



مانیفست سایفرپانک‌ها

در عصر ارتباطات، حریم خصوصی برای جامعه‌ی باز یک نیاز است. حریم خصوصی محرمانه‌گی نیست. یک موضوع خصوصی چیز نیست که فرد نمی‌خواهد همگان از آن با خبر باشند. اما یک موضوع محرمانه چیز نیست که فرد نمی‌خواهد هیچکس از آن مطلع شود. حریم خصوصی یک توانایی است. توانایی آشکار شدن به شکل انتخاب شده.

اگر دو شخص با هم به نوعی معاملاتی داشته باشند، هر دو از مرادداشتان خاطراتی خواهند داشت. هر کدام از طرفین می‌تواند در مورد این خاطرات حرف بزند، پس چطور ممکن است که از آن پیشگیری کرد؟ ممکن است بشود بر ضد آن قانونگذاری کرد اما «آزادی بیان» حتی از حریم خصوصی برای جامعه باز، نیاز مبرم‌تری است. ما در طلب آنیم که هیچ سخنی را محدود نکنیم.

حال که حریم خصوصی مطلوب ماست، باید اطمینان حاصل کنیم که در یک تراکنش هر طرف فقط از آن اطلاعاتی که برای انجام تراکنش به صورت مستقیم به آن نیاز است، مطلع می‌شود. از آنجا که دربارهی هر اطلاعاتی میتوان سخن گفت، باید اطمینان داشته باشیم که تا جای ممکن اطلاعات کمی را فاش کنیم. در بیشتر موارد [برای انجام معامله] نیاز به هویت شخصی چشمگیر نیست. وقتی که در مغازه‌ای مجله‌ای را می‌خرم و پول نقد را به صندوقدار می‌دهم نیازی نیست که هیچ‌کس بداند: «من کیستم؟». وقتی از خدمات دهنده‌ی رایانامه‌ام می‌خواهم که پیام‌هایم را دریافت یا ارسال کند، خدمات دهنده نیازی ندارد که بداند هویت من چیست یا با چه کسانی صحبت می‌کنم و چه می‌گویم یا چه می‌شنوم. او فقط باید بداند که چطور پیام را به مقصد برساند و چقدر من به او هزینه‌ی خدمات بدهکارم. وقتی که هویت من توسط سازوکارهای ضمنی آشکار شود، دیگر من حریم خصوصی ندارم. در اینجا نمیتوانم به صورت انتخاب شده آشکار سازی کنم، من در واقع همیشه خودم را آشکار کنم.

بنابر آنچه گفته شد، **حریم خصوصی در یک جامعه باز نیازمند سامانه های تراکنش گمنامانه (anonymous) است.** یک سامانه‌ی تراکنش گمنامانه یک سامانه‌ی تراکنش محرمانه نیست. یک سامانه تراکنش گمنامانه سامانه‌ای است که به افراد این توانایی را می‌دهد که: هویتشان را فقط و فقط وقتی که بخواهند آشکار کنند. این جوهره‌ی گمنامانگی است.

حریم خصوصی در یک جامعه‌ی باز نیازمند رمزنگاری است. من اگر چیزی می‌گویم، می‌خواهم فقط توسط آنها که در نظر دارم شنیده شود. اگر محتوای حرف من در اختیار همگان است من حریم خصوصی ندارم.

وقتی رمزنگاری میکنیم خبر از میل به نگه داشتن حریم خصوصی می‌دهیم، و اگر رمزگذاری ضعیف انجام شود نشان از رغبت کمتر به رعایت حریم خصوصی است. گذشته از این، در زمانی که گمنامی حالت پیشفرض است، برای اینکه امکان آشکار کردن هویت را به یک فرد بدهیم نیاز به سیستم‌های امضای مبتنی بر رمزنگاری داریم.

