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