تلفن های هوشمند به تمام صحبت‌های اطراف خود گوش می‌دهند!

آیا می توان متوجه شد که چه زمانی از میکروفون استفاده می شود؟

در صورت فعال شدن میکروفون، آیا داده های ضبط شده از طریق اینترنت به سرورهای خاصی منتقل می گردند یا خیر؟

ضریب نفوذ تلفن همراه به بالاترین مقدار طی سال های اخیر رسیده، و میکروفون ها نیز یکی از اجزای ضروری موبایل ها به شمار می روند، به همین دلیل نگرانی در مورد حریم شخصی تا حد زیادی افزایش یافته است.

به نقل از دیجیاتو، دیگر اسمارت فون ها دیگر فقط برای مکالمه به کار نمی روند؛ دستیارهای هوشمندی که با صدا کنترل می شوند، مانند سیری از اپل، اسیستنت از گوگل، کورتانا از مایکروسافت، همگی در تلفن های همراه جدید به صورت پیش فرض حضور دارند و از آنها برای جستجوی اینترنتی، تنظیم یادآورها، و تعیین قرارهای ملاقات استفاده می کنیم.

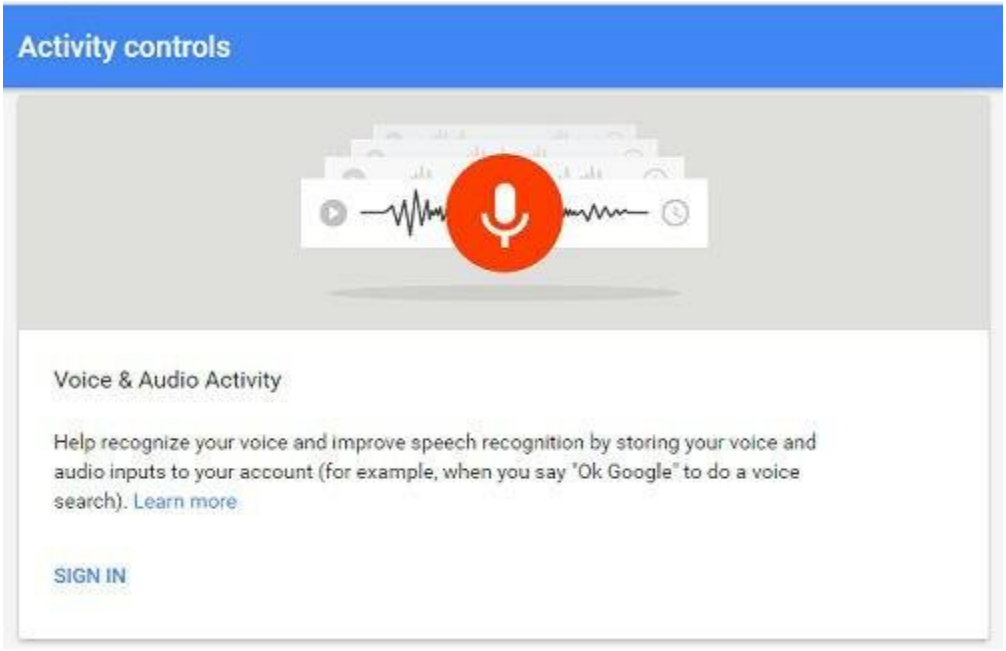
در مقابل، اکثر اپلیکیشن ها و بازی ها نیز هنگام نصب، درخواست دسترسی به میکروفون را از کاربر دارند. با این تفاسیر، آیا می توان متوجه شد که چه زمانی از میکروفون استفاده می شود؟ یا در صورت فعال شدن میکروفون، آیا داده های ضبط شده از طریق اینترنت به سرورهای خاصی منتقل می گردند یا خیر؟

مایکل دی موی سرپرست بخش محرمانگی داده در مرکز دموکراسی و تکنولوژی (CDT) در این رابطه می گوید:

اسمارت فون در واقع دیوایس ردیابی و شنود کوچکی به شمار می رود، ولی اکثر ما چنین دیدی نسبت به آن نداریم، چون دستگاه شخصی بی آزاری به نظر می آید که همه جا همراهمان است و حتی هنگام خواب نیز در کنارمان قرار دارد.

