

داده و قدرت

جنگ‌های پنهانی برای جمع‌آوری داده‌ها

و کنترل جهان شما

نویسنده: بروس اسنر

مترجم: مهندس کمال کمایی

مدرس دانشگاه و متخصص امنیت سایبری از دانشگاه تهران



سرشناسه: اشنایر، بروس، ۱۹۶۴ - م.
Schneier, Bruce
عنوان و نام پدید آور: داده و قدرت: جنگ‌های پنهانی برای جمع‌آوری داده‌ها و کنترل جهان شما / نویسنده بروس اشنایر؛
مترجم: کمال کمایی.
مشخصات نشر: اهواز: پژوهندگان راه دانش، ۱۳۹۶.
مشخصات ظاهری: ۲۷۹ ص.

وضعیت فهرست نویسی: فیا

Electronic surveillance – Social aspects: موضوع:

Information technology – Social aspects: موضوع:

Computer security: موضوع:

Privacy, Right of: موضوع:

Social control: موضوع:

Data and Goliath: the hidden battles to collect your data and control your world, [2015] عنوان اصلی

شماره افزوده: کمایی، کمال، ۱۳۵۳ -، مترجم

شماره کتابشناسی ملی: ۴۸۲۸۰۲۶

رده بندی دیویی: ۰۰۵/۸

رده کنگر: ۱۳۹۶ ۵۲۵الف/HMA۴۶

اشارات پژوهندگان راه دانش



ناشر: پژوهندگان راه دانش

شماره نشر: ۱۲۰۷

نام کتاب: داده و قدرت (جنگ‌های پنهانی برای جمع‌آوری داده‌ها و کنترل جهان شما)

نویسنده: بروس اشنایر

مترجم: مهندس کمال کمایی

تیراژ: ۱۰۰۰

نوبت چاپ: اول ۱۳۹۶

چاپ: ترنگ

صفحه آرای: پژوهندگان

سایز: وزیری

شابک: ۹۷۸-۶۰۰-۳۴۵-۲۰۴-۶

قیمت: ۲۴۰۰۰ تومان

www.ketab.ir/pajo

حق چاپ و نشر محفوظ است.

طبق قانون حقوق نویسندگان و مصنفان هرگونه کپی برداری به هر روش پیگرد قانونی دارد.

۰۹۱۲۸۸۸۴۹۶۹ - ۶۶۱۲۰۵۵۴

تهران: خیابان ۱۶ آذر شمالی، ساختمان بعثت، طبقه سوم

۰۹۱۶۱۱۸۵۱۱۸ - ۳۲۲۰۲۸۰۲ - ۳۲۲۱۹۲۰۲

اهواز: خیابان نادری شرقی، نبش خیابان گرمی خراط

فهرست

مقدمه.....	۵
بخش اول: دنیایی که خلق می‌کنیم.....	۱۵
فصل ۱: داده به مثابه محصول جانبی پردازش.....	۱۷
فصل ۲: داده برای نظارت.....	۲۵
فصل ۳: تریه و تحلیل داده‌هایمان.....	۴۱
فصل ۴: کسب و کار حاصل از نظارت.....	۵۷
فصل ۵: نظارت و کنترل در.....	۷۱
فصل ۶: تثبیت کنترل سازمان.....	۹۱
بخش دوم: چه چیزی در خطر است.....	۱۰۳
فصل ۷: آزادی سیاسی و عدالت.....	۱۰۵
فصل ۸: برابری و انصاف تجاری.....	۱۲۵
فصل ۹: رقابت تجاری.....	۱۳۹
فصل ۱۰: حریم خصوصی.....	۱۴۵
فصل ۱۱: امنیت.....	۱۵۵
بخش سوم: چه باید بکنیم.....	۱۷۷
فصل ۱۲: اصول.....	۱۷۹
فصل ۱۳: راه‌حلی برای دولت.....	۱۹۳
فصل ۱۴: راه‌حلی برای شرکت‌های بزرگ.....	۲۲۱
فصل ۱۵: راه‌حل‌ها برای بقیه ما.....	۲۴۹
فصل ۱۶: هنجارهای اجتماعی و بده بستان‌های کلان داده.....	۲۶۵

مقدمه

اگر می‌خواهید واقعاً باور کنید که در یک جهان علمی - تخیلی زندگی می‌کنید، کافیت نگاهی به تلفن همراه خود بیندازید. این ابزار جذاب، پر زرق و برق و فوق‌العاده قدرتمند آن چنان در زندگی ما رسوخ کرده که آن را امر بدیهی و مسلم و جز لاینفک زندگی برمی‌شماریم. دیگر کاملاً عادی شده که تلفن همراه را از جیب خود در بیاوریم و بدون در نظر گرفتن اینکه در کجای این کره خاکی قرار گرفته‌ایم با شخص دیگری تماس برقرار کنیم و اصلاً هم اهمیتی ندارد که آن شخص در کجای این ساره اسوده است.

