Additions to the Malware Section

These are all the malware items that have been added to this directory since 2018, in reverse chronological order. (In some cases, the latest reference was updated after the item was added.)

Added: 2024-01-18 — Latest reference: 2024-01-18

UHD Blu-ray denies your freedom — The anatomy of an Authoritarian Subjugation System

Added: 2022-08-22 — Latest reference: 2022-07-26

UEFI makes computers vulnerable to advanced persistent threats that are almost impossible to detect once installed...

- Added: 2024-07-31 — Latest reference: 2024-05-24

  Spotify sold a music streaming device but they no longer support it. Due to its proprietary nature, it can no longer be updated or even used. Users requested Spotify to make the software that runs on the device libre, and Spotify refused, so these devices are now e-waste. Spotify is now offering refunds to save the purchasers from losing money on these products, but this wouldn't prevent the products from being e-waste, and wouldn't save users from being jerked around by Spotify. This is an example of how software that is not free controls the user instead of the user controlling the software. It is also an important lesson for us to insist the software in a device be libre before we buy it.

- Added: 2024-05-23 — Latest reference: 2024-03-15

  Microsoft is using malware tactics to get users to switch to their web browser, Microsoft Edge, and their search engine, Microsoft Bing. When users launch the Google Chrome browser Microsoft injects a pop up advertisement in the corner of the screen advising users to switch to Bing. Microsoft also imported users Chrome browsing data without their knowledge or consent.

- Added: 2024-04-07 — Latest reference: 2024-03-11

  GM is spying on drivers who own or rent their cars, and give away detailed driving data to insurance companies through data brokers. These companies then analyze the data, and hike up insurance prices if they think the data denotes “risky driving.” For the car to make this data available to anyone but the owner or renter of the car should be a crime. If the car is owned by a rental company, that company should not have access to it either.

- Added: 2024-02-22 — Latest reference: 2023-12-23

  Surveillance cameras put in by government A to surveil for it may be surveilling for government B as well. That's because A put in a product made by B with nonfree software.

  (Please note that this article misuses the word “hack” to mean “break security.”)

- Added: 2024-01-20 — Latest reference: 2023-11-10

  Microsoft has been annoying people who wanted to close the proprietary program OneDrive on their computers, forcing them to give the reason why they were closing it. This prompt was removed after public pressure.

  This is a reminder that angry users still have the power to make developers of proprietary software remove small annoyances. Don't count on public outcry to make them remove more profitable malware, though. Run away from proprietary software!

- Added: 2024-01-03 — Latest reference: 2023-12-06

  Newag, a Polish railway manufacturer, puts DRM inside trains to prevent third-party repairs.

    - The train's software contains code to detect if the GPS coordinates are near some third party repairers, or the train has not been running for some time. If yes, the train will be “locked up” (i.e. bricked). It was also possible to unlock it by pressing a secret combination of buttons in the cockpit, but this ability was removed by a manufacturer's software update.
    - The train will also lock up after a certain date, which is hardcoded in the software.
    - The company pushes a software update that detects if the DRM code has been bypassed, i.e. the lock should have been engaged but the train is still operational. If yes, the controller cabin screen will display a scary message warning about “copyright violation”.
- Added: 2024-01-03 — Latest reference: 2023-11-30

  x86 and ARM based computers shipped with UEFI are potentially vulnerable to a design omission called LogoFAIL. A cracker can replace the BIOS logo with a fake one that contains malicious code. Users can't fix this omission because it is in the nonfree UEFI firmware that users can't replace.

- Added: 2024-01-03 — Latest reference: 2023-11-08

  Recent autos offer a feature by which the drivers can connect their snoop-phones to the car. That feature snoops on the calls and texts and gives the data to the car manufacturer, and to the state.

  A good privacy law would prohibit cars recording this data about the users' activities. But not just *this* data—lots of other data too.

- Added: 2023-12-30 — Latest reference: 2018-09-17

  Clash Royale is an online game with an “optimized” *gacha* system that makes it very addictive for players, and very profitable for its developers.

- Added: 2023-12-26 — Latest reference: 2023-09-05

  Google Nest snooper/surveillance cameras are always tethered to Google servers, record videos 24/7, and are subscription-based, which is an injustice to people who use them. The article discusses the rise in prices for “plans” you can buy from Google, which include storing videos in the “cloud”—another word for someone else's computer.

- Added: 2023-12-20 — Latest reference: 2023-11-30

  To block non-Apple repairs, Apple encodes the iMonster serial number in the original parts. This is called “parts pairing”. Swapping parts between working iMonsters of the same model causes malfunction or disabling of some functionalities. Part replacement may also trigger persistent alerts, unless it is done by an Apple store.

- Added: 2023-12-09 — Latest reference: 2023-11-09

  Samsung's Push Service proprietary app sends notifications to the user's phone about “updates” in Samsung apps, including the Gaming Hub, but these updates only sometimes have to do with a new version of the apps. Many times, the notifications from Gaming Hub are simply ads for games that they think the user should install based on the data collected from the user. Most importantly, it cannot be permanently disabled.

- Added: 2023-12-09 — Latest reference: 2023-11-07

  Chamberlain Group blocks users from using third-party software with its garage openers. This is an intentional attack on using free software. The official garage opener proprietary mobile app is now also infested with ads, including up-selling its other services and devices.

- Added: 2023-12-08 — Latest reference: 2023-11-10

  In Australia, people assume that “smart” means “tethered.” When people's ISP goes down, all the tethered devices become useless.

  That's in addition to the nasty things tethered devices do when they are “functioning” normally—such as snoop on the commands sent to the device and the results they report.

Smart *users* know better than to accept tethered devices.

- Added: 2023-11-20 — Latest reference: 2023-08-22

  Some Bambu Lab 3D printers were reported to start printing without user's consent, as a result of a malfunction of the servers to which they were tethered. This caused significant damage.

- Added: 2023-11-19 — Latest reference: 2023-08-08

  The Yandex company has started to give away Yango taxi ride data to Russia's Federal Security Service (FSB). The Russian government (and whoever else receives the the data) thus has access to a wealth of personal information, including who traveled where, when, and with which driver. Yandex claims that it complies with European regulations for data collected in the European Economic Area, Switzerland or Israel. But what about the rest of the world?

- Added: 2023-11-15 — Latest reference: 2023-09-06

  In an article from Mozilla, every car brand they researched has failed their privacy tests. Some car manufacturers explicitly mention that they collect data which includes “sexual activities” and “genetic information”. Not only collecting any of such data is a huge privacy violation in the first place, some companies assume drivers and passengers' consent before they get in the car. Notably, Tesla threatens that the car may be “inoperable” if the user opts out of data collection.

- Added: 2023-11-04 — Latest reference: 2022-09-22

  Windows 11 Home and Pro now require internet connection and a Microsoft account to complete the installation. Windows 11 Pro had an option to create a local account instead, but the option has been removed. This account can (and most certainly will) be used for surveillance and privacy violations. Thankfully, a free software tool named Rufus can bypass those requirements, or help users install a free operating system instead.

- Added: 2023-11-02 — Latest reference: 2019-12-11

  As tech companies add microphones to a wide range of products, including refrigerators and motor vehicles, they also set up transcription farms where human employees listen to what people say and tweak the recognition algorithms.

- Added: 2023-10-29 — Latest reference: 2023-09-27

  Philips Hue, the most ubiquitous home automation product in the US, is planning to soon force users to log in to the app server in order to be able to adjust a lightbulb, or use other functionalities, in what amounts to a massive user-tracking data grab.

- Added: 2023-07-15 — Latest reference: 2023-07-04

  Driverless cars in San Francisco collect videos constantly, using cameras inside and outside, and governments have already collected those videos secretly.

  As the Surveillance Technology Oversight Project says, they are “driving us straight into authoritarianism.” We must regulate *all* cameras that collect images that can be used to track people, to make sure they are not used for that.

- Added: 2023-07-15 — Latest reference: 2023-05-30

  Some employers are forcing employees to run “monitoring software” on their computers. These extremely intrusive proprietary programs can take screenshots at regular intervals, log keystrokes, record audio and video, etc. Such practices have been shown to deteriorate employees' well-being, and trade unions in the European union have voiced their concerns about them. The requirement for employee's consent, which exists in some countries, is a sham because most often the employee is not free to refuse. In short, these practices should be abolished.

- Added: 2023-07-08 — Latest reference: 2023-06-12

  Edge sends the URLs of images the user views to Microsoft's servers by default, supposedly to “enhance” them. And these images may end up on the NSA's servers.

Microsoft claims its nonfree browser sends the URLs without identifying you, which cannot be true, since at least your IP address is known to the server if you don't take extra measures. Either way, such enhancer service is unjust because any image editing should be done on your own computer using installed free software.

The article describes how to disable sending the URLs. That makes a change for the better, but we suggest that you instead switch to a freedom-respecting browser with additional privacy features such as IceCat.

- Added: 2023-05-29 — Latest reference: 2023-05-04

Controlling Honeywell internet thermostats with the dedicated app has proven unreliable, due to recurrent connection issues with the server these thermostats are tethered to.

- Added: 2023-05-18 — Latest reference: 2023-05-10

HP delivers printers with a universal back door, and recently used it to sabotage them by remotely installing malware. The malware makes the printer refuse to function with non-HP ink cartrides, and even with old HP cartridges which HP now declares to have “expired.” HP calls the back door “dynamic security,” and has the gall to claim that this “security” protects users from malware.

If you own an HP printer that can still use non-HP cartridges, we urge you to disconnect it from the internet. This will ensure that HP doesn't sabotage it by “updating” its software.