واقعیت این است که موبایل، اطلاعات گسترده ای را از کاربر خود و محیط اطراف جمع آوری می کند و در این میان داده های صوتی نقش برجسته ای دارند.

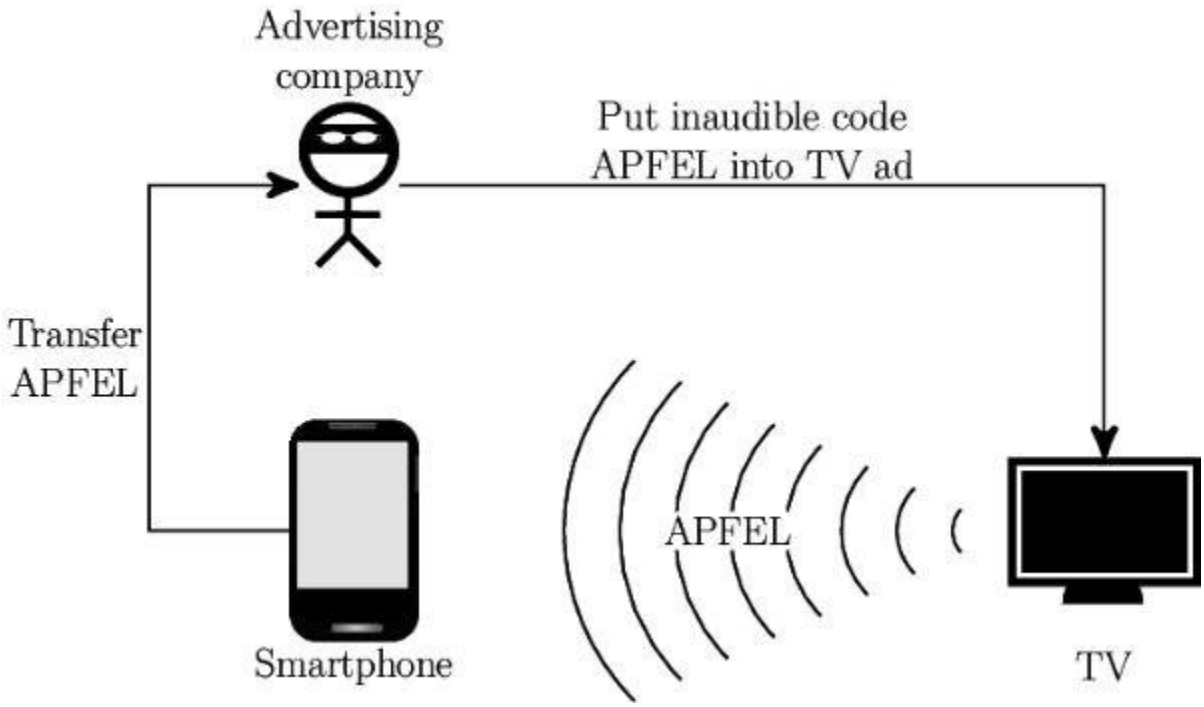
اگر به این اظهار نظر شک دارید و از سرویس های گوگل بهره می گیرید، کافیست به این لینک سری بزنید. با ورود به حساب کاربری خود، می توانید تمامی فعالیت هایتان را در دیوایس ها و خدمات مختلف مشاهده کنید، از کروم گرفته تا جستجو، اندروید، یوتوب و غیره.



