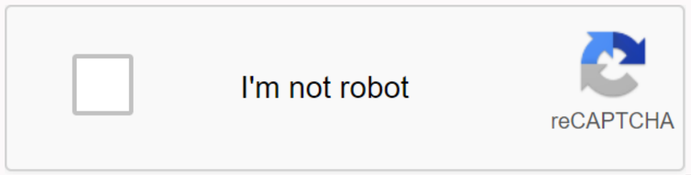


Continue

# Four track app

When it comes to websites, we have increasingly sophisticated methods at our disposal to block ads that sometimes track our wandering around the Internet. However, most of us spend a lot of time in these days in mobile apps that do not have transparency in how we are tracked or sold, nor tools designed to block this behavior. We need to rely on operating system developers, in particular Apple and Google, to announce legitimate practices to developers when it comes to behavioral monitoring, requesting personal information and transferring data to remote servers. OS manufacturers are also responsible for complying with these requirements. The rules applied are very broad, except for abuses that can be quickly verified by internal reviewers, most often playing out when users and researchers report violations. For example, Apple rules require apps to obtain someone's permission before transferring personal data and should describe how and where the data will be used. Apple does not control these rules by intercepting network connections or by requiring remote database auditing. (The company declined to interview this story.) When applications ask for permits, it's not really done easily, says Franziska Roesner, an associate professor of computer science and engineering at the University of Washington who researches computer security and privacy. iOS doesn't necessarily know if the app benefits from using your location, so they ask the user, she says. Apple must rely on the developer's disclosure of what is being done with that location data. Some roesner works trying to reconcile the purpose of the application and the interface elements with the type of release that is requested so that the request is not misused. Many developers embed features in the form of third-party analytics packages and ad technology code, which seem to be related to harmless user information with information collected from other sources. So even if the data sent from the app looks benign separately, it can uniquely identify the user or be used for purposes that the developer does not know about. Developers usually did not audit this code and could not detail what it was doing. A recent case study was a program by Meitu, a company of the same name that applies anime-style photos of people's faces. The free app has been available in China for years, but the English version went viral. When security researchers examined the software accessories, they found that it was loaded with analysis and advertising packages, only some of which were linked to the work code, and that it requested numerous permissions for Android and iOS.Meitu told me at the time that kerfuffle it included a certain geographic location and app-checking code to meet the requirements of the advertising network in China , where jailbroken devices can be used to deceive advertisers , and advertisers may require their messages to be geofenced to appear in certain regions. Apple confirmed that the program was and remains in compliance. This visualization of the Haystack project provides a stark picture of the extent of mobile connections with other countries, benign or otherwise. The U.S. Federal Trade Commission may not intervene on behalf of consumers unless there are allegations that the company violated the privacy law, including COPPA (Child Online Privacy Protection Rule), or that the company has filed a statement about what it is doing and lied about. The FTC's website has a page about your claims and results regarding data privacy, including those related to the programs. So what does the user do? Academics are all about it. The two complementary efforts that continue to cooperate will increase the control of those who have mobile devices to monitor app connections, help uncover bad actors and poorly designed private data security transfers, and allow you to launder or completely block private information. Listening on your behalf Team, led by Northeastern University's Dave Choffnes, associate professor at his College of Computer and Information Sciences, has developed ReCon, a sort of virtual private network (VPN) for personally identifiable data (AII field jargon). Unlike a regular VPN that protects data in a secure tunnel between a user's device and a data center or enterprise server to avoid snoopers, ReCon also uses a VPN connection to act as a scanning proxy server to check all data passing between the smartphone and the rest of the Internet. It works by installing a network profile on iOS or Android, just like regular VPN services. ReCon can fully check the content of unencrypted connections, which is also clear to everyone on a public Wi-Fi network or other network failoapoints when vpn is not used. Choffnes and his colleagues found some surprising practices. For example, he says GrubHub accidentally sent user passwords to Crashlytics, a Google-owned company that helps developers accurately identify code failures. When informed, GrubHub reviewed its code and had Crashlytics delete all related data that contains passwords. The group extracts data from app connections and tries to determine which parts of it are INAI. It is both harder and easier than it may sound. Most data is sent structurally using the API and often in a standard JSON format that groups data into a label (key) and its associated value. However, the team also applies machine learning, allowing it to identify the AI more widely, even if it appears without using any standard structure format or displayed in surprising places. The ReCon project publishes several data from several hundred early users listing the apps, the type of data they transmit, the severity score, whether the developer was informed and when inappropriate behaviour was detected (if indeed it was). For those who have installed the program, ReCon has console that allows you to to block or modify the information you send. For example, a user can block all samples of a particular type of AAI or block all local data sent from a particular app. However, because