlika između službenika Uprave za bezbednost saobraćaja (*Transportation Security Administration, TSA*) koji pronalazi pornografiju u vašem koferu ili ako je pronalazi vaš supružnik. Postoji razlika između policije koja sazna o vašoj upotrebi droge ili ako saznaju vaši prijatelji. Povrede privatnosti nisu sve jednako štetne. Neki od nas u marginalnim socioekonomskim situacijama, marginalizovanim rasnim, političkim, etničkim i verskim grupama, više su pogođeni. Neki od nas na visokim položajima od kojih javnost ima visoka očekivanja, još su više pogođeni. Životi nekih od nas zavise od privatnosti.

Naša privatnost je pod stalnim nadzorom. Razumevanje kako se to dešava je presudno za razumevanje onoga šta je u pitanju.

KRATKOROČNOST

Kroz veći deo istorije naše interakcije i razgovori bili su kratkoročni. To je način na koji mi prirodno razmišljamo o razgovoru. Izuzeci su bili dovoljno retki da se primete: sačuvani dnevnik, stenograf koji zapisuje postupak u sudnici, snimljeni govor političkog kandidata.

Ovo se promenilo. Kompanije imaju sve manje sastanaka licem u lice. Prijatelji se druže na mreži. Moja supruga i ja vodimo intimne razgovore putem SMS poruka. Svi se ponašamo kao da su ti razgovori kratkoživeći, ali nisu. Sačuvani su na način nad kojim mi nemamo kontrolu.

Teško je da se izbrišu razgovori koji su snimljeni. Oliver North je to shvatio još davne 1987. godine, kada se ispostavilo da su poruke za koje je mislio da ih je izbrisao sačuvao sistem PROFS Notes Bele kuće, pređašnji oblik e-pošte. Bill Gates je ovo shvatio deceniju kasnije, kada su njegovi razgovori putem e-pošte, dostavljeni tužiocu u antitrustovskom postpuku protiv Microsofta. Preko 100 žena koje su poznate ličnosti shvatilo je to 2014. godine, kada su njihove intimne fotografije, neke koji su navodno bile izbrisane, ukradene sa njihovih iCloud naloga i kada su deljene šire i dalje nego što su one ikada nameravale.

Sve je teže i teže biti kratkoročan. Govorni razgovor je uglavnom još uvek nezabeležen, ali koliko će to da traje? Sistemi za nadzor maloprodajnih objekata registruju naše prisustvo, čak i ako ne radimo ništa osim gledanja i čak ako sve plaćamo u gotovini. Neki barovi beleže lične podatke svih koji uđu. Ne mogu gotovinom više da platim ni čašu vina u avionu. Sveprožimajuće snimanje naših života ovo će još više da pogorša.

Pisac naučne fantastike Charles Stross opisao je to kao kraj praistorije. Nećemo ništa da zaboravimo, jer ćemo uvek biti u mogućnosti da ga vratimo iz memorije nekog računara. Ovo je novina za našu vrstu i biće blagodat kako budućim istoričarima, takođe i onima koji su u sadašnjosti a žele valjane podatke za samoprocenu i promišljanje.

Pošto smo sve snimili i trajno stavili na raspolaganje, promeniće nas i pojedinačno i kao društvo. Naša percepcija i sećanja nisu ni približno tako oštri kao što mislimo da jesu. Ne primećujemo neke stvari, čak i važne stvari. Mi pogrešno pamtimo, čak i stvari za koje smo sigurni da ih se tačno sećamo. Zaboravljamo važne stvari za koje smo bili sigurni da nikada nećemo da ih zaboravimo. To znaju ljudi koji vode dnevnike. Stare unose mogu da čitaju kao da ih je pisao neko drugi. Već sam primetio, pošto imam svoju e-poštu unazad dve decenije, kako se razlikuje moj način razmišljanja o sopstvenoj prošlosti.

Jedna četvrtina odraslih Amerikanaca ima kriminalni dosije. Čak i manja kršenja zakona mogu zauvek da prate ljude i imaju ogroman uticaj na njihov život. To je razlog zašto mnoge vlade imaju postupak za brisanje krivičnih dosijea pošto protekne neko vreme. Izgubiti kratkoročnost znači da će sve što kažete i uradite zauvek da bude povezano s vama.

Voditi razgovore koji nestaju čim se obave je društvena norma koja nam omogućava da budemo opušteniji i ugodniji i da kažemo stvari koje možda ne bismo rekli da nas je snimao magnetofon. Dugoročno, zaboravljanje i delimično zaboravljanje je način kako obrađujemo našu istoriju. Zaborav je važan faktor praštanja. Individualno i društveno pamćenje bledi, a rane iz prošlosti manje bole. Ovo nam pomaže da oprostimo nepravde iz prošlosti. Nisam ubeđen da će se moj brak poboljšati otkrivanjem zapisa starih prepirki. Gubitak kratkoročnosti biće ogromna društvena i psihološka promena, za koju mislim da naše društvo nije pripremljeno.