جالب تر اینکه با کلیک روی گزینه Filter by date & product و انتخاب Voice & Audio و فشردن دکمه Search می توانید تمام جستجوهای صوتی خود را در سرویس های گوگل مشاهده کنید؛ این محتوای صوتی به طور کامل در سرورهای مربوطه ذخیره شده اند و همین حالا نیز می توانید دوباره آنها را اجرا نمایید.
بسیاری افراد از ذخیره شدن این محتوا اطلاع ندارند. گوگل می گوید رویکردی شفاف در این رابطه دارد و به افراد اجازه می دهد هر زمان که بخواهند، اطلاعات خودشان را ببینند؛ اما از طرف دیگر، هیچگاه ندیده ایم گوگل به طور رسمی و عمومی اعلام کند این داده ها مستقیماً ذخیره و نگهداری می شوند.
البته در مقایسه با گوگل، بسیاری شرکت های دیگر نیز هستند که حتی اجازه دسترسی کاربر به داده های جمع آوری شده خودشان را نیز نمی دهند، و در نهایت مهم ترین نکته این است که ما به هیچ وجه نمی دانیم کمپانی های مختلف با این اطلاعات چه کار می کنند.

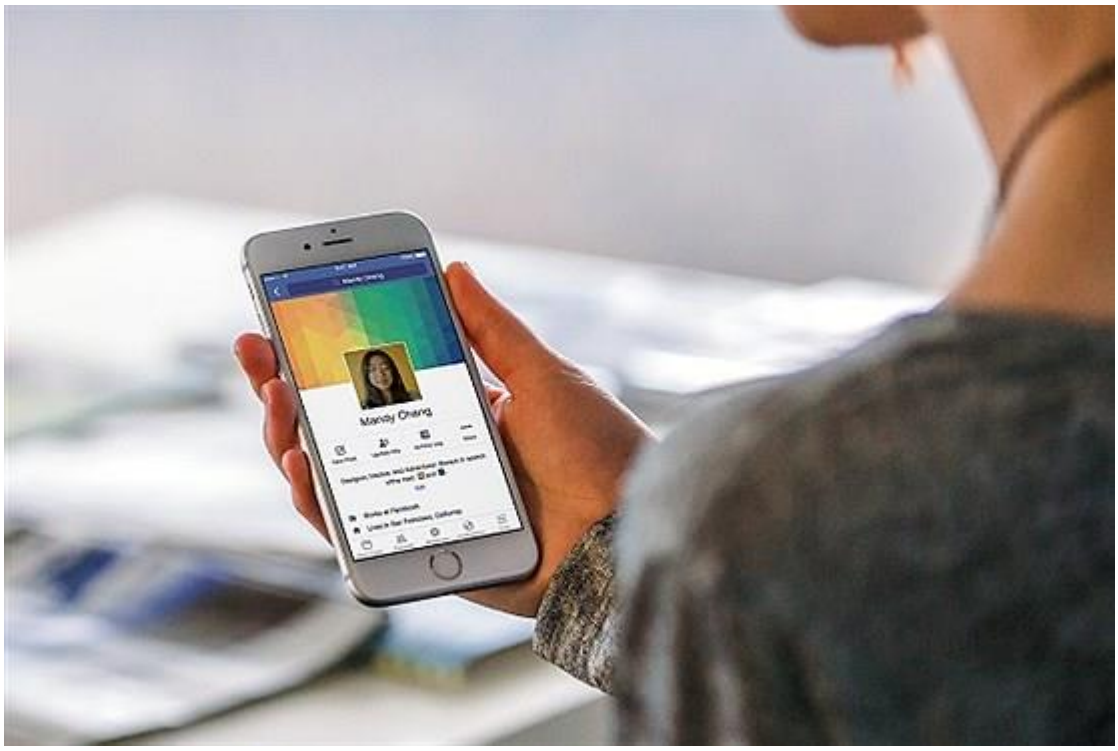
می توان حدس زد حداقل برای یک بار، اطلاعات ضبط شده توسط یک انسان گوش داده می شود، و در نهایت الگوریتم های اختصاصی روی آنها پیاده سازی و اجرا می گردد تا الگوهای ویژه را تشخیص داده و جزئیات سودمندی در مورد رفتارها و علائق کاربر به دست آید.
داده های صوتی همه چیز را فاش می سازند. نویزهای محیطی می توانند نشان دهند که در اتاق نشیمن قرار دارید یا در حمام؛ صداهای پس زمینه، افراد حاضر در محل و در کنار شما را مشخص می سازند؛ حتی استفاده از میکروفون برای تعیین سطح نویز فضای اطراف می تواند زمانی که به خواب رفته اید را به شرکت مربوطه نشان دهد.
دی موی در این رابطه می گوید:
اگر تصور می کنید صحبت های مهم و ارزشمندی نمی گویید و بنابراین نیازی به نگرانی ندارید، اشتباه می کنید. داده های صوتی با انواع و اقسام اطلاعات دیگر ترکیب می شوند و با کاوش درون آنها، می توان تصویری کامل و جامع از شما به دست آورد.
فناوری های مورد استفاده در این حوزه خیلی عجیب و غریب نیستند. در واقع هم اکنون بیشتر آنها با دیگر تکنولوژی های مرتبط در تعامل بوده و دائماً با یکدیگر به تبادل اطلاعات می پردازند.

