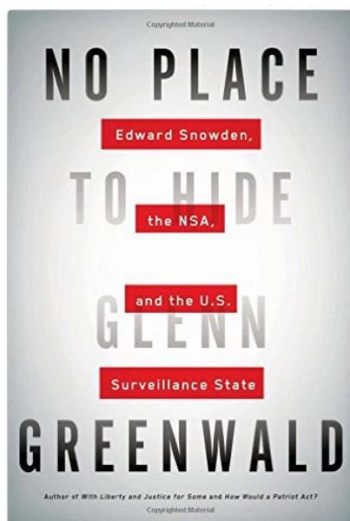


# اینترنت آدم‌ها (۱۱)

## جایی برای پنهان شدن نمانده است

□ نوشته علیرضا محمدی فر



همچنان که در مقاله اول از این سلسله از مقالات گفتیم با وجود دستاوردهای بسیار بزرگ و شگفت‌انگیز در عصر اطلاعات، به دلیل توانی که فناوری‌های اطلاعات و ارتباطات در محدود کردن حریم خصوصی انسان دارند می‌توانند دورانی را بیافرینند که شاید آیندگان آن را دوران تاریک یا قرون وسطی در عصر اطلاعات نام بگذارند. از سوی دیگر، گفتیم که کنار گذاشتن و نادیده گرفتن فناوری‌های اطلاعات و ارتباطات برای انسان این روزگار به دلیل منافع بی‌شماری که دارد ناممکن است و نمی‌تواند به عنوان یک راه حل مطرح شود. در این مقاله به مخالفت‌ها با مهم‌ترین فناوری حافظ حریم خصوصی انسان، یعنی رمزنگاری پرداخته‌ایم.

شاید برای آدم‌های خوب مشکل زیادی به وجود نیامد، اما بی‌گمان برای آدم‌های خیلی خوب \_ منظورمان آدم‌های خلاق و کسانی است که در طول تاریخ بشر تحول‌آفرین بوده‌اند \_ مسئله به وجود می‌آورد. دانشمندی را تصور کنید که نتیجه تحقیقاتش پیش از آن که رسماً انتشار یابد به دلیل از بین رفتن یک زیرساخت مستحکم برای حریم خصوصی به سرقت برود؛ داستان‌نویس یا شاعری را تصور کنید که اثر خلاقانه‌اش پیش از انتشار عمومی توسط کسانی دیگر منتشر شود؛ مجسمه‌سازی را تصور کنید که در نیمه راه ساختن یک اثر بدیع، مشابه آنچه را می‌خواسته بسازد در گالری‌های مختلف و در اینترنت ببیند. اگر حریم خصوصی نباشد \_ یا به تعبیر گلن گرین‌والد، جایی برای پنهان شدن نمانده باشد \_ انگیزه‌ای برای خلاقیت وجود نخواهد داشت. مغزها تنبل خواهند شد و به تدریج هوش انسان بلااستفاده خواهد شد. (استفان هاکینگ گفته است که هوش مصنوعی سبب انقراض انسان خواهد شد، اما آنچه می‌تواند انسان را منقرض کند، حذف حریم خصوصی انسان، به ویژه، آن گونه که در بخش پیشین این سلسله از مقالات گفتیم، عدم برخورد با ذخیره‌گرهای خصوصی، مانند حافظه فلش، کارت SD، یا دیسک سخت متعلق به هر فرد به عنوان بخشی از مغز آن فرد است؛ درباره سخن هاکینگ بعدها در بخشی که به هوش مصنوعی خواهیم پرداخت بیشتر خواهیم گفت.)