Note how the author of the Guardian article credulously repeats HP's assertion that the “dynamic security” feature protects users against malware, not recognizing that the article demonstrates it does the opposite.

- Added: 2023-04-29 — Latest reference: 2023-02-14

Microsoft is remotely disabling Internet Explorer, forcibly redirecting users to Microsoft Edge.

Imposing such change is malicious, and the fact that the redirection is from one unjust program (IE) to another unjust program (Edge) does not excuse it.

- Added: 2023-04-29 — Latest reference: 2023-01-19

Microsoft released an “update” that installs a surveillance program on users' computers to gather data on some installed programs for Microsoft's benefit. The update is rolling out automatically, and the program runs “one time silently.”

- Added: 2023-04-25 — Latest reference: 2023-02-28

Volkswagen tracks the location of every driver, and sells that data to third-parties. However, it refuses to use the data to implement a feature for the benefit of its customers unless they pay extra money for it.

This came to attention and brought controversy when Volkswagen refused to locate a car-jacked vehicle with a toddler in it because the owner of the car had not subscribed to the relevant service.

- Added: 2023-04-25 — Latest reference: 2022-07-14

BMW is now luring British customers into paying for the built-in heated-seat feature of their new cars on a subscription basis. People also have the option to buy the feature when they are paying for the car, but those who bought a used car have to pay BMW extra money to remotely enable the heated seats. This is probably done by BMW accessing a back door in the car software.

- Added: 2023-04-25 — Latest reference: 2022-07-04

A bug in Tesla cars software lets crackers install new car keys, unlock cars, start engines, and even prevent real owners from accessing their cars.

A cracker even reported that he was able to disable security systems and take control of 25 cars.

Please note that these articles wrongly use the word “hacker” instead of cracker.

- Added: 2023-04-12 — Latest reference: 2023-04-06

Tesla cars record videos of activity inside the car, and company staff can watch those recordings and copy them. Or at least they were able to do so until last year.

Tesla may have changed some security functions so that this is harder to do. But if Tesla can get those recordings, that is because it is planning for some people to use them in some situation, and that is unjust already. It should be illegal to make a car that takes photos or videos of the people in the car—or of people outside the car.

- Added: 2023-04-04 — Latest reference: 2023-04-03

  The Pinduoduo app snoops on other apps, and takes control of them. It also installs additional malware that is hard to remove.

- Added: 2023-04-04 — Latest reference: 2023-04-01

  GM is switching to a new audio/video system in its cars in order to collect complete information about what people in the car watch or listen to, and also how they drive.

  The new system for navigation and “driving assistance” will be tethered to various online dis-services, and GM will snoop on everything the users do with them. But don't feel bad about that, because some of these subscriptions will be gratis for the first 8 years.

- Added: 2023-03-15 — Latest reference: 2023-02-08

  As soon as it boots, and without asking any permission, Windows 11 starts to send data to online servers. The user's personal details, location or hardware information are reported to Microsoft and other companies to be used as telemetry data. All of this is done is the background, and users have no easy way to prevent it—unless they switch the computer offline.

- Added: 2023-01-29 — Latest reference: 2023-01-23

  A dispute between Blizzard and one of its partners caused World of Warcraft to go offline in China. The shutdown may not be permanent, but even if it is not, the fact that a business disagreement can stop all users in China from playing the game illustrates the injustice of requiring the use of a specific server.

  We expect that users must pay to use that server, but whether that is the case is a side issue. Even if use of that server is gratis, the harm comes from the fact that the program doesn't allow people to make and use other servers for that job.

  Let's hope game fans in China learn the importance of rejecting nonfree games.

- Added: 2023-01-08 — Latest reference: 2022-11-30

  Hackers discovered dozens of flaws in the security (in the usual narrow sense) of many brands of automobiles.

  Security in the usual narrow sense means security against unknown third parties. We are more concerned with security in the broader sense—against the manufacturer as well as against unknown third parties. It is clear that each of these vulnerabilities can be exploited by the manufacturer too, and by any government that can threaten the manufacturer enough to compel the manufacturer's cooperation.

- Added: 2022-12-13 — Latest reference: 2022-11-14

  The iMonster app store client programs collect many kinds of data about the user's actions and private communications. “Do not track” options are available, but tracking doesn't stop if the user activates them: Apple keeps on collecting data for itself, although it claims not to send it to third parties.

  Apple is being sued for that.

- Added: 2022-12-05 — Latest reference: 2022-10-14

  The Microsoft Office encryption is weak, and susceptible to attack.

Encryption is a tricky field, and easy to mess up. It is wise to insist on encryption software that is (1) free software and (2) studied by experts.

- Added: 2022-12-03 — Latest reference: 2022-11-30

  Obeying a demand by the Chinese government, Apple restricted the use of AirDrop in China. It imposed a ten-minute time limit during which users can receive files from non contacts. This makes it nearly impossible to use AirDrop for its intended purpose, which is to exchange files with strangers between iMonsters in physical proximity. This happened after it became known that dissenters were using the app to distribute digital anti-government fliers anonymously.

- Added: 2022-11-26 — Latest reference: 2022-10-11

  Xiaomi provides a tool to unlock the bootloader of Xiaomi smartphones and tablets, but this requires creating an account on the company's servers, i.e. providing your phone number. This is the price you have to pay for “legally” running a free software operating system on Xiaomi devices. But the manufacturer retains control of the unlocked device through a backdoor in the bootloader —the same backdoor that was remotely used to unlock it.

- Added: 2022-09-21 — Latest reference: 2022-09-00

  B-CAS [1] is the digital restrictions management (DRM) system used by Japanese TV broadcasters, including NHK (public-service TV). It is sold by the B-CAS company, which has a de-facto monopoly on it. Initially intended for pay-TV, its use was extended to digital free-to-air broadcasting as a means to enforce restrictions on copyrighted works. The system encrypts works that permit free redistribution just like other works, thus denying users their nominal rights.

  On the client side, B-CAS is typically implemented by a card that plugs into a compatible receiver, or alternatively by a tuner card that plugs into a computer. Beside implementing drastic copying and viewing restrictions, this system gives broadcasters full power over users, through back doors among other means. For example:

  - It can force messages to the user's TV screen, and the user can't turn them off.
  - It can collect viewing information and send it to other companies to take surveys. Until 2011, user registration was required, so the viewing habits of each customer were recorded. We don't know whether this personal information was deleted from the company's servers after 2011.
  - Each card has an ID, which enables broadcasters to force customer-specific updates via the back door normally used to update the decryption key. Thus pay-TV broadcasters can disable decryption of the broadcast wave if subscription fees are not paid on time. This feature could also be used by any broadcaster (possibly instructed by the government) to stop certain persons from watching TV.
  - As the export of B-CAS cards is illegal, people outside Japan can't (officially) decrypt the satellite broadcast signal that may spill over to their location. They are thus deprived of a valuable source of information about what happens in Japan.

  These unacceptable restrictions led to a sort of cat-and-mouse game, with some users doing their best to bypass the system, and broadcasters trying to stop them without much success: cryptographic keys were retrieved through the back door of the B-CAS card, illegal cards were made and sold on the black market, as well as a tuner for PC that disables the copy control signal.

  While B-CAS cards are still in use with older equipment, modern high definition TVs have an even nastier version of this DRM (called ACAS) in a special chip that is built into the receiver. The chip can update its own software from the company's servers, even when the receiver is turned off (but still plugged into an outlet). This feature could be abused to disable stored TV programs that the power in place doesn't agree with, thus interfering with free speech.

  Being part of the receiver, the ACAS chip is supposed to be tamper-resistant. Time will tell…

  [1] We thank the free software supporter who translated this article from Japanese, and shared his experience of B-CAS with us. (Unfortunately, the article presents DRM as a good thing.)

- Added: 2022-09-20 — Latest reference: 2022-08-24

  A security researcher found that the iOS in-app browser of TikTok injects keylogger-like JavaScript code into outside web pages. This code has the ability to track all users' activities, and to retrieve

any personal data that is entered on the pages. We have no way of verifying TikTok's claim that the keylogger-like code only serves purely technical functions. Some of the accessed data could well be saved to the company's servers, and even sent to third parties. This would open the door to extensive surveillance, including by the Chinese government (to which TikTok has indirect ties). There is also a risk that the data would be stolen by crackers, and used to launch malware attacks.

The iOS in-app browsers of Instagram and Facebook behave essentially the same way as TikTok's. The main difference is that Instagram and Facebook allow users to access third-party sites with their default browser, whereas TikTok makes it nearly impossible.

The researcher didn't study the Android versions of in-app browsers, but we have no reason to assume they are safer than the iOS versions.

Please note that the article wrongly refers to crackers as “hackers.”

- Added: 2022-09-14 — Latest reference: 2022-08-07

  Some Epson printers are programmed to stop working after they have printed a predetermined number of pages, on the pretext that ink pads become saturated with ink. This constitutes an unacceptable infringement on users' freedom to use their printers as they wish, and on their right to repair them.

- Added: 2022-09-14 — Latest reference: 2022-04-14

  Today's “smart” TVs push people to surrender to tracking via internet. Some won't work unless they have a chance to download nonfree software. And they are designed for programmed obsolescence.

- Added: 2022-09-13 — Latest reference: 2022-08-29

  US states that ban abortion talk about making it a crime to go to another state to get an abortion. They could use various forms of location tracking, including the network, to prosecute abortion-seekers. The state could subpoena the data, so that the network's “privacy” policy would be irrelevant.

  That article explains why wireless networks collect location data, one unavoidable reason and one avoidable (emergency calls). It also explains some of the many ways the location data are used.