سال گذشته CDT در مورد سرویس جدیدی به نام SilverPushبه کمیسیون تجارت فدرال (FTC) هشدار داد. در این فناوری از پیام های صوتی خاص برای ردیابی فعالیت های افراد در دیوایس های مختلف استفاده می شود.
به عنوان مثال تلویزیون در حین پخش پیام های بازرگانی، نوعی محتوای صوتی مخفی را نیز پخش می کند که توسط گوش انسان قابل شناسایی نیست، اما موبایل به راحتی آن را تشخیص می دهد. بدین ترتیب، شرکت مربوطه می تواند مالک مشترک موبایل و تلویزیون را بشناسد.
طی سالیان اخیر، شرکت های تبلیغاتی به راهکارها و تکنولوژی های مختلفی متوسل شده اند تا دیوایس های مرتبط با یکدیگر را شناسایی کنند، زیرا بدین ترتیب می توانند فعالیت های افراد را ردیابی کرده و تبلیغات را به صورت هدفمند برای آنها پخش نمایند.



با این حال، چندان دور از ذهن نیست که چنین فناوری هایی از سوی دیگر شرکت ها و نهادهای خصوصی، دولتی یا جاسوسی به کار گرفته شود؛ کافیست پیام مخفی خاصی از طریق تلویزیون پخش شود تا تمامی موبایل های موجود در اتاق شناسایی شده و هویت کل گروه حاضر مشخص گردد.
اگر نگرانید که موبایلتان به هر آنچه می گویید گوش می دهد، باید بدانید تنها نیستید. اینترنت پر است از داستان هایی در مورد استراق سمع دیجیتال .افراد زیادی احساس می کنند صحبت هایشان در نزدیکی تلفن های همراه برای ارائه تبلیغات هدفمند به کار می رود.