همچنان که در بخش پیشین از این سلسله از مقالات گفتیم، در دنیای سایبری امروز فناوری رمزنگاری (encryption) می‌تواند از حریم

«در ۱۶ ماه گذشته که در سرتاسر جهان درباره اهمیت حفظ حریم خصوصی صحبت کرده‌ام، بارها از جانب افراد مختلف با این پاسخ روبه‌رو بوده‌ام که «چیزی برای پنهان کردن ندارم، پس چرا باید نگران تجاوز به حریم خصوصی‌ام باشم». همواره پاسخ یکسانی برای همه آنها داشته‌ام. خودکاری از جیب بیرون می‌آورم، نشانی ایمیل را می‌نویسم، و می‌گویم که این نشانی ایمیل من است، از شما می‌خواهم که هرگاه به خانه رسیدید، گذرواژه‌های همه حساب‌های ایمیل‌تان را برای من ایمیل کنید، تا ببینم بر روی خط چه کارهایی انجام می‌دهید، آنچه را می‌خوانید و آنچه را منتشر می‌کنید بخوانم. بالاخره، اگر آدم بدی نباشید، اگر هیچ کار نادرستی انجام نمی‌دهید، نباید چیزی برای پنهان کردن داشته باشید. هیچ‌کس تا به حال به من پاسخ نداده است.»<sup>۱</sup>

سخنان فوق بخشی از یک سخنرانی گلن گرین‌والد<sup>۲</sup>، یکی از نخستین روزنامه‌نگاران است که مطالب مختلفی درباره فایل‌های ادوارد اسنودن منتشر کرده است.

گلن گرین‌والد که نویسنده کتابی پر فروش است به نام «جایی برای پنهان شدن نمانده است»<sup>۳</sup>، معتقد است که نمی‌توان آن گونه که مردم عادی باور دارند آدم‌ها را به دو دسته آدم‌های خوب و آدم‌های بد

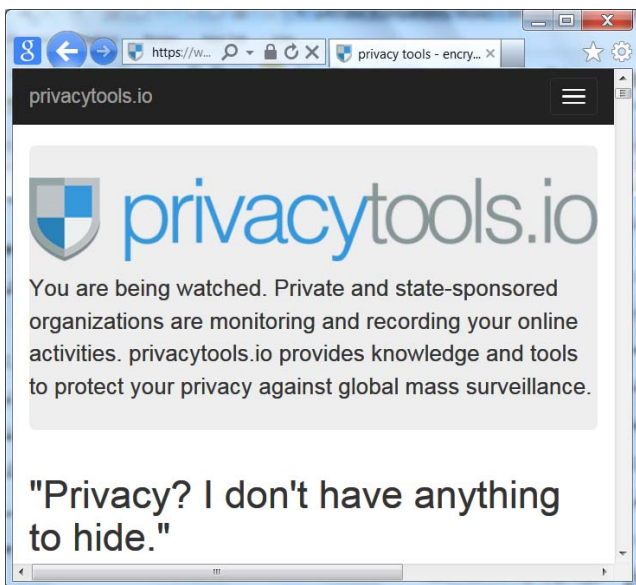
<sup>1</sup> [http://www.ted.com/talks/glenn\\_greenwald\\_why\\_privacy\\_matters](http://www.ted.com/talks/glenn_greenwald_why_privacy_matters)

<sup>2</sup> Glenn Greenwald

<sup>3</sup> No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State

واقعیت آن است که چه جمهوری خواهان و چه دمکرات‌های آمریکا مطمئناً به اهمیت رمزنگاری برای امنیت داده‌های شهروندان واقف هستند، اما آنها سرمستانه بیشتر به قدرتی فکر می‌کنند که داشتن شاه کلیدهای بازکننده قفل رمزنگاری در اختیار آنها قرار خواهد داد. هر چند، چنین قدرتی به تدریج می‌تواند کشور آمریکا را چیزی شبیه به اتحاد جماهیر شوروی سابق کند. (جالب آن که نگاه‌ها به مالکیت خصوصی هم در حال تغییر است، امروزه به جای به تملک در آوردن یک آلبوم موسیقی یا یک فیلم می‌توانیم مشترک سایت‌هایی مانند Netflix یا Spotify شویم؛<sup>۷</sup> در آینده به جای خرید خودرو می‌توانیم از خودران‌هایی بهره بگیریم که با سرویس‌هایی شبیه به سرویس‌های Uber<sup>۸</sup> به سرعت در دسترس مان قرار می‌گیرند؛ و مانند آن! پس شاید چیزی شبیه به «مارکسیسم-کامی‌ایسم» [رئیس‌اف‌بی‌آی] پدیدار شود!!)