  Networks should never do localization for emergency calls except when you make an emergency call, or when there is a court order to do so. It should be illegal for a network to do precise localization (the kind needed for emergency calls) except to handle an emergency call, and if a network does so illegally, it should be required to inform the owner of the phone in writing on paper, with an apology.

- Added: 2022-09-12 — Latest reference: 2015-07-28

  Many retail businesses publish cr...apps that ask to spy on the user's own data—often many kinds.

  Those companies know that snoop-phone usage trains people to say yes to almost any snooping.

- Added: 2022-08-31 — Latest reference: 2020-06-11

  Network location tracking is used, among other techniques, for targeted advertising.

- Added: 2022-08-28 — Latest reference: 2022-08-22

  Tesla sells an add-on software feature that drivers are not allowed to use.

  This practice depends on a back door, which is unjust in itself. Asking users to buy something years in advance to avoid having to pay an even higher price later is manipulative.

- Added: 2022-08-28 — Latest reference: 2022-07-20

  Shortcuts, a built-in scripting app on Apple devices, doesn't give you complete freedom to share scripts (a.k.a. “shortcuts”). Exporting a script as a file requires an Apple ID, and may be subjected to censorship by Apple.

In this situation (and many others), switching from iPhony/iBad to a freedom respecting device gives you both convenience and freedom. The assumption that you must sacrifice convenience to get freedom is often wrong. Jails are inconvenient.

- Added: 2022-08-22 — Latest reference: 2022-07-30

  The nonfree software in a Tesla artificially limits the car's driving range, demanding ransom to unlock the battery's full charge.

  This is one more reason why cars must not be “connected.”

- Added: 2022-08-22 — Latest reference: 2022-07-01

  ATMs and vending machines in Russia run nonfree software—The machines' owners cannot fix them.

- Added: 2022-08-22 — Latest reference: 2020-09-22

  The Markup investigated 80,000 popular web sites and reports on how much they snoop on users. Almost 70,000 had third-party trackers. 5,000 fingerprinted the browser to identify users. 12,000 recorded the user's mouse clicks and movements.

- Added: 2022-08-22 — Latest reference: 2019-05-14

  Adobe revoked the license of some older versions of its applications, and warned customers that they can get sued for using them.

  This is further proof that users of nonfree software are in the hands of its developer.

- Added: 2022-06-14 — Latest reference: 2022-06-02

  Canada has fined the company Tim Hortons for making an app that tracks people's movements to learn things such as where they live, where they work, and when they visit competitors' stores.

- Added: 2022-06-04 — Latest reference: 2022-05-24

  A worldwide investigation found that most of the applications that school districts recommended for remote education during the COVID-19 pandemic track and collect personal data from children as young as below the age of five. These applications, and their websites, send the collected information to ad giants such as Facebook and Google, and they are still being used in the classrooms even after some of the schools reopened.

- Added: 2022-05-10 — Latest reference: 2022-04-28

  The US government sent personal data to Facebook for every college student that applied for US government student aid. It justified this as being for a “campaign.”

  The data included name, phone number and email address. This shows the agency didn't even make a handwaving attempt to anonymize the student. Not that anonymization usually does much good—but the failure to even try shows that the agency was completely blind to the issue of respecting students' privacy.

- Added: 2022-05-08 — Latest reference: 2016-03-06

  Electronic Arts made one of its games permanently unplayable by shutting down its servers. This game was heavily reliant on the company's servers, and because the software is proprietary, users can't modify it to make it connect to some other server. If the game were free, people could still play what they purchased.

- Added: 2022-04-19 — Latest reference: 2022-04-04

  New Amazon worker chat app would ban specific words Amazon doesn't like, such as “union”, “restrooms”, and “pay raise”. If the app was free, workers could modify the program so it acts as they wish, not how Amazon wants it.

- Added: 2022-04-18 — Latest reference: 2022-03-01

The nonfree app “Along,” developed by a company controlled by Zuckerberg, leads students to reveal to their teacher personal information about themselves and their families. Conversations are recorded and the collected data sent to the company, which grants itself the right to sell it. See also Educational Malware App “Along”.

- Added: 2022-04-12 — Latest reference: 2022-03-21

  Apple prevents people from upgrading their Mac hardware by imposing DRM on its removable SSD storage.

- Added: 2022-04-06 — Latest reference: 2022-02-15

  Honorlock set a network of fake test answer honeypot sites, tempting people to get exam answers, but that is a way to entrap students, so as to identify them and punish them, using nonfree JS code to identify them.

- Added: 2022-04-06 — Latest reference: 2022-01-29

  “Smart” TV manufacturers spy on people using various methods, and harvest their data. They are collecting audio, video, and TV usage data to profile people.

- Added: 2022-04-04 — Latest reference: 2022-02-19

  Hewlett-Packard is implementing DRM in its printers so they refuse to print with ink cartridges from another supplier.

- Added: 2022-04-04 — Latest reference: 2022-02-15

  Dymo is now embedding DRM in the paper rolls for its label printers to make those printers reject equivalent paper rolls made by other companies. This is implemented by an RFID tag, which keeps track of how many labels remain on the roll, and blocks further printing when the roll is empty—an efficient way to prevent reusing the same RFID with a third-party roll.

- Added: 2022-04-04 — Latest reference: 2022-02-09

  A security failure in Microsoft's Windows is infecting people's computers with RedLine stealer malware using a fake Windows 11 upgrade installer.

- Added: 2022-04-04 — Latest reference: 2022-01-27

  The data broker X-Mode bought location data about 20,000 people collected by around 100 different malicious apps.

- Added: 2022-02-27 — Latest reference: 2019-03-21

  The MoviePass dis-service is planning to use face recognition to track people's eyes to make sure they won't put their phones down or look away during ads—and trackers.

- Added: 2022-01-31 — Latest reference: 2022-01-04

  A critical bug in Apple's iOS makes it possible for attackers to alter a shutdown event, tricking the user into thinking that the phone has been powered off. But in fact, it's still running, and the user can't feel any difference between a real shutdown and the fake shutdown.

- Added: 2022-01-31 — Latest reference: 2017-09-02

  Instagram is forcing users to give away their phone numbers and won't let people continue using the app if they refuse.

- Added: 2022-01-19 — Latest reference: 2022-01-05

  The Norton 360 antivirus updated its program to install a cryptocurrency miner on users' computers without people's permission. The miner is not turned on by default but there is no way to completely uninstall the crypto mining software, which has upset some users.

- Added: 2022-01-11 — Latest reference: 2022-01-01

The legacy company that made Blackberry phones is about to kill them off by shutting down the server they are tethered to.

If the software on those phones were free (as in freedom), people could modify their software so they could talk to some other server.

- Added: 2022-01-11 — Latest reference: 2010-03-28

  Sony restricted access to the PlayStation 3 GPU, so people who installed a GNU/Linux operating system on the console couldn't use it at full capacity. When some of them broke the restriction, Sony removed the ability to install other operating systems. Then users broke that restriction too, but got sued by Sony.

- Added: 2022-01-11 — Latest reference: 2005-12-27

  To install and use third-party operating systems and programs on the Xbox console, people had to break the restrictions imposed by Microsoft.

- Added: 2021-12-19 — Latest reference: 2021-11-20

  NordicTrack, a company that sells exercise machines with ability to show videos limits what people can watch, and recently disabled a feature that was originally functional. This happened through automatic update and probably involved a universal back door.

- Added: 2021-12-19 — Latest reference: 2021-11-20

  Hundreds of Tesla drivers were locked out of their cars as a result of Tesla's app suffering from an outage, which happened because the app is tethered to the company's servers.

- Added: 2021-12-19 — Latest reference: 2021-11-11

  Some researchers at Google found a zero-day vulnerability on MacOS, which crackers used to target people visiting the websites of a media outlet and a pro-democracy labor and political group in Hong Kong.

  Please note that the article wrongly refers to crackers as “hackers”.

- Added: 2021-11-19 — Latest reference: 2021-10-25

  EdTech companies use their surveillance power to manipulate students, and direct them into tracks towards various levels of knowledge, power and prestige. The article argues that these companies should obtain licenses to operate. That wouldn't hurt, but it doesn't address the root of the problem. All data acquired in a school about any student, teacher, or employee must not leave the school, and must be kept in computers that belong to the school and run free (as in freedom) software. That way, the school district and/or parents can control what is done with those data.

- Added: 2021-11-18 — Latest reference: 2021-11-09

  A building in LA, with a supermarket in it, demands customers load a particular app to pay for parking in the parking lot, and accept pervasive surveillance. They also have the option of entering their license plate numbers in a kiosk. That is an injustice, too.

- Added: 2021-11-18 — Latest reference: 2021-11-04

  Apple's new tactic to restrict users from repairing their own device and impose DRM on people is to completely disable its Face ID functionality when you replace its screen.

- Added: 2021-11-18 — Latest reference: 2021-08-18

  Microsoft is making it harder and harder to replace default apps in its Windows operating system and is pressuring users to use its proprietary programs instead. We believe the best approach to this would be replacing Windows with a free (as in freedom) operating system like GNU. We also maintain a list of fully free distributions of GNU.

- Added: 2021-11-18 — Latest reference: 2018-02-28

Spotify app harvests users' data to personally identify and know people through music, their mood, mindset, activities, and tastes. There are over 150 billion events logged daily on the program which contains users' data and personal information.

- Added: 2021-11-09 — Latest reference: 2016-02-11

  A pacemaker running proprietary code was misconfigured and could have killed the implanted person. In order to find out what was wrong and get it fixed, the person needed to break into the remote device that sets parameters in the pacemaker (possibly infringing upon manufacturer's rights under the DMCA). If this system had run free software, it could have been fixed much sooner.