تابستان سال گذشته، پس از اینکه فیسبوک به استراق سمع از طریق اپلیکیشن خود محکوم شد، بیانیه کوتاه زیر را منتشر ساخت:
فیسبوک از میکروفون موبایل شما برای ارائه تبلیغات یا تغییر آنچه در فیدهای خبری می بینید، بهره نمی گیرد. ما تنها در صورتی به میکروفون دسترسی داریم که شما اجازه داده باشید، و از ویژگی هایی استفاده کنید که به دریافت صوت نیاز داشته باشند.
اما چرا این گمان در بین کاربران به وجود آمد که فیسبوک به صحبت های آنها گوش کرده و تبلیغات را بر اساس آنها تغییر می دهد؟ پروفسور جیسون هونگ از دانشکده علوم کامپیوتر دانشگاه کارنگی ملون می گوید:
دو توضیح وجود دارد: یا این وضعیت کاملاً تصادفی بوده، یا اینکه کاربران مورد بحث ابتدا به وب سایتی رفته و موضوع یا کالایی را مشاهده نموده، سپس در مورد آن با دوستان خود گفتگو کرده اند. فیسبوک با وب سایت ها و پایگاه های خبری متعددی در جهان در ارتباط است و اطلاعات مربوط به محتوایی که کاربران می بینند را دریافت می دارد، بنابراین به راحتی می تواند تبلیغات مرتبط به آنها را به نمایش درآورد.
او در ادامه گفت «تا جایی که ما اطلاع داریم، میکروفون به صورت دائم شنود نمی گردد.«



به هر حال از بیانیه فیسبوک مشخص نمی شود که آنها با اطلاعات و داده های صوتی افراد چه کار می کنند، اما می دانیم کل مدل کسب و کار این کمپانی بر جمع آوری داده و تبلیغات فوق العاده هدفمند بنا نهاده شده. شاید تصور کنید دریافت تبلیغات اختصاصی نتیجه منفی ندارد، اما ماجرا پیچیده تر از اینهاست.

دی موی می گوید:
زمانی که از خدماتی به رایگان استفاده می کنید، مطمئن باشید بهای آن را با اطلاعات خود می پردازید، و در این میان مشخص نیست که کدام سمت قضیه بر دیگری می چربد. اینترنتی که من می بینیم با آنچه شما می بینید، تفاوتی اساسی دارد. محتوایی که برای هرکدام از ما به نمایش در می آید، کاملاً به اطلاعات جمع آوری شده از ما وابسته است.
بر این اساس، افرادی که به گروه های نژادی مختلف تعلق دارند، آگهی های شغلی متفاوتی را دریافت می کنند، یا تبلیغ وام های پر بهره برای اشخاصی که در وضعیت مالی نامناسبی گرفتار آمده اند، به نمایش در می آید.
چه کاری از دستمان بر می آید؟
با معرفی خدماتی همچون سیری یا گوگل اسیستنت، موبایل شما همواره در جستجوی کلمه کلیدی مربوطه به صداهای