با این حال هر روز صبح وقتی تلفن همراه را از جیب خود درمی‌آوریم دست به یک معامله ضمنی (پنهانی) با شرکت مخابرات می‌زنیم: "می‌خواهم تماس تلفنی برقرار کنم؛ و در عوض آن به شرکت مخابرات اجاره می‌دهم." در تمام اوقات از موقعیت مکانی من مطلع باشد. در واقع این معامله یک قرارداد نانوشته است اما این نوع معامله در ذات چنین خدماتی قرار دارد. شاید درباره آن فکر نکرده بودید، اما اکنون که به آن اشاره کردم شاید به درستی تصور کنید که این چه معامله خوبیست. تلفن‌های همراه واقعاً عالی و معجزه هستند، این تلفن‌ها کار نمی‌کنند مگر آنکه در ابتدا شرکت مخابرات بداند کجا هستند و تا زمانی که شرکت مخابرات مکان دقیق آن‌ها را نداند هیچ مکالمه‌ای برقرار نمی‌گردد، که این بدین معناست که شرکت‌های مخابرات دائماً شما را تحت کنترل دارند و شما را می‌پایند.

این شکل خیلی نزدیک و دقیقی از نظارت بشمار می‌آید: تا زمانی که همراه شما محل زندگی و محل کارتان را مشخص و ردیابی می‌کند، حتی پیگیری می‌کند که چه قدر تعطیلات آخر هفته را کجا سپری کنید و نیز مشخص می‌سازد چه موقع به کلیسا می‌روید (و یا کاه کلیسا)، چه مدت در یک بار می‌مانید و در هنگام رانندگی با چه سرعتی می‌رانید. تلفن همراه می‌داند که روزهای خود را با چه کسانی سپری می‌کنید، با چه کسانی برای نهار قرار ملاقات دارید و یا با چه کسی هم‌بستر می‌شوید (چرا که تلفن‌های همراه همه‌ی گوشی‌های حوزه جغرافیایی شما را ردیابی می‌کند).

داده‌های جمع‌آوری شده احتمالاً می‌توانند یک تصویر بهتر از چگونگی گذران زمان شما را نسبت به آنچه انجام می‌دهید ترسیم کنند زیرا بر پایه حافظه انسانی استوار نیست. در سال ۲۰۱۲ پژوهشگران توانستند در پیش‌بینی اینکه افراد در ۲۴ ساعت آینده در محدوده ۲۰ متری در چه جایی خواهند بود، استفاده کنند.

قبل از تلفن همراه اگر کسی می‌خواست تمام این کارها را انجام دهد باید کارآگاه خصوصی استخدام می‌کرد تا شما را بر پایه داده به‌دست آمده دنبال کند. اکنون که این شغل منسوخ گشته، تلفن همراه موجود در جیب شما تمامی این کارها را به‌صورت اتوماتیک انجام می‌دهد. ممکن است که هیچ کسی این داده را بازیابی نکند اما برای استفاده موجود هستند.

داده مکان شما با ارزش است و هر کسی می‌تواند به آن دسترسی داشته باشد. پلیس این داده را می‌خواهد. تحلیل مکانی تلفن همراه در بازرسی‌های جنایی به طرق مختلف مفید است. پلیس می‌تواند یک تلفن را برای تشخیص مکان آن "ping" کند، از داده‌های تاریخی برای تشخیص اینکه کجا بوده استفاده کند، تمام داده‌های مکانی تلفن همراه را از یک منطقه خاص جمع‌آوری کند تا نشان دهد چه کسی و چه زمانی آنجا بوده است. علاوه بر این پلیس از این داده‌ها برای این اهداف دقیقاً استفاده می‌کند.

دولت‌ها نیز از این داده‌هایی برای ارباب و کنترل اجتماعی استفاده می‌کنند. در سال ۲۰۱۴ دولت اوکراین این پیام‌ور را به‌صورت مثبت و دوستانه به آن دسته از مردم کیف که در زمان خاص در مکان خاصی قرار داشتند ارسال کرد: "مشترک گرامی، شما به‌عنوان یک اخلالگر توده ثبت شده‌اید." فکر نکنید که این رفتار به کشتارهای توتالیتیه محدود می‌گردد؛ در سال ۲۰۱۲ پلیس میشیگان داده مربوط به هر تلفن همراهی که در یک منطقه نزدیک به اعتراضات کارگری بود را مورد جستجو قرار داد. تظاهرکنندگان این زحمت را خود ندادند که اول مجوز بگیرند.