- Added: 2021-11-04 — Latest reference: 2021-10-13

  Adobe has licensed its Flash Player to China's Zhong Cheng Network who is offering the program bundled with spyware and a back door that can remotely deactivate it.

  Adobe is responsible for this since they gave Zhong Cheng Network permission to do this. This injustice involves “misuse” of the DMCA, but “proper,” intended use of the DMCA is a much bigger injustice. There is a series of errors related to DMCA.

- Added: 2021-10-12 — Latest reference: 2021-10-07

  Facebook's nonfree client forces its useds to look at the newsfeed. A used of Facebook developed a browser add-on to make it easier to unfollow everyone and thus make the newsfeed empty. Many of the people used by Facebook loved this, because they regard the newsfeed as a burden that Facebook imposes on them.

  If the client software for Facebook were free, useds could probably make the newsfeed disappear by modifying the client not to display it.

- Added: 2021-10-12 — Latest reference: 2021-09-22

  Some Xiaomi phones have a malfeature to bleep out phrases that express political views the Chinese government does not like. In phones sold in Europe, Xiaomi leaves this deactivated by default, but has a back door to activate the censorship.

  This is the natural result of having nonfree software in a device that can communicate with the company that made it.

- Added: 2021-10-12 — Latest reference: 2021-06-25

  El Salvador Dictatorship's Chivo wallet is spyware, it's a proprietary program that breaks users' freedom and spies on people; demands personal data such as the national ID number and does face recognition, and it is bad security for its data. It also asks for almost every malware permission in people's smartphones.

  The article criticizes it for faults in “data protection”, though “data protection” is the wrong approach to privacy anyway.

- Added: 2021-10-08 — Latest reference: 2021-09-21

  Google's proprietary Chrome web browser added a surveillance API (idle detection API) which lets websites ask Chrome to report when a user with a web page open is idle.

- Added: 2021-09-20 — Latest reference: 2021-09-17

  Apple has made it impossible to load Navalny's tactical voting app into an iPhone in Russia.

  It is impossible because (1) the iPhone refuses to load apps from anywhere other than Apple, and (2) Apple has obeyed a Russian censorship law. The first point is enforced by Apple's nonfree software.

- Added: 2021-09-15 — Latest reference: 2021-08-17

Various models of security cameras, DVRs, and baby monitors that run proprietary software are affected by a security vulnerability that could give attackers access to live feeds.

- Added: 2021-09-01 — Latest reference: 2021-08-24

  Recent Samsung TVs have a back door with which Samsung can brick them remotely.

- Added: 2021-09-01 — Latest reference: 2021-08-20

  The Russian communications watchdog tells Google and Apple to remove Navalny's app from their stores.

  Because Apple controls what a user can install, this is absolute censorship. By contrast, because Android does not do that, users can install apps even if Google does not offer them.

- Added: 2021-07-30 — Latest reference: 2021-07-18

  The pegasus spyware used vulnerabilities on proprietary smartphone operating systems to impose surveillance on people. It can record people's calls, copy their messages, and secretly film them, using a security vulnerability. There's also a technical analysis of this spyware available in PDF format.

  A free operating system would've let people to fix the bugs for themselves but now infected people will be compelled to wait for corporations to fix the problems.

  Please note that the article wrongly refers to crackers as “hackers”.

- Added: 2021-07-15 — Latest reference: 2021-07-09

  A newly found Microsoft Windows vulnerability can allow crackers to remotely gain access to the operating system and install programs, view and delete data, or even create new user accounts with full user rights.

  The security research firm accidentally leaked instructions on how the flaw could be exploited but Windows users should still wait for Microsoft to fix the flaw, if they fix it.

  Please note that the article wrongly refers to crackers as “hackers”.

- Added: 2021-07-15 — Latest reference: 2021-07-05

  Advertising companies are experimenting to manipulate people's minds, and impose a new way of advertising by altering their dreams. This “targeted dream incubation” would trigger “refreshing dreams” of the product, according to the companies.

- Added: 2021-07-04 — Latest reference: 2021-06-22

  Peloton company which produces treadmills recently locked people out of basic features of people's treadmills by a software update. The company now asks people for a membership/subscription for what people already paid for.

  The software used in the treadmill is proprietary and probably includes back doors to force software updates. It teaches the lesson that if a product talks to external networks, you must expect it to take in new malware.

  Please note that the company behind this product said they are working to reverse the changes so people will no longer need subscription to use the locked feature.

  Apparently public anger made the company back down. If we want that to be our safety, we need to build up the anger against malicious features (and the proprietary software that is their entry path) to the point that even the most powerful companies don't dare.

- Added: 2021-06-27 — Latest reference: 2021-06-19

  Google automatically installed an app on many proprietary Android phones. The app might or might not do malicious things but the power Google has over proprietary Android phones is dangerous.

- Added: 2021-06-22 — Latest reference: 2021-06-17

  Almost all proprietary health apps harvest users' data, including sensitive health information, tracking identifiers, and cookies to track user activities. Some of these applications are tracking users across different platforms.

- Added: 2021-06-17 — Latest reference: 2021-06-03

  TikTok apps collect biometric identifiers and biometric information from users' smartphones. The company behind it does whatever it wants and collects whatever data it can.

- Added: 2021-06-13 — Latest reference: 2020-04-13

  Google, Apple, and Microsoft (and probably some other companies) are collecting people's access points and GPS coordinates (which can identify people's precise location) even if their GPS is turned off, without the person's consent, using proprietary software implemented in person's smartphone. Though merely asking for permission would not necessarily legitimize this.

- Added: 2021-06-09 — Latest reference: 2018-08-13

  Google will track people even if people turn off location history, using Google Maps, weather updates, and browser searches. Google basically uses any app activity to track people.

- Added: 2021-06-08 — Latest reference: 2021-05-30

  Apple is systematically undermining interoperability. At the hardware level, it does this via nonstandard plugs, buses and networks. At the software level, it does this by not letting the user have any data except within one app.

- Added: 2021-06-08 — Latest reference: 2018-08-13

  Since the beginning of 2017, Android phones have been collecting the addresses of nearby cellular towers, even when location services are disabled, and sending that data back to Google.

- Added: 2021-06-02 — Latest reference: 2021-05-24

  Apple is moving its Chinese customers' iCloud data to a datacenter controlled by the Chinese government. Apple is already storing the encryption keys on these servers, obeying Chinese authority, making all Chinese user data available to the government.

- Added: 2021-05-26 — Latest reference: 2021-05-13

  Ford is planning to force ads on drivers in cars, with the ability for the owner to pay extra to turn them off. The system probably imposes surveillance on drivers too.

- Added: 2021-05-18 — Latest reference: 2021-05-04

  A motorcycle company named Klim is selling airbag vests with different payment methods, one of them is through a proprietary subscription-based option that will block the vest from inflating if the payments don't go through.

  They say there is a 30-days grace period if you miss a payment but the grace period is no excuse to the insecurity.

- Added: 2021-05-13 — Latest reference: 2021-05-06

  60% of school apps are sending student data to potentially high-risk third parties, putting students and possibly all other school workers under surveillance. This is made possible by using unsafe and proprietary programs made by data-hungry corporations.

  Please note that whether students consent to this or not, doesn't justify the surveillance they're imposed to.

- Added: 2021-05-06 — Latest reference: 2021-05-03

  The United States' government is reportedly considering teaming up with private companies to monitor American citizens' private online activity and digital communications.

What creates the opportunity to try this is the fact that these companies are already snooping on users' private activities. That in turn is due to people's use of nonfree software which snoops, and online dis-services which snoop.

- Added: 2021-04-26 — Latest reference: 2021-04-06

  The WeddingWire app saves people's wedding photos forever and hands over data to others, giving users no control over their personal information/data. The app also sometimes shows old photos and memories to users, without giving them any control over this either.

- Added: 2021-04-16 — Latest reference: 2021-04-09

  A zero-day vulnerability in Zoom which can be used to launch remote code execution (RCE) attacks has been disclosed by researchers. The researchers demonstrated a three-bug attack chain that caused an RCE on a target machine, all this without any form of user interaction.

- Added: 2021-04-11 — Latest reference: 2021-02-16

  Google handed over personal data of Indian protesters and activists to Indian police which led to their arrest. The cops requested the IP address and the location where a document was created and with that information, they identified protesters and activists.

- Added: 2021-04-11 — Latest reference: 2020-07-02

  BMW is trying to lock certain features of its cars, and force people to pay to use part of the car they already bought. This is done through forced update of the car software via a radio-operated back door.

- Added: 2021-03-16 — Latest reference: 2021-03-10

  Amazon's monopoly and DRM is stopping public libraries from lending e-books and audiobooks. Amazon became powerful in e-book world by Swindle, and is now misusing its power and violates people's rights using Digital Restrictions Management.

  The article is written in a way that endorses DRM in general, which is unacceptable. DRM is an injustice to people.

- Added: 2021-03-16 — Latest reference: 2021-03-09

  Over 150 thousand security cameras that used Verkada company's proprietary software are cracked by a major security breach. Crackers have had access to security archives of various gyms, hospitals, jails, schools, and police stations that have used Verkada's cameras.

  It is injustice to the public for gyms, stores, hospitals, jails, and schools to hand “security” footage to a company from which the government can collect it at any time, without even telling them.

  Please note that the article wrongly refers to crackers as “hackers”.

- Added: 2021-03-16 — Latest reference: 2020-10-28

  TV manufacturers are turning to produce only “Smart” TV sets (which include spyware) that it's now very hard to find a TV that doesn't spy on you.