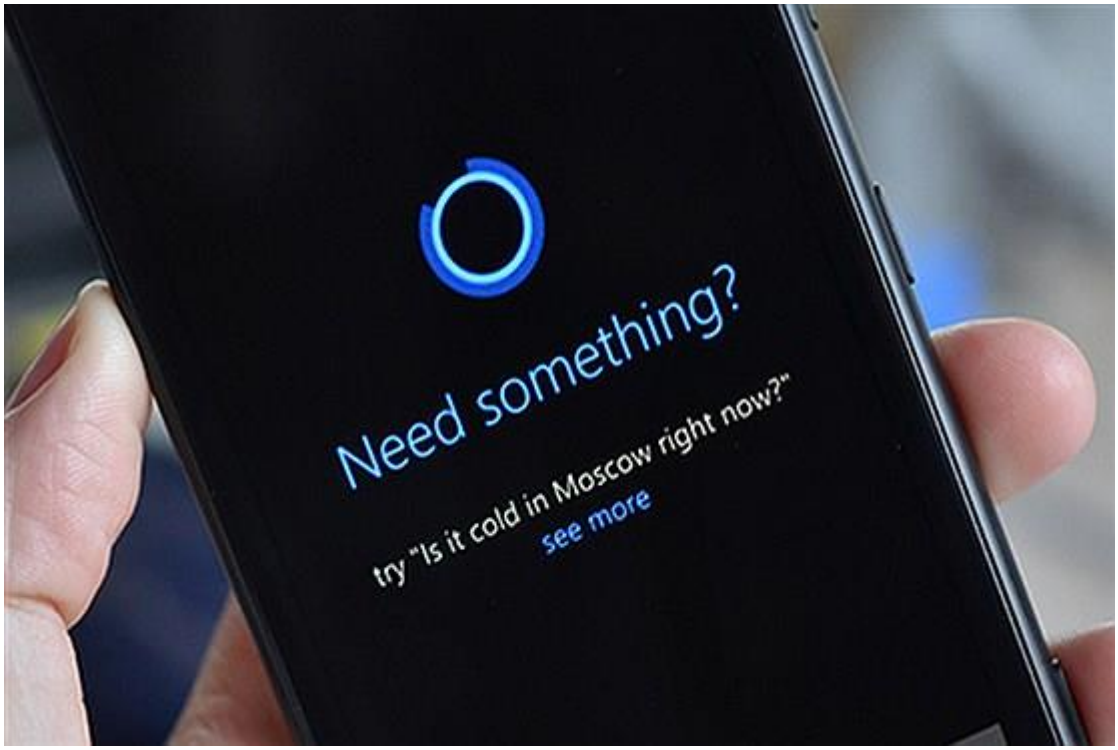
اطرافش گوش می دهد. البته طبق ادعای سازندگان، پردازش داده تا این مرحله به صورت محلی و درون خود موبایل صورت می گیرد و هیچ اطلاعاتی به بیرون منتقل نمی گردد.
پس از اینکه عبارت OK Google یا Hey Siri را بر زبان جاری سازید، صحبت های شما به طور کامل ضبط شده و به سرورهای مربوطه منتقل می گردد.
اگر می خواهید مانع از گوش سپردن همیشگی موبایل به محیط اطراف شوید، به راحتی می توانید از بخش تنظیمات گزینه مورد نظر را غیر فعال سازید. مثلاً در سیستم عامل اندروید به بخش تنظیمات، قسمت گوگل، گزینه Search & Now و سپس Voice رفته و در آنجا OK Google Detection را خاموش کنید.
هونگ در این رابطه می گوید:
شرکت های بزرگ و معتبر، معمولاً در اینگونه موارد بسیار شفاف عمل می کنند، چون کمیسیون تجارت فدرال و دیگر سازمان های دولتی به طور دائم آنها را زیر نظر داشته و در صورت مخفی کاری، جریمه های سختی را برایشان در نظر خواهند گرفت.
همچنین نهادهای خصوصی نیز تحقیقات متعددی در این رابطه انجام داده و به آنالیز خط به خط این اپلیکیشن ها می پردازند.

با این حساب به نظر نمی رسد با استراق سمع مخفیانه دائمی از سوی موبایل ها روبرو باشیم، اما هنوز هم مشخص نیست از داده های ضبط شده کاربر چه استفاده ای می شود. حتی اگر وقت بگذارید و متن سیاست های محرمانگی شرکت ها را مطالعه کنید، کاری که تقریباً هیچکس انجام نمی دهد، باز هم چیز زیادی دستگیرتان نمی شود. هونگ می گوید:
در واقع هیچ فردی متن های Privacy Policy را مطالعه نمی کند، و در صورتی که به آنها بگویید چه حجم وسیعی از داده های آنها به صورت آنلاین جمع آوری می شود، متعجب می شوند.
اما در این میان، اپلیکیشن های دیگری نیز وجود دارند که با اهداف نامشخص به میکروفون دستگاه دسترسی دارند، و می توانند بدون اطلاع کاربر به صحبت هایش گوش دهند. هونگ اضافه می کند:
با فعال شدن GPS حداقل آیکن کوچکی را بالای صفحه می بینیم و مشخص می شود که اپلیکیشنی از سرویس مکان یابی استفاده می کند، اما در مورد میکروفون و دیگر حسگرها چنین وضعیتی وجود ندارد.