یک صنعت کامل برای ردیابی بهنگام شما به‌طور عام وجود دارد. شرکت‌های اپراتور از تلفن شما در فروشگاه‌ها برای اینکه بفهمند چگونه خرید می‌کنید، برای ردیابی شما استفاده می‌کنند، در جاده برای اینکه مشخص کنند چقدر به یک فروشگاه خاص نزدیک هستید و آگاهی تبلیغاتی را بر اساس اینکه هم اکنون دقیقاً کجایید به گوشی شما ارسال کنند، شما را مورد ردیابی قرار می‌دهند. داده‌های مکانی شما بسیار ارزشمند هستند به گونه‌ای که شرکت‌های تابع همراه آن‌ها را به واسطه‌ها، که خودشان نیز به کسانی که خواهان این داده هستند و در ازای آن پول پرداخت می‌کنند، می‌فروشند. شرکت‌هایی از قبیل Sense Networks در استفاده از چنین داده‌هایی برای ساخت پروفایل شخصی ما تخصص دارند. شرکت‌های تلفن همراه تنها منبع داده تلفن همراه بشمار نمی‌آیند. شرکت آمریکایی Verint سیستم‌های رهگیری تلفن همراه را به شرکت‌های چندملیتی و هم به دولت‌ها در سراسر جهان می‌فروشند. وبسایت این شرکت این‌طور می‌گوید "ما یک رهبر جهانی در راه‌حل‌های داده و اکشن سریع هستیم که هدف ما بهینه‌سازی مشارکت مشتری، داده امنیتی و

کلاهبرداری ریسک و پذیرش و داده می‌باشد و در ۱۸۰ کشور جهان در بیش ۱۰۰۰۰ سازمان مشتری داریم. "شرکت بریتانیایی Cobham سیستمی را به فروش می‌رساند که به اشخاص امکان می‌دهد به یک تلفن تماس "کور" برقرار کند - یعنی تماسی که زنگ نمی‌خورد و قابل ردیابی نیست. تماس کور تلفن را وادار می‌کند بر روی یک فرکانس خاص سیگنال‌هایی را ارسال کند که این امر به فرستنده این امکان را می‌دهد آن تلفن را در محدوده و فاصله یک متری رهگیری کند. این شرکت بریتانیایی مشتریان دولتی در الجزایر، برونی، غنا، پاکستان، عربستان، سنگاپور و آمریکا را تغذیه می‌کند. شرکت Defentek که مرموزانه در کشور پاناما به ثبت رسیده، سیستمی را به فروش می‌رساند که می‌تواند هر شماره تلفن در جهان که برای شبکه، کاربر یا تلفن مقصد ناشناخته و ردیابی نشده، تعیین مکان و رهگیری" کند. این امر یک ادعای توخالی نیست. Tobias Engel پژوهشگر ارتباطات راه دور همین موضوع را در یک کنفرانس مربوط به هکر در سال ۲۰۰۸ مطرح کرد. این روزها مجریان کانال‌ها همین است.

این رهگیری مکانی بر اساس سیستم سلولی پایه‌ریزی شده است. یک سیستم کاملاً متفاوت و دقیق‌تر برای مکان‌یابی وجود دارد که در تلفن همراه شما تعبیه شده است: GPS. این همان چیزی است که داده مکانی را برای اپلیکیشن‌های گوناگون که بر روی تلفنشان اجرا می‌شود، فراهم می‌نماید. برخی اپلیکیشن‌ها از داده مکانی برای خدمات رسانی استفاده می‌کنند، Google maps, Uber, Yelp و غیره مثل Angry Birds درواقع اپلیکیشن‌هایی هستند که فقط می‌خواهند تلاش کنند داده را جمع‌آوری کنند و آن را به فروش رانند.

شما هم می‌توانید این کار را انجام دهید. اپلیکیشن "Location by" برنامه‌ای است که شما می‌توانید آن را بر روی گوشی شخص دیگر نصب کنید و او را رهگیری کنید. این اپلیکیشن برای مادر مضطربی که می‌خواهد از کارهای نوجوان خود سر درآورد یا یک همسر شکاک که می‌خواهد رفتار همسر یا دوست دختر خود را تحت نظر بگیرد، ابزار کاملاً ایده‌آلی است. کارفرمایان از این نوع اپلیکیشن‌ها برای جاسوسی کارکنان خود استفاده کرده‌اند. سازمان امنیت ملی آمریکا (NSA) و همتای بریتانیایی آن یعنی اداره ارتباطات حکومتی (GCHQ) از داده مکانی برای رهگیری افراد جامعه استفاده می‌کنند. اداره NSA داده مکانی تلفن همراه را از انواعی از منابع جمع‌آوری می‌کند: دکل‌های مخابراتی تلفن همراه که تلفن‌ها را به هم مرتبط می‌کنند، مکان شبکه‌های وای فای که تلفن‌ها به آن‌ها Log می‌کنند و داده مکان‌یابی GPS از اپلیکیشن‌های اینترنتی. دو پایگاه داده داخلی NSA کد با نام HAPPYFOOT و FASCIA حاوی داده مکانی جامع ابزارها در سراسر جهان هستند. در واقع NSA از پایگاه‌های داده برای رهگیری حرکات افراد، شناسایی افرادی که با افراد

مورد علاقه ارتباط برقرار می‌کند و هدف‌گیری حملات هوایی هواپیمای بدون سرنشین استفاده می‌کنند.