  It appears that those manufacturers business model is not to produce TV and sell them for money, but to collect your personal data and (possibly) hand over them to others for benefit.

- Added: 2021-03-12 — Latest reference: 2018-09-12

  Tiny Lab Productions, along with online ad businesses run by Google, Twitter and three other companies are facing a lawsuit for violating people's privacy by collecting their data from mobile games and handing over these data to other companies/advertisers.

- Added: 2021-03-09 — Latest reference: 2021-03-05

  At least 30 thousand organizations in the United States are newly “cracked” via holes in Microsoft's proprietary email software, named Microsoft 365. It is unclear whether there are other holes and

vulnerabilities in the program or not but history and experience tells us it wouldn't be the last disaster with proprietary programs.

- Added: 2021-03-09 — Latest reference: 2021-02-11

  Researchers at the security firm SentinelOne discovered a security flaw in proprietary program Microsoft Windows Defender that lurked undetected for 12 years. If the program was free (as in freedom), more people would have had a chance to notice the problem, therefore, it could've been fixed a lot sooner.

- Added: 2021-03-09 — Latest reference: 2020-04-30

  Proprietary programs Google Meet, Microsoft Teams, and WebEx are collecting user's personal and identifiable data including how long a call lasts, who's participating in the call, and the IP addresses of everyone taking part. From experience, this can even harm users physically if those companies hand over data to governments.

- Added: 2021-03-08 — Latest reference: 2020-04-27

  The proprietary program Microsoft Teams' insecurity could have let a malicious GIF steal user data from Microsoft Teams accounts, possibly across an entire company, and taken control of “an organization's entire roster of Teams accounts.”

- Added: 2021-03-07 — Latest reference: 2020-10-18

  Microsoft is forcing Windows users to install upgrades it pushes using its universal back doors. These upgrades can do various harms to users such as restricting computers from some functions and/or forcing users to defenselessly do whatever Microsoft tells them to do.

- Added: 2021-02-25 — Latest reference: 2021-02-20

  The proprietary program Clubhouse is malware and a privacy disaster. Clubhouse collects people's personal data such as recordings of people's conversations, and, as a secondary problem, does not encrypt them, which shows a bad security part of the issue.

  A user's unique Clubhouse ID number and chatroom ID are transmitted in plaintext, and Agora (the company behind the app) would likely have access to users' raw audio, potentially providing access to the Chinese government.

  Even with good security of data transmission, collecting personal data of people is wrong and a violation of people's privacy rights.

- Added: 2021-02-25 — Latest reference: 2021-02-18

  Microsoft is forcibly removing the Flash player from computers running Windows 10, using a universal backdoor in Windows.

  The fact that Flash has been disabled by Adobe is no excuse for this abuse of power. The nature of proprietary software, such as Microsoft Windows, gives the developers power to impose their decisions on users. Free software on the other hand empowers users to make their own decisions.

- Added: 2021-02-22 — Latest reference: 2021-02-19

  The Prodigy maths game played in schools at no cost entices students to play it at home, where the company tries to lure them into paying for a premium subscription in exchange for mere cosmetic features that, at school, underline the socioeconomic gap between those who can afford it and those who can't.

  The strategy of using schools as a fishing pool for customers is a common practice traditionally adopted by nonfree software companies.

- Added: 2021-02-22 — Latest reference: 2020-12-25

  The HonorLock online exam proctoring program is a surveillance tool that tracks students and collects data such as face, driving license, and network information, among others, in blatant violation of students' privacy.

Preventing students from cheating should not be an excuse for running malware/spyware on their computers, and it's good that students are protesting. But their petitions overlook a crucial issue, namely, the injustice of being forced to run nonfree software in order to get an education.

- Added: 2021-02-06 — Latest reference: 2021-02-01

  Many cr...apps, developed by various companies for various organizations, do location tracking unknown to those companies and those organizations. It's actually some widely used libraries that do the tracking.

  What's unusual here is that proprietary software developer A tricks proprietary software developers B1 ... B50 into making platforms for A to mistreat the end user.

- Added: 2021-02-04 — Latest reference: 2020-10-12

  Samsung is forcing its smartphone users in Hong Kong (and Macau) to use a public DNS in Mainland China, using software update released in September 2020, which causes many unease and privacy concerns.

- Added: 2021-01-27 — Latest reference: 2021-01-13

  The authorities in Venice track the movements of all tourists using their portable phones. The article says that *at present* the system is configured to report only aggregated information. But that could be changed. What will that system do 10 years from now? What will a similar system in another country do? Those are the questions this raises.

- Added: 2021-01-19 — Latest reference: 2021-01-11

  A cracker took control of people's internet-connected chastity cages and demanded ransom. The chastity cages are being controlled by a proprietary app (mobile program).

  (Please note that the article wrongly refers to crackers as "hackers".)

- Added: 2021-01-11 — Latest reference: 2021-01-08

  As of 2021, WhatsApp (one of Facebook's subsidiaries) is forcing its users to hand over sensitive personal data to its parent company. This increases Facebook's power over users, and further jeopardizes people's privacy and security.

  Instead of WhatsApp you can use GNU Jami, which is free software and will not collect your data.

- Added: 2021-01-08 — Latest reference: 2016-04-04

  Many popular mobile games include a random-reward system called *gacha* which is especially effective on children. One variant of gacha was declared illegal in Japan in 2012, but the other variants are still luring players into compulsively spending inordinate amounts of money on virtual toys.

- Added: 2021-01-05 — Latest reference: 2021-01-05

  Most Internet connected devices in Mozilla's “Privacy Not Included” list are designed to snoop on users even if they meet Mozilla's “Minimum Security Standards.” Insecure design of the program running on some of these devices makes the user susceptible to be snooped on and exploited by crackers as well.

- Added: 2021-01-04 — Latest reference: 2021-01-04

  The personal finance management software “Quicken” has a discontinuation policy, a.k.a. planned obsolescence, which is an injustice to users. A free (as in freedom) program would let users control the software. But when you use a proprietary software, you won't be in control.

- Added: 2021-01-04 — Latest reference: 2020-12-02

  Adobe Flash Player has a universal back door which lets Adobe control the software and, for example, disable it whenever it wants. Adobe will block Flash content from running in Flash Player

beginning January 12, 2021, which indicates that they have access to every Flash Player through a back door.

The back door won't be dangerous in the future, as it'll disable a proprietary program and make users delete the software, but it was an injustice for many years. Users should have deleted Flash Player even before its end of life.

- Added: 2021-01-04 — Latest reference: 2020-10-21

  As of 2019-2020, Minecraft players are being forced to move to Microsoft servers, which results in privacy violation. Microsoft publishes a program so users can run their own server, but the program is proprietary and it's another injustice to users.

  People can play Minetest instead. Minetest is free software and respects the user's computer freedom.

- Added: 2021-01-04 — Latest reference: 2020-09-07

  While the world is still struggling with COVID-19 coronavirus, many people are in danger of surveillance and their computers are infected with malware as a result of installing proprietary software.

- Added: 2020-12-26 — Latest reference: 2020-11-05

  HP tricked users into installing a mischievous update in their printers that made the devices reject all third-party ink cartridges.

- Added: 2020-12-23 — Latest reference: 2020-12-15

  United States officials are facing one of biggest crackings against them in years, when malicious code was sneaked into SolarWinds' proprietary software named Orion. Crackers got access to networks when users downloaded a tainted software update. Crackers were able to monitor internal emails at some of the top agencies in the US.

  (Please note that the article wrongly refers to crackers as "hackers".)

- Added: 2020-12-22 — Latest reference: 2020-12-20

  Commercial crackware can get passwords out of an iMonster, use the microphone and camera, and other things.

- Added: 2020-12-21 — Latest reference: 2020-12-19

  A Zoom executive carried out snooping and censorship for the Chinese government.

  This abuse of Zoom's power shows how dangerous that power is. The root problem is not the surveillance and censorship, but rather the power that Zoom has. It gets that power partly from the use of its server, but also partly from the nonfree client program.

- Added: 2020-12-18 — Latest reference: 2020-11-23

  Some Wavelink and JetStream wifi routers have universal back doors that enable unauthenticated users to remotely control not only the routers, but also any devices connected to the network. There is evidence that this vulnerability is actively exploited.

  If you consider buying a router, we encourage you to get one that runs on free software. Any attempts at introducing malicious functionalities in it (e.g., through a firmware update) will be detected by the community, and soon corrected.

  If unfortunately you own a router that runs on proprietary software, don't panic! You may be able to replace its firmware with a free operating system such as libreCMC. If you don't know how, you can get help from a nearby GNU/Linux user group.

- Added: 2020-12-17 — Latest reference: 2020-12-07

Baidu apps were caught collecting sensitive personal data that can be used for lifetime tracking of users, and putting them in danger. More than 1.4 billion people worldwide are affected by these proprietary apps, and users' privacy is jeopardized by this surveillance tool. Data collected by Baidu may be handed over to the Chinese government, possibly putting Chinese people in danger.

- Added: 2020-12-05 — Latest reference: 2020-11-26

  Microsoft's Office 365 suite enables employers to snoop on each employee. After a public outburst, Microsoft stated that it would remove this capability. Let's hope so.

- Added: 2020-11-25 — Latest reference: 2020-11-12

  Apple has implemented a malware in its computers that imposes surveillance on users and reports users' computing to Apple.

  The reports are even unencrypted and they've been leaking this data for two years already. This malware is reporting to Apple what user opens what program at what time. It also gives Apple power to sabotage users' computing.