12
Principi

Šteta od masovnog nadzora ima mnogo, a cena za pojedince i društvo u celini neproporcionalno prevazilazi korist. Mi možemo i moramo da učinimo nešto da to ispravimo. Pre konkretnih pravnih, tehničkih i socijalnih predloga želim da započnem ovo poglavlje sa određenim opštim principima. To su univerzalne istine o nadzoru i kako bi trebalo da se nosimo sa njim a odnosi se i na vladu i na korporacije.

Artikulisanje tih principa je lakši deo. Mnogo je teže primeniti ih u određenim okolnostima. „Život, sloboda i traganje za srećom“ su principi sa kojima se svi slažemo, ali trebalo bi samo da pogledamoi Vašington DC, da bismo videli koliko ih je teško primeniti. Bio sam na mnogim panelima i rasprava-ma na kojima se ljudi sa svih strana slažu oko opštih principa o prikupljanju podataka, nadzoru, nadgledanju, bezbednosti i privatnosti, ali se značajno ne slažu kako da se ti principi primene u stvarnom svetu.

BEZBEDNOST I PRIVATNOST

Debata se često karakteriše kao „bezbednost nasuprot privatnosti." Ovaj pojednostavljeni pogled zahteva od nas da napravimo neku vrstu temeljnog kompromisa između ta dva: da bismo postali bezbedni, moramo da žrtvujemo svoju privatnost i da se podvrgnemo nadzoru. Ako želimo da steknemo određen nivo privatnosti, moramo da prihvatimo da žrtvujemo deo bezbednosti.

To je lažni kompromis. Prvo, neke mere bezbednosti zahtevaju da se ljudi odreknu privatnosti, ali druge mere uopšte ne utiču na privatnost: brave na vratima, visoke ograde, čuvari, ojačana vrata u kokpitu u avionima. I drugo, privatnost i bezbednost su u osnovi usklađeni. Kad nemamo privatnost, osećamo se izloženi i ranjivi; osećamo se manje bezbedno. Slično tome, ako naši lični prostori i zapisi nisu bezbedni, imamo manje privatnosti. Četvrti amandman Ustava SAD govori o „pravu ljudi da budu sigurni u sebe, kuće, papire i efekte". Autori amadmana su prepoznali da je privatnost od ključne važnosti za bezbednost pojedinca.

Uokviravanje razgovora (engl. *framing the conversation*) kao razmena bezbednosti za privatnosti vodi do pogrešnih procena. Kompromis se često nudi u vidu novčanih troškova: „Koliko biste platili za privatnost?" Ili „Koliko biste platili za bezbednost?", Ali to su takođe pogrešno postavljeni kompromisi. Troškovi nebezbednosti su stvarni i jasni, čak i apstraktno. Troškovi gubitka privatnosti su apstraktno nejasni i postaju opipljivi tek kada se neko suoči sa njihovim posledicama. Zbog toga potcenjujemo privatnost kada je imamo, a njenu pravu vrednost prepoznajemo samo kada je nemamo. To je razlog zašto često čujemo da niko ne želi da plati privatnost i da stoga bezbednost apsolutno zasenjuje privatnost.

Kada se dilema bezbednost naspram privatnosti postavi kao izbor između života ili smrti, sva razumna rasprava

prestaje. Kako bilo ko može da govori o privatnosti kada su životi u pitanju? Ljudi koji su uplašeni spremnije će žrtvovati privatnost da bi se osećali bezbednije. Ovo objašnjava zašto je američkoj vladi posle 11. septembra data tako slobodna podrška za sprovođenje masovnog nadzora. Vlada je u osnovi rekla da svi moramo da se odreknemo privatnosti u zamenu za bezbednost. Većina nas nije znala za bolje i zato je prihvatila faustovsku pogodbu.

Problem je što je celokupna težina nebezbednosti porediva sa inkrementalnim upadom u privatnost. Američki sudovi to rade uveliko, govoreći po sledećem redosledu: „Slažemo se da ovaj ili onaj vladin program dovedi do gubitka privatnosti, ali rizik od nuklearne bombe u Njujorku je jednostavno prevelik." To je trapava karakteristika kompromisa. Ne radi se o tome da je nuklearna detonacija nemoguća ako se vrši nadzor, ni da je neizbežna ako ne vršimo. Verovatnoća je već vrlo mala, a bezbednosni program koji ugrožava našu privatnost mogao bi taj broj samo vrlo malo da smanji. To je kompromis koji bi trebalo razmotriti.

Generalno, ne bi trebalo da naš cilj bude pronalaženje prihvatljivog kompromisa između bezbednosti i privatnosti, jer možemo i trebalo bi da zadržimo zajedno i jedno i drugo.

BEZBEDNOST PRE NADZORA

Bezbednost i nadzor su oprečni dizajnerski zahtevi. Sistem koji je izgrađen za bezbednost je teže nadgledati. Suprotno tome, sistem izgrađen za lako nadgledanje teže je učiniti bezbednim. Ugrađena mogućnost nadzora u sistemu je nebezbedan, jer ne znamo kako da napravimo sistem koji dozvoljava nadzor samo *ispravnoj* vrsti ljudi. To smo videli u 11. poglavlju.