سازمان NSA ادعا می‌کند که می‌تواند تلفن‌های همراه را حتی زمانی که خاموش هستند رهگیری کند.

من فقط دارم درباره داده مکانی از یک منبع حرف می‌زنم - یعنی تلفن همراه - اما مسئله فراتر از این حرف‌هاست. کامپیوترهایی که شما با آن‌ها کار می‌کنید دائماً داده بسیار شخصی راجع به شما تولید می‌کنند. مثلاً آنچه که می‌خوانید، تماشا می‌کنید و به آن گوش می‌دهید و همچنین افرادی که با شما صحبت می‌کنند و آنچه به شما می‌گویند. در نهایت کامپیوتر آنچه را که بدان فکر می‌کنید تحت پوشش قرار می‌دهد و حداقل تا آن حد که اندیشه‌هایتان شما را به اینترنت و موتورهای جستجوگر سرین می‌دهند. ما در یک عصر طلایی نظارت و پایش زندگی می‌کنیم.

اسکات مک نیل، مدیر اجرایی شرکت Sun Microsystem در سال ۱۹۹۹ به‌صراحت و سادگی اذعان داشت: "شما تحت هر سرایلی حریم خصوصی صفر دارید. از آن فرار کنید." البته او درباره اینکه چگونه باید به نظارت کنترل و کاهش نشان داد در اشتباه است، اما در این مورد حق با اوست که فرار از این نظارت و پایش و حفظ حریم خصوصی روزبه‌روز سخت‌تر می‌شود.

کنترل و پایش به لحاظ معنایی بار سیاسی و عاقلانی دارد، اما من عمداً در اینجا از آن استفاده نمی‌کنم. ارتش آمریکا کنترل و پایش را به‌صورت "مشاهده و نظارت سیستماتیک" تعریف می‌کند. آن‌طور که من توضیح خواهم داد، کنترل الکترونیکی در دنیای معاصر دقیقاً همین‌طور است. ما برای دولت‌ها و شرکت‌های چندملیتی مانند کتاب گشوده هستیم. بنابراین آنان در نفوذ در زندگی شخصی جمعی ما بیش از گذشته است.

معاملاتی که شما به‌طور مکرر با شرکت‌های گوناگون انجام می‌دهید، در واقع نوعی نظارت و پایش در ازای خدمات رایگان محسوب می‌گردند. اریک اسمیت^۱ رئیس گرگال و مدیر ایده‌های آن آقای جارد کوهن^۲ در کتابشان که در سال ۲۰۱۳ موسوم به عصر جدید دیجیتال^۳ بر این موضوع تأکید کرده‌اند.

من در اینجا خلاصه‌ای از پیام آن‌ها را بازگو می‌کنم: اگر شما به ما اجازه بدهید که همه داده شما را داشته باشیم، ما به شما آگهی تبلیغاتی دلخواهتان را نشان خواهیم داد و آن را رایگان از طریق جستجوی وب، ایمیل و همه انواع خدمات در اختیار شما قرار می‌دهیم. در حقیقت، این موهبت

1 Eric Schmidt

2 Jared Cohen

3 New Digital Age

بزرگی است. ما همه حیوانات اجتماعی هستیم، و هیچ چیز گیراتر و جذاب‌تر از برقراری ارتباط با افراد جامعه نیست. ابزارهای دیجیتال به آسان‌ترین و سریع‌ترین شکل ممکن برای برقراری ارتباط با دیگران بدل شده‌اند. چرا ما به دولت‌ها و حکومت‌ها اجازه می‌دهیم به داده ما دسترسی داشته باشند؟ چون از تروریست‌ها می‌ترسیم، از آدم‌های غریبه‌ای که کودکان ما را اغفال می‌کنند ترس و وحشت داریم، از فروشندگان مواد مخدر واهمه داریم، از هر آنچه که بچه‌های سبک مایه و جلف به مدگرایی تمایل پیدا می‌کنند ترس و وحشت داریم. این درواقع همان توجیه سازمان NSA برای برنامه‌های کنترل و پایش عموم مردم است؛ یعنی اگر اجازه دهید که داده شخصی شما به دست ما برسد، ما ترس شما را می‌ریزیم و خیال شما را آسوده می‌کنیم.