- Added: 2020-11-23 — Latest reference: 2020-11-09

  According to FTC, the company behind the Zoom conferencing software has lied to users about its end-to-end encryption for years, at least since 2016.

  People can use free (as in freedom) programs such as Jitsi or BigBlueButton, better still if installed in a server controlled by the users.

- Added: 2020-11-21 — Latest reference: 2020-04-15

  Riot Games' new anti-cheat is malware; runs on system boot at kernel level on Windows. It is insecure software that increases the attack surface of the operating system.

- Added: 2020-11-19 — Latest reference: 2020-03-26

  The Apple iOS version of Zoom is sending users' data to Facebook even if the user doesn't have a Facebook account. According to the article, Zoom and Facebook don't even mention this surveillance on their privacy policy page, making this an obvious violation of people's privacy even in their own terms.

- Added: 2020-11-14 — Latest reference: 2020-11-06

  A new app published by Google lets banks and creditors deactivate people's Android devices if they fail to make payments. If someone's device gets deactivated, it will be limited to basic functionality, such as emergency calling and access to settings.

- Added: 2020-11-14 — Latest reference: 2019-05-28

  Microsoft forces people to give their phone number in order to be able to create an account on the company's network. On top of mistreating their users by providing nonfree software, Microsoft is tracking their lives outside the computer and violates their privacy.

- Added: 2020-11-10 — Latest reference: 2020-06-12

  The company behind Zoom does not only deny users' computer freedom by developing this piece of nonfree software, it also violates users' civil rights by banning events and censoring users to serve the agenda of governments.

  Freedom respecting programs such as Jitsi or BigBlueButton can be used instead, better still if installed in a server controlled by its users.

- Added: 2020-11-02 — Latest reference: 2020-10-22

  Microsoft is imposing its surveillance on the game of Minecraft by requiring every player to open an account on Microsoft's network. Microsoft has bought the game and will merge all accounts into its network, which will give them access to people's data.

Minecraft players can play Minetest instead. The essential advantage of Minetest is that it is free software, meaning it respects the user's computer freedom. As a bonus, it offers more options.

- Added: 2020-11-02 — Latest reference: 2019-12-16

  Microsoft is tricking users to create an account on their network to be able to install and use the Windows operating system, which is malware. The account can be used for surveillance and/or violating people's rights in many ways, such as turning their purchased software to a subscription product.

- Added: 2020-10-28 — Latest reference: 2020-10-22

  The addictive Genshin Impact relentlessly coerces players to spend money by overwhelming the game play with loot boxes.

- Added: 2020-10-16 — Latest reference: 2020-09-10

  Internet-enabled watches with proprietary software are malware, violating people (specially children's) privacy. In addition, they have a lot of security flaws. They permit security breakers (and unauthorized people) to access the watch.

  Thus, ill-intentioned unauthorized people can intercept communications between parent and child and spoof messages to and from the watch, possibly endangering the child.

  (Note that this article misuses the word “hackers” to mean “crackers.”)

- Added: 2020-10-06 — Latest reference: 2020-03-11

  Roblox (among many other games) created anti-features which sucker children into utilizing third-party payment services without authorization.

- Added: 2020-09-30 — Latest reference: 2020-07-27

  The Mellow sous-vide cooker is tethered to a server. The company suddenly turned this tethering into a subscription, forbidding users from taking advantage of the “advanced features” of the cooker unless they pay a monthly fee.

- Added: 2020-09-28 — Latest reference: 2020-09-27

  Many employers are using nonfree software, including videoconference software, to surveil and monitor staff working at home. If the program reports whether you are “active,” that is in effect a malicious surveillance feature.

- Added: 2020-09-28 — Latest reference: 2020-09-18

  Facebook snoops on Instagram users by surreptitously turning on the device's camera.

- Added: 2020-09-23 — Latest reference: 2020-08-18

  Oculus headsets require users to identify themselves to Facebook. This will give Facebook free rein to pervasively snoop on Oculus users.

- Added: 2020-09-02 — Latest reference: 2020-08-30

  Apple is putting the squeeze on all business conducted through apps for iMonsters.

  This is a symptom of a very big injustice: that Apple has the power to decide what software can be installed on an iMonster. That it is a jail.

- Added: 2020-08-21 — Latest reference: 2020-08-18

  New Toyotas will upload data to AWS to help create custom insurance premiums based on driver behaviour.

  Before you buy a “connected” car, make sure you can disconnect its cellular antenna and its GPS antenna. If you want GPS navigation, get a separate navigator which runs free software and works with Open Street Map.

- Added: 2020-08-21 — Latest reference: 2020-08-18

  Apple can remotely cut off any developer's access to the tools for developing software for iOS or MacOS.

  Epic (Apple's target in this example) makes nonfree games which have their own malicious features, but that doesn't make it acceptable for Apple to have this sort of power.

- Added: 2020-08-20 — Latest reference: 2020-08-11

  TikTok exploited an Android vulnerability to obtain user MAC addresses.

- Added: 2020-08-18 — Latest reference: 2020-04-20

  Apple whistleblower Thomas Le Bonniec reports that Apple made a practice of surreptitiously activating the Siri software to record users' conversations when they had not activated Siri. This was not just occasional, it was systematic practice.

  His job was to listen to these recordings, in a group that made transcripts of them. He does not believes that Apple has ceased this practice.

  The only reliable way to prevent this is, for the program that controls access to the microphone to decide when the user has “activated” any service, to be free software, and the operating system under it free as well. This way, users could make sure Apple can't listen to them.

- Added: 2020-08-14 — Latest reference: 2020-08-03

  Google Nest is taking over ADT. Google sent out a software update to its speaker devices using their back door that listens for things like smoke alarms and then notifies your phone that an alarm is happening. This means the devices now listen for more than just their wake words. Google says the software update was sent out prematurely and on accident and Google was planning on disclosing this new feature and offering it to customers who pay for it.

- Added: 2020-08-12 — Latest reference: 2020-07-28

  The Focals eyeglass display, with snooping microphone, has been eliminated. Google eliminated it by buying the manufacturer and shutting it down. It also shut down the server these devices depend on, which caused the ones already sold to cease to function.

  It may be a good thing to wipe out this product—for “smart,” read “snoop”—but Google didn't do that for the sake of privacy. Rather, it was eliminating competition for its own snooping product.

- Added: 2020-07-09 — Latest reference: 2020-07-01

  BMW will remotely enable and disable functionality in cars through a universal back door.

- Added: 2020-07-09 — Latest reference: 2020-06-30

  “Bossware” is malware that bosses coerce workers into installing in their own computers, so the bosses can spy on them.

  This shows why requiring the user's “consent” is not an adequate basis for protecting digital privacy. The boss can coerce most workers into consenting to almost anything, even probable exposure to contagious disease that can be fatal. Software like this should be illegal and bosses that demand it should be prosecuted for it.

- Added: 2020-07-01 — Latest reference: 2015-04-21

  Runescape is a popular online game with some addictive features derived from behavioral manipulation techniques. Certain repetitive aspects of the game, like grinding, can be minimised by becoming a paying member, and can thus encourage children and impressionable people to spend money on the game.

- Added: 2020-06-26 — Latest reference: 2020-06-26

Most apps are malware, but Trump's campaign app, like Modi's campaign app, is especially nasty malware, helping companies snoop on users as well as snooping on them itself.

The article says that Biden's app has a less manipulative overall approach, but that does not tell us whether it has functionalities we consider malicious, such as sending data the user has not explicitly asked to send.

- Added: 2020-06-25 — Latest reference: 2020-06-25

  TV manufacturers are able to snoop every second of what the user is watching. This is illegal due to the Video Privacy Protection Act of 1988, but they're circumventing it through EULAs.

- Added: 2020-06-22 — Latest reference: 2020-06-16

  A disasterous security bug touches millions of products in the Internet of Stings.

  As a result, anyone can sting the user, not only the manufacturer.

- Added: 2020-06-13 — Latest reference: 2019-09-06

  Best Buy made controllable appliances and shut down the service to control them through.

  Best Buy acknowledged that it was mistreating its customers by doing so, and offered reimbursement of the affected appliances. The fact remains, however, that tethering a device to a server is a way of restricting and harassing users. The nonfree software in the device is what stops users from cutting the tether.

- Added: 2020-06-07 — Latest reference: 2020-05-07

  Wink sells a “smart” home hub that is tethered to a server. In May 2020, it ordered the purchasers to start paying a monthly fee for the use of that server. Because of the tethering, the hub is useless without that.

- Added: 2020-05-25 — Latest reference: 2020-05-25

  Tesla's cars have a universal remote back door. Tesla used it to disable the autopilot features on people's cars to make them pay extra for re-enabling the features.

  This kind of malfeature is only possible with proprietary software—free software is controlled by its users who wouldn't let do such things to them.

- Added: 2020-05-03 — Latest reference: 2020-04-30

  Xiaomi phones report many actions the user takes: starting an app, looking at a folder, visiting a website, listening to a song. They send device identifying information too.

  Other nonfree programs snoop too. For instance, Spotify and other streaming dis-services make a dossier about each user, and they make users identify themselves to pay. Out, out, damned Spotify!

  Forbes exonerates the same wrongs when the culprits are not Chinese, but we condemn this no matter who does it.

- Added: 2020-04-14 — Latest reference: 2020-04-13

  The Google Play Terms of Service insist that the user of Android accept the presence of universal back doors in apps released by Google.

  This does not tell us whether any of Google's apps currently contains a universal back door, but that is a secondary question. In moral terms, demanding that people accept in advance certain bad treatment is equivalent to actually doing it. Whatever condemnation the latter deserves, the former deserves the same.