بهترین راهکار در این زمینه، نصب نکردن اپلیکیشن های متفرقه و اجازه ندادن به آنها برای دسترسی به میکروفون است .
هونگ پیشنهاد می کند:
اولین پنگوئنی نباشید که در آب می پرد. تا اپلیکیشنی منتشر شد، سریع به سراغش نروید و نصبش نکنید. حداقل یکی دو هفته صبر پیشه نمایید. گوگل و اپل روش های خوبی برای یافتن و حذف اپلیکیشن های مخرب دارند، اما باید چند روز به آنها مهلت بدهید.
همچنین در نسخه های جدید سیستم عامل اندروید، می توانید برای اطمینان از مجوزهای دسترسی به بخش تنظیمات و منوی Privacy and Safety بروید. در اینجا بخشی به نام App Permissions وجود دارد که دسترسی به امکانات مختلف سخت افزاری را در بین برنامه های مختلف نشان می دهد و با کمی کنکاش، می توانید موارد مشکوک را شناسایی کنید.
بالاخره نگران باشیم یا نه؟
در مقایسه با دیگر تکنیک ها و ترفندهای مورد استفاده برای ردیابی فعالیت آنلاین کاربران، فضای داده های صوتی هنوز به اندازه کافی پیشرفت نکرده و توسعه نیافته، اما با توجه به اینکه هر روز دیوایس های بیشتری با قابلیت شنیداری عرضه می شوند، نگرانی نیز در این حوزه افزایش می یابد.

هونگ معتقد است:
این روزها موبایل، تلویزیون هوشمند، اسپیکرهای خانگی و حتی اسباب بازی ها، همگی دائماً به محیط اطراف خود گوش می

دهند، و به زودی تشخیص مسیر این داده ها بیش از حد دشوار خواهد شد، چون هر کمپانی می خواهد به سرورها و خدمات کلاود خود متصل شود.
این قابلیت ها، شرایط دشواری را برای کاربران و حتی متخصصین حوزه امنیت پیش می آورد، و درک اینکه واقعاً چه اتفاق در حال وقوع است، ناممکن می گردد.
CDTمعتقد است باید قوانین پایه ای برای حفظ محرمانگی و حریم شخصی و تضمین امنیت کاربران وجود داشته باشد، ضمن اینکه کمپانی ها نیز ملزم گردند که تا جای ممکن اطلاعات کمتری را از افراد جمع آوری کنند. آنها واقعاً به این حجم از داده نیاز ندارند، ولی هر آنچه که در اختیارشان قرار گیرد را جمع می کنند تا شاید در آینده کاربردی برای آن پیدا نمایند.
دی موی اظهار داشت «در جهان واقعی به این عمل شرکت ها، احتکار داده گفته می شود».



ایده اصلی پشت این حرکت، باور عمومیست که می گوید تکنولوژی باعث بهتر شدن زندگی خواهد شد، اما همواره ممکن است اهداف خوب دستخوش تحریف شوند، و در نهایت نمی دانیم که از اطلاعات شخصی ما چه استفاده ای خواهد شد.
در حال حاضر نمی توان تصمیمی آگاهانه گرفت، چون هیچکس نمی داند پشت پرده چه خبر است. بنابراین شاید تنها راه موجود عمل کردن به گفته های دی موی باشد:
اگر از این سرویس ها و خدمات روی موبایل خود استفاده می کنید، در درجه اول باید بدانید دیگر چیزی به اسم حالت شخصی و خصوصی وجود ندارد. سامانه های هوش مصنوعی را به منزله دستیار شخصی یا دوست خود ندانید، همه آنها ابزارهای ردیابی و جمع آوری محتوا هستند.
اپلیکیشن های پیام رسان و شبکه های اجتماعی صرفاً با هدف جمع آوری داده و استفاده تجاری طراحی و عرضه می شوند، پس هیچ وقت به تنظیمات پیش فرض آنها اعتماد نکنید، همه چیز را زیر نظر بگیرید و از حریم شخصی خود محافظت نمایید.