البته، مقاومت‌ها نیز آغاز خواهد شد، و در چنین وضعیتی نرم‌افزارهای رمزنگاری زیرزمینی جای خود را باز خواهند کرد. همین امروز هم سایت‌های وب فراوانی برای مقابله با سیاست‌های NSA و اف‌بی‌آی به وجود آمده است، مانند سایت وب <https://www.privacytools.io>



<sup>7</sup> [http://www.pcmag.com/article2/0,2817,2489562,00.asp?mailing\\_id=1435137&mailing=whatsnewnow&mailingID=2CBB1CFF778C96F365A1BC1B8B26E994](http://www.pcmag.com/article2/0,2817,2489562,00.asp?mailing_id=1435137&mailing=whatsnewnow&mailingID=2CBB1CFF778C96F365A1BC1B8B26E994)  
<sup>8</sup> <https://www.uber.com>

خصوصی ساییری مردم محافظت کند. اما موضوع رمزنگاری و حفاظت از داده‌ها از یک موضوع فناوری به یک موضوع سیاسی، به ویژه در کشور آمریکا تبدیل شده است. به عنوان مثال، به ترجمه چکیده‌ای از مقاله گاردین با عنوان «جمهوری خواهان فکر می‌کنند که اگر داده‌ها رمزنگاری شود تروریست‌ها برنده می‌شوند»<sup>۴</sup> توجه نمایید:

«فوائد رمزنگاری \_ که در همه جا از بانک‌داری الکترونیک گرفته تا ایمیل به کار گرفته می‌شود \_ چنان بدیهی است که گویی سیاستمداران ضد آن اصلاً در این باره با هیچ متخصص کامپیوتری مشورت نکرده‌اند. به عنوان مثال، جب بوش، برادر رئیس جمهور اسبق آمریکا و نامزد فعلی جمهوری خواهان می‌گوید که برای مقابله با اشرار باید جلوی رمزنگاری برخط شهروندان گرفته شود. تعبیرات بوش بازتاب نظریات خطرناک جیم کامی<sup>۵</sup>، رئیس اف‌بی‌آی است که کمپینی عمومی را بر ضد آپل و گوگل برای جلوگیری از رمزنگاری در آیفون‌ها و وسایل اندرویدی به راه انداخته است.

جب بوش در یک کمپین انتخاباتی گفته است که اگر از رمزنگاری استفاده کنید، کار دولت در یافتن اشرار دشوارتر می‌شود. او نمی‌داند که ما برای بسیاری از کارهای مان در اینترنت، مانند امور بانکی از رمزنگاری بهره می‌گیریم.

متأسفانه، به نظر می‌آید که عقاید بوش بخشی از الگوی طراحی شده برای نامزدهای جمهوری خواه انتخابات ریاست جمهوری ۲۰۱۶ باشد. به نظر می‌رسد که هیچ کدام از آنها درکی از فناوری‌های امنیت داده و نقش بسیار اساسی رمزنگاری در امنیت ساییری ما نداشته باشند. حتی یکی دیگر از نامزدها در پاسخ به این پرسش که آیا آپل و گوگل باید رمزنگاری دو سر ارتباط<sup>۶</sup> را پیاده‌سازی کنند یا نه، گفته است که باید دیوارهای ساییری فرو بزنند. این در حالی است که رمزنگاری دو سر ارتباط اگر قدرتمند باشد بهترین دفاع را در برابر حملات ساییری به وجود می‌آورد.

مایه خجالت است که کاخ سفید هنوز در برابر برنامه‌های خطرناک رئیس اف‌بی‌آی ناپستاده است. در دنیای مدرن، اهمیت رمزنگاری قدرتمند را نمی‌توان دست کم گرفت. پس نامزدهای ریاست جمهوری ما در چه زمانی این حقیقت را درک خواهند کرد؟»

<sup>4</sup> <http://www.theguardian.com/commentisfree/2015/aug/22/republicans-think-encrypted-data-terrorists-win>  
<sup>5</sup> Jim Comey  
<sup>6</sup> end-to-end encryption