- Added: 2020-03-25 — Latest reference: 2017-03-07

  The CIA exploited existing vulnerabilities in “smart” TVs and phones to design a malware that spies through their microphones and cameras while making them appear to be turned off. Since the spyware sniffs signals, it bypasses encryption.

- Added: 2020-03-04 — Latest reference: 2020-03-01

  The Alipay Health Code app estimates whether the user has Covid-19 and tells the cops directly.

- Added: 2020-02-24 — Latest reference: 2019-11-19

  Internet-tethered Amazon Ring had a security vulnerability that enabled attackers to access the user's wifi password, and snoop on the household through connected surveillance devices.

  Knowledge of the wifi password would not be sufficient to carry out any significant surveillance if the devices implemented proper security, including encryption. But many devices with proprietary software lack this. Of course, they are also used by their manufacturers for snooping.

- Added: 2020-02-17 — Latest reference: 2019-12-22

  The ToToc messaging app seems to be a spying tool for the government of the United Arab Emirates. Any nonfree program could be doing this, and that is a good reason to use free software instead.

  Note: this article uses the word “free” in the sense of “gratis.”

- Added: 2020-02-17 — Latest reference: 2019-12-19

  Some Avast and AVG extensions for Firefox and Chrome were found to snoop on users' detailed browsing habits. Mozilla and Google removed the problematic extensions from their stores, but this shows once more how unsafe nonfree software can be. Tools that are supposed to protect a proprietary system are, instead, infecting it with additional malware (the system itself being the original malware).

- Added: 2020-02-15 — Latest reference: 2020-02-02

  Many Android apps fool their users by asking them to decide what permissions to give the program, and then bypassing these permissions.

  The Android system is supposed to prevent data leaks by running apps in isolated sandboxes, but developers have found ways to access the data by other means, and there is nothing the user can do to stop them from doing so, since both the system and the apps are nonfree.

- Added: 2020-02-15 — Latest reference: 2019-12-17

  Most modern cars now record and send various kinds of data to the manufacturer. For the user, access to the data is nearly impossible, as it involves cracking the car's computer, which is always hidden and running with proprietary software.

- Added: 2020-02-15 — Latest reference: 2019-12-09

  iMonsters and Android phones, when used for work, give employers powerful snooping and sabotage capabilities if they install their own software on the device. Many employers demand to do this. For the employee, this is simply nonfree software, as fundamentally unjust and as dangerous as any other nonfree software.

- Added: 2020-02-01 — Latest reference: 2020-01-29

  The Amazon Ring app does surveillance for other companies as well as for Amazon.

- Added: 2020-01-20 — Latest reference: 2020-01-09

  Android phones subsidized by the US government come with preinstalled adware and a back door for forcing installation of apps.

  The adware is in a modified version of an essential system configuration app. The back door is a surreptitious addition to a program whose stated purpose is to be a universal back door for firmware.

  In other words, a program whose raison d'être is malicious has a secret secondary malicious purpose. All this is in addition to the malware of Android itself.

- Added: 2019-10-31 — Latest reference: 2019-10-13

  Safari occasionally sends browsing data from Apple devices in China to the Tencent Safe Browsing service, to check URLs that possibly correspond to “fraudulent” websites. Since Tencent collaborates with the Chinese government, its Safe Browsing black list most certainly contains the websites of political opponents. By linking the requests originating from single IP addresses, the government can identify dissenters in China and Hong Kong, thus endangering their lives.

- Added: 2019-10-20 — Latest reference: 2019-04-08

  Apple plans to require that all application software for MacOS be approved by Apple first.

  Offering a checking service as an option could be useful and would not be wrong. Requiring users to get Apple's approval is tyranny. Apple says the check will only look for malware (not counting the malware that is part of the operating system), but Apple could change that policy step by step. Or perhaps Apple will define malware to include any app that the Chinese government does not like.

  For free software, this means users will need to get Apple's approval after compilation. This amounts to a system of surveilling the use of free programs.

- Added: 2019-10-19 — Latest reference: 2019-10-13

  The Chinese Communist Party's “Study the Great Nation” app requires users to grant it access to the phone's microphone, photos, text messages, contacts, and internet history, and the Android version was found to contain a back-door allowing developers to run any code they wish in the users' phone, as “superusers.” Downloading and using this app is mandatory at some workplaces.

  Note: The Washington Post version of the article (partly obfuscated, but readable after copy-pasting in a text editor) includes a clarification saying that the tests were only performed on the Android version of the app, and that, according to Apple, “this kind of ‘superuser’ surveillance could not be conducted on Apple's operating system.”

- Added: 2019-10-16 — Latest reference: 2019-10-07

  Apple censors the Taiwan flag in iOS on behalf of the Chinese government. When the region is set to Hong Kong, this flag is not visible in the emoji selection widget but is still accessible. When the region is set to mainland China, all attempts to display it will result in the “empty emoji” icon as if the flag never existed.

  Thus, not only does Apple use the App Store as an instrument of censorship, it also uses the iThing operating system for that purpose.

- Added: 2019-10-15 — Latest reference: 2019-10-10

  Apple has banned the app that Hong Kong protesters use to communicate.

  Obeying the “local laws” about what people can do with software is no excuse for censoring what software people can use.

- Added: 2019-10-15 — Latest reference: 2019-10-07

  Adobe has cancelled the software subscriptions of all users in Venezuela. This demonstrates how a requirement for subscription can be turned into a tool for sabotage.

- Added: 2019-10-04 — Latest reference: 2019-08-27

  A very popular app found in the Google Play store contained a module that was designed to secretly install malware on the user's computer. The app developers regularly used it to make the computer download and execute any code they wanted.

  This is a concrete example of what users are exposed to when they run nonfree apps. They can never be completely sure that a nonfree app is safe.

- Added: 2019-10-03 — Latest reference: 2019-09-09

The Facebook app tracks users even when it is turned off, after tricking them into giving the app broad permissions in order to use one of its functionalities.

- Added: 2019-10-03 — Latest reference: 2017-08-31

  The recent versions of Microsoft Office require the user to connect to Microsoft servers at least every thirty-one days. Otherwise, the software will refuse to edit any documents or create new ones. It will be restricted to viewing and printing.

- Added: 2019-09-18 — Latest reference: 2019-09-09

  Some nonfree period-tracking apps including MIA Fem and Maya send intimate details of users' lives to Facebook.

- Added: 2019-09-16 — Latest reference: 2019-09-16

  Tesla users claim Tesla force-installed software to cut down on battery range, rather than replace the defective batteries. Tesla did this to avoid having to run their warranty.

  This means that proprietary software can potentially be a way to commit perjury with impunity.

- Added: 2019-09-11 — Latest reference: 2019-08-22

  ChromeBooks are programmed for obsolescence: ChromeOS has a universal back door that is used for updates and ceases to operate at a predefined date. From then on, there appears to be no support whatsoever for the computer.

  In other words, when you stop getting screwed by the back door, you start getting screwed by the obsolescence.

- Added: 2019-09-11 — Latest reference: 2019-08-21

  Microsoft recorded users of Xboxes and had human workers listen to the recordings.

  Morally, we see no difference between having human workers listen and having speech-recognition systems listen. Both intrude on privacy.

- Added: 2019-09-10 — Latest reference: 2019-09-06

  Keeping track of who downloads a proprietary program is a form of surveillance. There is a proprietary program for adjusting a certain telescopic rifle sight. A US prosecutor has demanded the list of all the 10,000 or more people who have installed it.

  With a free program there would not be a list of who has installed it.

- Added: 2019-09-10 — Latest reference: 2019-08-31

  A series of vulnerabilities found in iOS allowed attackers to gain access to sensitive information including private messages, passwords, photos and contacts stored on the user's iMonster.

  The deep insecurity of iMonsters is even more pertinent given that Apple's proprietary software makes users totally dependent on Apple for even a modicum of security. It also means that the devices do not even try to offer security against Apple itself.

- Added: 2019-08-31 — Latest reference: 2019-08-16

  A game published on Facebook aimed at leading children to spend large amounts of their parents' money without explaining it to them.

- Added: 2019-08-23 — Latest reference: 2019-08-13

  When Apple suspects a user of fraud, it judges the case secretly and presents the verdict as a fait accompli. The punishment to a user found guilty is being cut off for life, which more-or-less cripples the user's Apple devices forever. There is no appeal.

- Added: 2019-08-15 — Latest reference: 2019-08-15

Skype refuses to say whether it can eavesdrop on calls.

That almost certainly means it can do so.

- Added: 2019-08-15 — Latest reference: 2019-08-15

  Apple is putting DRM on iPhone batteries, and the system proprietary software turns off certain features when batteries are replaced other than by Apple.

- Added: 2019-08-06 — Latest reference: 2019-08-02

  Out of 21 gratis Android antivirus apps that were tested by security researchers, eight failed to detect a test virus. All of them asked for dangerous permissions or contained advertising trackers, with seven being more risky than the average of the 100 most popular Android apps.

  (Note that the article refers to these proprietary apps as “free”. It should have said “gratis” instead.)

- Added: 2019-08-03 — Latest reference: 2019-07-08

  Many unscrupulous mobile-app developers keep finding ways to bypass user's settings, regulations, and privacy-enhancing features of the operating system, in order to gather as much private data as they possibly can.

  Thus, we can't trust rules against spying. What we can trust is having control over the software we run.

- Added: 2019-07-21 — Latest reference: 2019-07-21

  Google “Assistant” records users' conversations even when it is not supposed to listen. Thus, when one of Google's subcontractors discloses a thousand confidential voice recordings, users were easily identified from these recordings.