some applications fail without location coordinates, the team searches for coarsening GPS information instead of completely blocking it. The program subsystem still receives relevant information, but other countries can't pin it to where you are, up to a few meters, notes Choffnes. Of course, examining the flow of data from users themselves puts a massive privacy red flag, which is part of recon evolution. Its developers do not ask for passwords, try to avoid storing outgoing values and check only whether, say, the password is apparently transmitted without encryption. The group ultimately wants to perform distributed machine learning without disseminating users' private or sensitive information, such as the domain they visit. Before it ever gets off the PhoneThe Haystack Project, a collaboration at the International Institute of Computer Science (ICSI) at the University of California, Berkeley, among many academic institutions, begins an Android program that captures data directly at source. (It's not available on iOS yet.) Like ReCon, Haystack Lumen's privacy monitoring program acts as a VPN, but it maneuvers data inside rather than sends it from the device for analysis. Because it's in user control, the app may be authorized to intercept https connections and analyze everything sent between apps and servers. ReCon, sitting outside the device and network, can't, although it can determine the connection went to a certain destination, rough payload size, and connection frequency. The Lumen app monitors what Android apps do with your data. ICSI researcher Narseo Vallina-Rodriguez says that the fact that Lumen does not send data from the device means that its developers need to be careful to set up a smartphone with processing tasks. Currently, the tool measures and reports what programs are doing, although it may offer blocking controls in the future. The program reports on completely anonymised parts of the information so that researchers can understand what personal information is extracted and transmitted. We see tons of things like some programs linking the MAC address to a Wi-Fi access point as a local proxy, says Vallina-Rodriguez. (The MAC address of the base station identifies it uniquely and is used by Apple, Google and other enterprise-operated Wi-Fi local databases.) While certain types of personal data require the app to encourage Android to request user permission, we've found apps and third-party services that somehow use channels without user awareness, says Vallina-Rodriguez. He notes that an Android file that contains various system information information, such as buffer size, may also have unique network identifiers, including an IP address, and which is sent without a user both projects have friendly competition and cooperation plans. The effort is likely to remain separate, but add dimensions or link data to get a bigger picture of app behavior. And the ReCon team would like to create a software network device, Raspberry Pi, that works as a sniffer or proxy or firmware network router, to let someone see the interaction on all network devices, especially Internet of Things software that has all sorts of privacy and security issues in their own kinds. Both ReCon and Lumen are seeking more funds to improve projects and make them viable for large-scale consumer deployment. [Photo: Unsplash user Oliur Rahman] As informative as RecCon and Liumen are, what apps do with our data remains an unbreakable theme. Many privacy experts and researchers point out that dense legal documents are used to define disclosure, not to be linked to verifiable individual elements that can be verified by the software (or people). Privacy disclosure is almost impossible for typical users to analyze, and even lawyers trained in the field may need to devote hours of effort to confirm whether they are being complied with. Choffnes notes: The privacy policy, which is what they claim they will do, tends to be written in a very broad way, which gives them wiggle room to avoid running afoul of the FTC's deceptive business practices rules. The more vague they are, the less chances they failed to disclose the information they grab. Until you reveal it, almost everything happens, says Stacey Gray, policy adviser at the Privacy Forum, a group that pulls out industries, consumer advocates and other stakeholders. If you are not deceptive in your policy, you can do almost anything. When things become particularly murky, she says, is where the use of data is unexpected, inappropriate, or sensitive. The restaurant search app may ask for a location to make recommendations around you. However, if it also sells your location as an income stream without disclosing, it's unexpected or inappropriate. You don't give up that right intentionally, but it can easily be hidden in the miasma of legal terminology. Gray also cites unintended consequences when an app developer and a third-party ad technology network may operate through reasonable terms, but an unrelated party may violate privacy. She cites a situation in May 2016 when the company said it could use advertising targeting to find women in Planned Parenthood clinics and serve them with ads about anti-abortion religious counseling services. This action may be legitimate, but certainly undesirable for related users, ad networks, or publishers. (The service operator said that it can put ads on Facebook pages; Facebook has stated that it cannot find any posts about him or his ads.) The same conflicts that led to the ad blocking wars, it is unlikely that business models are behind mobile apps ensure greater transparency, making research for ReCon and Lumen even more important. As Choffnes explains, most of the progress in this field comes from academia; these are things that are clear in the public interest and would not come out of the business community, because their incentives are balanced to promote this behaviour, not consumer privacy. [Correction, published on 5/31/17: An earlier version of this story incorrectly reported Dave Choffnes's academic membership.] conscience.]