مسئله این است که این معاملات، دست کم تا آنجا که امروزه جا افتاده‌اند و ساخته شده‌اند، معاملات خوب و منصفانه‌ای نیستند. ما خیلی راحت پذیرای این نوع معامله شدیم، بدون آنکه اصلاً شرایط و مفاد آن را همیده باشیم.

چیزی که در اینجا رافع دارد این است که تکنولوژی امروزی به شرکت‌های چندملیتی و دولت‌ها قابلیت‌های وسیعی برای نظارت و پایش عموم مردم می‌دهد. نظارت و پایش عموم مردم خطرناک است. این کار موجب تبعیض تقریباً در هر زمینه‌ای مثل تبعیض نژادی، مذهبی، طبقاتی و باورهای سیاسی می‌شود. این امر عموم مردم را در برابر کار انجام‌شده قرار می‌دهد و قدرت انتخاب را از آن‌ها می‌گیرد و حفظ موازنه معنادار را از بین می‌برد. نظارت و پایش در ما احساس ناامنی به وجود می‌آورد و آزادی ما را سلب می‌کند. قوانین و قواعدی که ما برای حفاظت خودمان از خطرات بر اساس سیستم‌های تکنولوژیکی پیشین وضع کرده بودیم، اکنون به‌طور اسفباری بی‌خاصیت شده‌اند؛ این قوانین کارایی خود را از دست داده‌اند. ما باید آن‌ها را بازنویس کنیم و در این راه درنگ جایز نیست. در این کتاب من در سه قسمت این مسئله را بررسی می‌کنم:

قسمت اول جامعه تحت نظر که ما در آن زندگی می‌کنیم را توصیف می‌کند. در بخش اول نگاهی به انواع داده یا داده‌های شخصی که ما در گذران زندگی تولید می‌کنیم، می‌اندازیم. این امر فقط داده مکان‌یابی تلفن همراهی که من توصیف کردم نیست، در واقع نیز شامل داده یا داده‌ها در خصوص مکالمات تلفنی، ایمیل، پیامک‌های ما علاوه بر همه صفحات وبی که قرائت می‌کنیم، داده‌های معاملات مالی و غیره می‌شود. خیلی از ما هنوز نمی‌دانیم که کامپیوترها تا چه اندازه در همه امور زندگی ما عجین شده‌اند یا اینکه هنوز نمی‌دانیم که حافظه کامپیوتر آن‌قدر ارزان شده است که می‌تواند به‌طور نامحدود همه داده‌ای که تولید می‌کنیم را ذخیره کند. خیلی از ما نیز این را

دست کم می گیریم که افشا خودمان با استفاده از داده یا داده‌هایی که فکر می‌کنیم محرمانه و بی‌نام هستند چقدر آسان و راحت شده است.

فصل ۲ نشان می‌دهد که چگونه همه این اطلاعات با داده‌ها برای پایش و نظارت مورد استفاده قرار می‌گیرند. این نوع نظارت‌ها در همه‌جا جاری و ساری است و به‌طور خودکار انجام می‌گیرد، بدون اینکه انسان در آن دخالتی داشته باشد و از چشم ما پنهان هستند، این به‌نوعی نظارت و پایشی است که به‌طور فراگیر همگان را دربر می‌گیرد.

تمرکز بر اینکه شرکت‌های چندملیتی و دولت‌ها چگونه این داده‌ها یا داده را جمع‌آوری می‌کنند کار چندان دشواری نیست، اما این امر یک تصویر تحریف‌شده و مخدوش در اختیار ما می‌گذارد. داستان واقعاً از این قرار است که جریان‌های مختلف داده چگونه پردازش، همبسته و تجزیه و تحلیل می‌شوند و این داده در واقع داده شخص خاصی نیست، بلکه می‌تواند داده هر کسی باشد. نظارت و پایش فراگیر عموم مردم است. از تعداد زیاد نظارت و پایش‌های موردی بسیار متفاوت است، نظارت و پایش همگانی در مدتی انجام می‌گیرد که در گذشته هرگز سابقه نداشته است. در فصل ۳ در این باره بحث خواهیم کرد.

شرکت‌های چندملیتی که ما با آن‌ها تعامل می‌کنیم، یا در مقام مشتری یا در مقام کاربران، داده‌های حاصل از نظارت و پایش را به‌طور وسیع - جمع‌آوری می‌کنند. فصل ۴ به مدل‌های تجاری نظارت و پایش، اساساً آگهی‌های تبلیغاتی خصوصی اختصاص می‌یابد. یک صنعت واسطه‌گری داده، به‌طور تمام‌عیار پدید آمده که از اطلاعات و داده‌های شخصی ما سود می‌برد و آن داده بدون آگاهی و رضایت ما خرید و فروش می‌شود. عامل اصلی و نه تنها مرکز آن در واقع یک مدل جدید پردازشی است، که در این مدل داده ما در برابر ذخیره می‌شود. وسیله ابزارهایی مثل آیفون که شدیداً تحت نظارت سازنده قرار دارد در دسترس قرار می‌گیرد. نتیجه آن چیزی نیست جز دسترسی بی‌سابقه شرکت به شخصی‌ترین داده ما و کنترل همه‌جانبه بر آن داده.