Moramo da prepoznamo da je za društvo u celini bezbednost kritičnija od nadzora. Odnosno, moramo da odaberemo bezbednu informacionu infrastrukturu koja onemogućava

nadzor, a ne nebezbednu infrastrukturu koja omogućava lak nadzor.

Obrazloženje se primenjuje generalno. Naša infrastruktura može da se koristi i u dobre i u loše svrhe. Pljačkaši banaka voze se autoputevima, koriste struju, kupuju u prodavnicama hardvera i jedu u noćnim restoranima, baš kao i pošteni ljudi. I nevini i zločinci podjednako koriste mobilne telefone, e-poštu i Dropbox. Kiša pada na pravedne i nepravedne.

Uprkos tome, društvo nastavlja da funkcioniše, jer poštena, pozitivna i korisna upotreba naše infrastrukture daleko prevazilazi nepoštenu, negativnu i štetnu. Procenat vozača na našim auto putevima koji su pljačkaši banaka je zanemariv, kao i procenat korisnika elektronske pošte koji su kriminalci. Ima mnogo više smisla dizajnirati sve ove sisteme za većinu nas kojima je potrebna bezbednost od kriminalaca, telemarketara, a ponekad i sopstvenih vlada.

Davanjem prioriteta bezbednosti, zaštitili bismo svetske tokove informacija, uključujući i naš, od prisluškivanja kao i od raznih štetnih napada kao što su krađe i nanošenje štete. Zaštitili bismo naše tokove informacija od vlada, nedržavnih aktera i kriminalaca. Svet bismo učinili bezbednijim.

Tor je odličan primer. To je besplatni softver otvorenog koda koji možete koristiti da anonimno krstarite Internetom. Početno je razvijen uz finansiranje Američke laboratorije za istraživanje pomorstva (*US Naval Research Laboratory*), a potom uz pomoć Stejt departmenta. Koriste ga disidenti širom sveta da bi izbegli nadzor i cenzuru. Naravno, koriste ga i kriminalci u iste svrhe. Torovi programeri stalno ažuriraju program kako bi izbegli pokušaje kineske vlade da ga onemogući. Znamo da NSA neprekidno pokušava da provali u njega, i po dokumentu NSA iz 2007. godine koji je objavio Snouden, nije uspela. Znamo da je FBI hakovao računare 2013. i 2014. jer nisu mogli da provale u Tor. Istovremeno, verujemo da pojedinci koji rade i u NSA i u GCHK-u anonimno pomažu u očuvanju Tora. Ali tu je

nezgodacija: Tor je ili dovoljno jak da zaštiti anonimnost i onih koji nam se sviđaju i onih koji nam se ne sviđaju, ili nije dovoljno jak da zaštiti anonimnost ni jednog od njih.

Naravno, nikad neće postojati budućnost u kojoj niko ne špijunira. To je naivno. Od početka istorije vlade su uvek špijunirale; postoji čak nekoliko špijunskih priča u Starom zavetu. Pitanje je u kakav svet mi želimo da krenemo. Da li želimo da smanjimo neravnotežu moći ograničavanjem vladinih sposobnosti da nadgledaju, cenzurišu i kontrolišu? Ili da dopustimo vladama da imaju sve veću moć nad nama?

„Bezbednost nad nadzorom", naravno nije apsolutno pravilo. Postoje slučajevi kada je neophodno osmisliti sisteme zaštite od manjine nas koji smo nepošteni. Bezbednos aviona je primer toga. Broj terorista koji lete avionima je zanemarljiv u poređenju sa brojem neterorista, ali mi oblikujemo čitave aerodrome zbog tih nekoliko, jer propust u bezbednosti aviona je smrtonosniji od terorističke bombe bilo gde drugde postavljenje. Ipak (mi) ne dizajniramo čitavo naše društvo za prevenciju terorizma.

Postoje i slučajevi kada moramo da dizajniramo odgovarajući nadzor u sistemima. Želimo da službe transporta mogu da prate pakete u realnom vremenu. Želimo da znamo odakle dolazi hitni poziv sa mobilnog telefona. U tim slučajevima, naravno, ne koristimo reč „nadzor"; koristimo neki manje emocionalno opterećen termin kao što je „praćenje paketa".

Ovde je opšti princip da bi trebalo da sistemi budu dizajnirani sa minimalnim nadzorom potrebnim za rad, a tamo gde je nadzor potreban trebalo bi da prikupe minimalnu potrebnu količinu informacija i čuvaju je za najkraće moguće vreme.

TRANSPARENTNOST

Transparentnost je od vitalnog značaja za svako otvoreno i slobodno društvo. Otvoreni vladini zakoni i zakoni o slobodi informisanja omogućavaju građanima da znaju o čemu se