ما نمیتوانیم از دولت‌ها، بنگاه‌ها و سایر سازمان‌های بزرگ بی نام و نشان انتظار داشته باشیم از روی لطف حریم خصوصی ما را به ما ببخشند. این به نفع آنهاست که از [رازهای] ما بگویند و باید انتظار این را داشته باشیم که چنین کنند. جلوگیری کردن از سخن گفتن آنها و نشر اطلاعات توسط آنها، جنگیدن با حقیقت اطلاعات است. اطلاعات نه تنها می‌خواهد آزاد باشد بلکه اشتیاق و آرزوی آزادی دارد. اطلاعات تا پرکردن همه‌ی فضای قابل استفاده برای ذخیره‌سازی گسترش می‌یابد. اطلاعات پسرعموی جوانتر و قوی‌تر شایعه است. اطلاعات بادپاست. از شایعه چشمان بیشتری دارد، بیشتر میداند، و کمتر می‌فهمد. اگر انتظار داریم حریم خصوصی داشته باشیم باید از آن دفاع کنیم. ما باید همراه شویم و سامانه‌هایی را بسازیم که امکان انجام تراکنش‌های گمنامانه را بدهند. برای قرن‌ها مردمان از حریم خصوصی خودشان با نجوا و تاریکی و پاکت‌های نامه و درهای بسته و قاصدها و اشارات راز گونه دفاع کرده‌اند. فنون گذشته امکان حریم خصوصی قوی را فراهم نمیکرد، اما تکنولوژی‌های الکترونیکی این اجازه را به ما میدهند. ما «سایفرپانک‌ها» خودمان را وقف سامانه‌های گمنامانه کرده ایم. **ما از حریم خصوصی‌مان با رمزنگاری، سامانه‌های ارسال گمنامانه‌ی رایانامه و امضاهای دیجیتال و پول الکترونیکی دفاع میکنیم.**

سایفرپانک‌ها کد می‌نویسند. ما می‌دانیم که بلاخره کسی باید برای دفاع از حریم خصوصی نرم‌افزار بنویسد. و چون نمی‌شود حریم خصوصی داشت مگر برای همه، ما نرم‌افزار را خواهیم نوشت. ما کدهامان را منتشر خواهیم کرد تا یاران سایفرپانکمان با آن تمرین و بازی کنند. استفاده از کدهای ما برای همه‌ی کارهای در همه جای دنیا جایز خواهد بود. برای ما اهمیت چندانی ندارد اگر شما نرم‌افزاری که ما مینویسیم را تایید نمی‌کنید. ما می‌دانیم که نرم‌افزار را نمی‌توان از بین برد و یک سامانه‌ی بسیار گسترده شده را نمی‌توان خاموش کرد.

سایفرپانک‌ها از وضع مقررات برای رمزگذاری بیزارند. چرا که رمزگذاری از اساس یک عمل شخصیت است. عمل رمزگذاری در واقع اطلاعات را از فضای عمومی خارج میکند. حتی قوانین ضد رمزگذاری فقط تا مرزهای سیاسی ملل و قدرت اعمال خشونتشان وسعت می‌یابند. **رمزگذاری ناگزیر در تمام جهان گسترده خواهد شد، و بدنبال آن سامانه‌های تراکنش‌های گمنامانه ممکن خواهد شد.**

برای اینکه حریم شخصی گسترده شود باید بخشی از یک قرارداد اجتماعی باشد. مردم باید همراه شوند و این سامانه‌ها را برای نفع عموم راه‌اندازی کنند. حریم شخصی یک فرد تا حوزه‌ای که یارانش با او همکاری میکنند گسترش خواهد یافت. ما سایفرپانک‌ها مشتاق سوال‌ها، نگرانی‌ها و امیدهای شما هستیم که ممکن است نگاه شما را معطوف به مسئله کند، تا مبدا ما خودمان را فریب دهیم. در هر حال ما به خاطر اینکه کسانی با اهداف ما مخالفت کنند راهمان را عوض نخواهیم کرد.

سایفرپانک‌ها به صورت فعالانه در حال امن‌تر کردن شبکه‌ها برای حریم شخصی هستند. باشد که با شتاب با هم پیشرویم. به پیش!

اریک هیوز

بیستم فروردین ۱۳۷۲