فصل پنج به بررسی کنترل از جانب دولت‌ها می‌پردازد. دولت‌های سراسر جهان شهروندان خود را دقیقاً می‌بایند و هم در داخل کشور و هم در سطح بین‌الملل به کامپیوترهایشان نفوذ پیدا می‌کنند. دولت‌ها می‌خواهند برای یافتن تروریست‌ها و مجرمان در زندگی هر شخصی تجسس کنند و - بسته به نوع حکومت - فعالان سیاسی، دگراندیشان، فعالان زیست‌محیطی، مدافعان حقوق مصرف‌کننده و آزاداندیشان را رهگیری کنند. این جانب عمدتاً بر روی سازمان NSA تمرکز می‌کنم چراکه این

همان آژانس دولتی سری است که ما آن را به دلیل انتشار اسناد از جانب ادوارد اسنودن^۱ کاملاً می‌شناسیم.

شرکت‌های چندملیتی و دولت‌ها اشتباهی سری‌ناپذیری برای گرفتن داده‌ها دارند و من در فصل ۶ بحث خواهم کرد که چگونه شرکت چندملیتی و دولت‌ها با یکدیگر همکاری می‌کنند. من آن را یک شراکت نظارت عمومی - خصوصی می‌نامم و این نوعی ائتلاف است که هر روز عمیق‌تر می‌شود. این دلیل اصلی است که نظارت و پایش خیلی پیچیده و مرموز است و مانع تلاش‌ها برای اصلاح سیستم خواهد شد.

همه این مسائل مهم هستند، حتی اگر شما به شرکت‌هایی بزرگ که با آن‌ها تعامل می‌کنید و دولت‌هایی که زرادخانه‌های زندگی می‌کنید اعتماد داشته باشید. با توجه به این موضوع قسمت دوم به بسیاری از آسیب‌های مرتبط به هم که از نظارت همگانی فراگیر ناشی می‌شود، می‌پردازد. در فصل ۷، بنده آسیب‌های ناشی از نظارت و پایش دولتی را مورد بحث قرار خواهم داد. تاریخ مکرراً خطرات اجازه دادن به دولت‌ها در انجام نظارت‌ها و پایش‌های همگانی بی‌محابا بر شهروندان خود را به اثبات رسانده است. آسیب‌های بالقوه شامل تبعیض و کنترل، اثرات مخوف بر آزادی بیان و اندیشه آزاد، اذیت و آزار اجتناب‌ناپذیر و محدود کردن آزادی می‌گذارد. اینترنت این توانایی را دارد که به یک نیروی محرکه عظیم برای ترویج آزادی در سراسر جهان بدل شود؛ ما داریم آن امکان بالقوه را با اجازه دادن به دولت‌ها در انجام نظارت و پایش سراسری به هدر می‌دهیم.

فصل ۸ به آسیب‌های ناشی از نظارت‌های بی‌قید و بند شرکتی اشاره می‌کند. شرکت‌های خصوصی هم اکنون «محل‌هایی» بر روی اینترنت که در آن‌ها گرد هم می‌آییم را تحت نظر دارند و آن‌ها داده‌ها را که ما در آنجا رد و بدل می‌کنیم به سود خود می‌فروشند. ما با اجازه دادن به شرکت‌ها در داشتن اطلاعات درباره همه چیز خودمان در واقع به آن‌ها اجازه می‌دهیم ما را مقوله‌بندی و طبقه‌بندی کنند و زندگی‌های ما را دست‌کاری کنند. این دست‌کاری وسیعاً پنهان و بی‌قاعده است و هرچه تکنولوژی پیشرفت می‌کند تأثیر آن بیشتر خواهد شد.

نظارت و پایش فراگیر همچنین به آسیب‌های دیگری منجر می‌شود. فصل ۹ از آسیب‌های اقتصادی به خصوص در مؤسسات تجاری آمریکا بحث می‌کند که این آسیب‌ها زمانی خود را نشان می‌دهند که شهروندان از کشورهای مختلف تلاش کنند از خودشان در برابر نظارت و پایش که از جانب سازمان NSA و متحدان آن انجام می‌گیرد دفاع کنند. اینترنت یک پلتفرم یا چهارچوب جهانی است و تلاش‌ها از جانب کشورهایایی مثل آلمان و برزیل در ایجاد دیوار ملی دور داده‌ها برای

شرکت‌هایی که اجازه نظارت به دولت نمی‌دهند بسیار گران تمام می‌شود. (بخصوص شرکت‌های آمریکایی).

من در فصل ۱۰ پیرامون خطراتی که در اثر نبود حریم خصوصی ایجاد می‌شود بحث خواهم کرد. مدافعان نظارت از Stasi (سازمان امنیت آلمان شرقی سابق) گرفته تا دیکتاتور شیلی آگوستو پینوشه تا به اریک اشمیت در گوگل - همیشه به این ضرب‌المثل قدیمی استناد می‌کنند که «اگر چیزی برای پنهان کردن نداری دیگر ترس لزومی ندارد». این در واقع یک مفهوم به‌طور خطرناک محدود از ارزش حریم خصوصی است. حریم خصوصی نیاز ضروری انسان است و در توانایی ما در کنترل چگونگی ارتباط با جهان نقش محوری دارد. زندگی عاری از حریم خصوصی اساساً غیر انسانی است و هیچ فرق نمی‌کند که آیا نظارت و پایش به وسیله پلیس مخفی که ما را در هرجایی دنبال می‌کند انجام بگیرد یا توسط یک الگوریتم کامپیوتر که هرگونه حرکت ما را رهگیری می‌کند.

در فصل ۱۱، من مضرات و آسیب‌های ایجاد شده در امنیت ناشی از نظارت و پایش را بیان می‌کنم. نظارت جمعی رتبه‌بندی نمی‌شود، به‌عنوان یک مزیت امنیتی تلقی می‌شود، یعنی چیزی که ما را از تروریسم در امان نگه می‌دارد. با این حال، هیچ دلیل قطعی از موفقیت‌های واقعی علیه تروریسم حاصل از نظارت و پایش جمعی وجود ندارد. انجام نظارت همگانی و جمعی فراگیر مستلزم داشتن و نگهداری از یک اینترنت ناامن می‌باشد که هم ما را از دولت‌ها، مجرمان و هکرها رقیب دچار ناامنی می‌کند.

سرانجام، بخش سه آنچه که باید برای حفاظت از خودمان از نظارت شرکتی و دولتی انجام دهیم را برمی‌شمارد. راه‌حل‌ها به پیچیدگی مسائل هستند و اغلب نیاز به توجه دقیق دارند. قبل از این که توصیه‌های سیاستی و فنی خاص را ارائه دهم، در فصل ۱۲ هشتم، اصول کلی را پیشنهاد می‌کنم که باید راهنمای تفکر ما باشد.

در زیر دو فصل به توصیه‌های سیاستی خاص اختصاص یافته است: بریتانیا در فصل ۱۳ و برای شرکت‌های چند ملیتی در فصل ۱۴، برخی از این توصیه‌ها مفصل‌تر از دیگر توصیه‌ها است و برخی آرمانی‌تر هستند تا این که فوراً قابل اجرا باشند. اما همه مهم هستند و نادیده گرفتن یکی از آن‌ها می‌تواند دیگر راه‌حل‌ها را خدشه‌دار کند.

فصل ۱۵ به آنچه که هر یک از ما می‌توانیم به‌طور انفرادی انجام دهیم می‌پردازد. من توصیه فنی عملی و همچنین پیشنهادهایی را برای اقدام سیاسی معرفی می‌کنم. ما در دنیایی زندگی می‌کنیم که در آن تکنولوژی می‌تواند بر سیاست غلبه کند و نیز دنیایی است که سیاست می‌تواند بر تکنولوژی غلبه کند که در اینجا برای ادامه حیات ما به هر دو این‌ها نیاز داریم.

من این بحث را در فصل ۱۶ با بررسی آنچه که باید به طور جمعی در مقام یک جامعه انجام دهیم به پایان می‌رسانم. اکثر توصیه‌ها در فصل ۱۳ و ۱۴ مستلزم یک دگرگونی در چگونگی استنباط ما از نظارت و پایش و چگونگی ارج نهادن به حریم خصوصی می‌باشد، زیرا تا زمانی که جامعه برای تغییر آن‌ها همت نکند ما دست به اصلاحات قانونی جدی نخواهیم زد. در اینجا ارزش زیادی در انباشتن داده ما برای پژوهش پزشکی، بهبود آموزش و پرورش و دیگر کارهایی که به جامعه سود می‌رساند وجود دارد. ما باید درک کنیم که چگونه به طور جمعی به آن ارزش ضمن به حداقل رساندن مضرات و آسیب‌ها دست یابیم. این امر در واقع همان موضوع اساسی است که زیربنای این کتاب را تشکیل می‌دهد.

این کتاب خیلی چیزها را در برمی‌گیرد و ضرورتاً همه به طور سریع همه چیز را به هم ربط می‌دهند. یادداشت‌های پایانی شامل مراجع گسترده و مفصل برای کسانی که علاقه به مطالعات عمیق‌تر دارند، می‌شود. این مراجع در این وبسایت کتاب همچنین وجود دارد.

www.schneider.com/dg.html در این سایت شما نیز هرگونه به‌روزرسانی‌ها در کتاب‌ها بر اساس رویدادهایی که بعد از اتمام نوشتن این کتاب به وجود آمده مشاهده خواهید کرد.

من با یک تعصب افراطی آمریکایی بودن نمی‌کنم. بیشتر مثال‌ها از کشور آمریکا می‌باشد و بیشتر توصیه‌ها به بهترین نحو در آمریکا به کار می‌رود. بنا به یک دلیل، این همان چیزی است که من می‌دانم. اما من نیز بر این باورم که کشور آمریکا به عنوان یک مثال منفرد به شمار می‌آید که در آن می‌توان نشان داد که چگونه امور مسیر اشتباهی را می‌کند و آمریکا یک موقعیت منحصر به فردی است که می‌توان در آن امور را بهتر و بهبود بخشید.

پیش‌زمینه من امنیتی و تکنولوژی است. سال‌هاست که من درباره پیچیدگی تأثیر تکنولوژی‌های امنیتی بر افراد جامعه و بالعکس قلم می‌زنم. من شاهد ظهور نظارت و پایش در عصر داده هستم و بسیاری از تهدیدها و ناامنی‌ها را در این دنیای جدید مشاهده کردم. من به تفکر در خصوص مسائل امنیتی و درباره مسائل اجتماعی وسیع‌تر از میان‌لنز مسائل امنیتی عادت کردم. این دیدگاه به من فهم منحصر به فردی هم از مسائل و راه‌حل‌ها می‌دهد.

این کتاب و این جانب ضد تکنولوژی نیستیم. اینترنت و عصر اطلاعات به طور اعم مزایای بزرگی برای جامعه به ارمغان آورده است. باور دارم آن‌ها در آینده همچنان این مزیت را خواهند داشت. من حتی ضد نظارت و پایش نیستم. مزایای کامپیوترهایی که می‌دانند ما چه کار می‌کنیم زندگی را تغییر شکل می‌دهند. نظارت و پایش محصولات و خدمات سنتی را دگرگون کرد و کاملاً مقولات جدیدی از تجارت را به ارمغان آورده است. نظارت و پایش یک ابزار ارزشمند برای اجرای قانون

است. نظارت و پایش به افراد در سراسر جهان در همه انواع شیوه‌ها کمک خواهد کرد و در آینده هم چنین کاری خواهد کرد.

با وجود این، تهدیدهای نظارت و پایش واقعی هستند و ما درباره آن‌ها به اندازه کافی حرف نمی‌زنیم. پاسخ من به همه این نظارت و پایش خزنده کاملاً انفعالی بوده است. ما درباره معاملاتی که انجام می‌دهیم فکر نمی‌کنیم، زیرا آن‌ها در مقابل ما به طور محسوس انجام نمی‌گیرند. تحولات تکنولوژیکی روی می‌دهند و ما آن‌ها را برای بیشترین کارها می‌پذیریم. نمی‌توان خودمان را سرزنش کنیم؛ تحولات آن قدر سریع روی داده است که ما واقعاً اثرات آن‌ها را ارزیابی نکرده‌ایم یا پیامدهایشان را نسنجیده‌ایم. این در واقع همان چیزی است که چگونه ما سر از یک جامعه نظارتی و پایشی در آورده‌ایم. جامعه نظارت و پایشی بر ما تحمیل شد.

قرار نبود که جامعه بدین شکل باشد. اما ما باید دست به کار شویم. می‌توانیم کار خود را با مذاکره مجدد معاملاتی که با آن اطلاعات انجام می‌دهیم آغاز کنیم. ما باید درباره چگونگی برخورد با تکنولوژی‌های جدید و فعال‌سازی یا نباشیم. ما باید درباره آنچه که از زیربنای تکنولوژی ما که می‌خواهیم آن‌طور باشد فکر کنیم و باید درباره این فکر کنیم که چه ارزش‌هایی را می‌خواهیم در درون این تکنولوژی‌ها بگنجانیم. ما باید ارزش داده‌های خود را در جامعه با ماهیت شخصی‌اش متعادل کنیم. ما باید ترس‌هایمان را بررسی کنیم. تصمیم بگیریم که به چه میزان از حریم خصوصی خود را می‌خواهیم عملاً بابت زندگی‌مان را فدا کنیم. ما باید بسیاری از مضرات و آسیب‌های نظارت و پایش هجومی را بفهمیم. ما باید از خودمان دفاع کنیم.