  Since Google “Assistant” uses proprietary software, there is no way to see or control what it records or sends.

  Rather than trying to better control the use of recordings, Google should not record or listen to the person's voice. It should only get commands that the user wants to send to some Google service.

- Added: 2019-07-17 — Latest reference: 2019-07-09

  Resourceful children figured out how to empty their parents' bank account buying packs of special players for an Electronic Arts soccer game.

  The random element of these packs (also called “loot boxes”) makes the game strongly addictive, but the fact that players are pressured to spend more in order to get ahead of their competitors further qualifies it as *predatory*. Note that Belgium made these loot boxes illegal in 2018.

  The only good reason to have a copy of such a proprietary game is to study it for free software development.

- Added: 2019-07-16 — Latest reference: 2019-07-10

  Apple appears to say that there is a back door in MacOS for automatically updating some (all?) apps.

  The specific change described in the article was not malicious—it protected users from surveillance by third parties—but that is a separate question.

- Added: 2019-07-15 — Latest reference: 2019-07-08

  Many Android apps can track users' movements even when the user says not to allow them access to locations.

  This involves an apparently unintentional weakness in Android, exploited intentionally by malicious apps.

- Added: 2019-07-15 — Latest reference: 2018-09-21

Clash of Clans is a good example of a gratis mobile game that its developers made very addictive for a large proportion of its users—and turned into a cash machine for themselves—by using psychological manipulation techniques.

(The article uses “free” to mean “zero price,” which is a usage we should avoid. We recommend saying “gratis” instead.)

- Added: 2019-06-27 — Latest reference: 2019-06-22

  Google Chrome is an instrument of surveillance. It lets thousands of trackers invade users' computers and report the sites they visit to advertising and data companies, first of all to Google. Moreover, if users have a Gmail account, Chrome automatically logs them in to the browser for more convenient profiling. On Android, Chrome also reports their location to Google.

  The best way to escape surveillance is to switch to IceCat, a modified version of Firefox with several changes to protect users' privacy.

- Added: 2019-06-10 — Latest reference: 2019-05-28

  In spite of Apple's supposed commitment to privacy, iPhone apps contain trackers that are busy at night sending users' personal information to third parties.

  The article mentions specific examples: Microsoft OneDrive, Intuit's Mint, Nike, Spotify, The Washington Post, The Weather Channel (owned by IBM), the crime-alert service Citizen, Yelp and DoorDash. But it is likely that most nonfree apps contain trackers. Some of these send personally identifying data such as phone fingerprint, exact location, email address, phone number or even delivery address (in the case of DoorDash). Once this information is collected by the company, there is no telling what it will be used for.

- Added: 2019-06-01 — Latest reference: 2019-05-30

  The Femm “fertility” app is secretly a tool for propaganda by natalist Christians. It spreads distrust for contraception.

  It snoops on users, too, as you must expect from nonfree programs.

- Added: 2019-05-29 — Latest reference: 2019-05-06

  Amazon Alexa collects a lot more information from users than is necessary for correct functioning (time, location, recordings made without a legitimate prompt), and sends it to Amazon's servers, which store it indefinitely. Even worse, Amazon forwards it to third-party companies. Thus, even if users request deletion of their data from Amazon's servers, the data remain on other servers, where they can be accessed by advertising companies and government agencies. In other words, deleting the collected information doesn't cancel the wrong of collecting it.

  Data collected by devices such as the Nest thermostat, the Philips Hue-connected lights, the Chamberlain MyQ garage opener and the Sonos speakers are likewise stored longer than necessary on the servers the devices are tethered to. Moreover, they are made available to Alexa. As a result, Amazon has a very precise picture of users' life at home, not only in the present, but in the past (and, who knows, in the future too?)

- Added: 2019-05-18 — Latest reference: 2019-05-15

  Users caught in the jail of an iMonster are sitting ducks for other attackers, and the app censorship prevents security companies from figuring out how those attacks work.

  Apple's censorship of apps is fundamentally unjust, and would be inexcusable even if it didn't lead to security threats as well.

- Added: 2019-05-10 — Latest reference: 2019-05-06

  BlizzCon 2019 imposed a requirement to run a proprietary phone app to be allowed into the event.

  This app is a spyware that can snoop on a lot of sensitive data, including user's location and contact list, and has near-complete control over the phone.

- Added: 2019-05-08 — Latest reference: 2019-04-26

The Jibo robot toys were tethered to the manufacturer's server, and the company made them all cease to work by shutting down that server.

The shutdown might ironically be good for their users, since the product was designed to manipulate people by presenting a phony semblance of emotions, and was most certainly spying on them.

- Added: 2019-05-08 — Latest reference: 2019-02-01

  The FordPass Connect feature of some Ford vehicles has near-complete access to the internal car network. It is constantly connected to the cellular phone network and sends Ford a lot of data, including car location. This feature operates even when the ignition key is removed, and users report that they can't disable it.

  If you own one of these cars, have you succeeded in breaking the connectivity by disconnecting the cellular modem, or wrapping the antenna in aluminum foil?

- Added: 2019-04-27 — Latest reference: 2019-04-24

  Some of users' commands to the Alexa service are recorded for Amazon employees to listen to. The Google and Apple voice assistants do similar things.

  A fraction of the Alexa service staff even has access to location and other personal data.

  Since the client program is nonfree, and data processing is done “in the cloud” (a soothing way of saying “We won't tell you how and where it's done”), users have no way to know what happens to the recordings unless human eavesdroppers break their non-disclosure agreements.

- Added: 2019-04-22 — Latest reference: 2019-04-21

  As of April 2019, it is no longer possible to disable an unscrupulous tracking anti-feature that reports users when they follow ping links in Apple Safari, Google Chrome, Opera, Microsoft Edge and also in the upcoming Microsoft Edge that is going to be based on Chromium.

- Added: 2019-04-22 — Latest reference: 2019-04-13

  Data collected by menstrual and pregnancy monitoring apps is often available to employers and insurance companies. Even though the data is “anonymized and aggregated,” it can easily be traced back to the woman who uses the app.

  This has harmful implications for women's rights to equal employment and freedom to make their own pregnancy choices. Don't use these apps, even if someone offers you a reward to do so. A free-software app that does more or less the same thing without spying on you is available from F-Droid, and a new one is being developed.

- Added: 2019-04-21 — Latest reference: 2019-04-04

  Microsoft has been force-installing a “remediation” program on computers running certain versions of Windows 10. Remediation, in Microsoft's view, means tampering with users' settings and files, notably to “repair” any components of the updating system that users may have intentionally disabled, and thus regain full power over them. Microsoft repeatedly pushed faulty versions of this program to users' machines, causing numerous problems, some of which critical.

  This exemplifies the arrogant and manipulative attitude that proprietary software developers have learned to adopt toward the people they are supposedly serving. Migrate to a free operating system if you can!

  If your employer makes you run Windows, tell the financial department how this wastes your time dealing with endless connections and premature hardware failures.

- Added: 2019-04-20 — Latest reference: 2019-04-15

  Volkswagen programmed its car engine computers to detect the Environmental Protection Agency's emission tests, and run dirty the rest of the time. In real driving, the cars exceeded emissions standards by a factor of up to 35.

Using free software would not have stopped Volkswagen from programming it this way, but would have made it harder to conceal, and given the users the possibility of correcting the deception.

Former executives of Volkswagen are being sued over this fraud.

- Added: 2019-04-18 — Latest reference: 2019-04-13

  Google tracks the movements of Android phones and iPhones running Google apps, and sometimes saves the data for years.

  Nonfree software in the phone has to be responsible for sending the location data to Google.

- Added: 2019-04-18 — Latest reference: 2018-11-23

  An Android phone was observed to track location even while in airplane mode. It didn't send the location data while in airplane mode. Instead, it saved up the data, and sent them all later.

- Added: 2019-04-17 — Latest reference: 2019-04-04

  Ebooks “bought” from Microsoft's store check that their DRM is valid by connecting to the store every time their “owner” wants to read them. Microsoft is going to close this store, bricking all DRM'ed ebooks it has ever “sold”. (The article additionally highlights the pitfalls of DRM.)

  This is another proof that a DRM-encumbered product doesn't belong to the person who bought it. Microsoft said it will refund customers, but this is no excuse for selling them restricted books.

- Added: 2019-04-15 — Latest reference: 2019-03-28

  OfficeMax cheated customers by using proprietary “PC Health Check” software rigged to give false results, deceiving the customer into thinking per computer was infected and buy unneeded support services from the company.

- Added: 2019-04-11 — Latest reference: 2019-03-21

  The Medtronics Conexus Telemetry Protocol has two vulnerabilities that affect several models of implantable defibrillators and the devices they connect to.

  This protocol has been around since 2006, and similar vulnerabilities were discovered in an earlier Medtronics communication protocol in 2008. Apparently, nothing was done by the company to correct them. This means you can't rely on proprietary software developers to fix bugs in their products.

- Added: 2019-04-09 — Latest reference: 2019-03-28

  Car companies are coming up with a list of clever reasons why they “have to” put cameras and microphones in the car.

  BMW says its software does not store any driver-monitoring information. If this means none of the data that come out of the cameras and microphones can be seen by anyone else, the cameras and microphones are not dangerous. But should we trust this claim? The only way it can deserve rational trust is if the software is free.

- Added: 2019-04-09 — Latest reference: 2019-03-25

  Many Android phones come with a huge number of preinstalled nonfree apps that have access to sensitive data without users' knowledge. These hidden apps may either call home with the data, or pass it on to user-installed apps that have access to the network but no direct access to the data. This results in massive surveillance on which the user has absolutely no control.

- Added: 2019-04-05 — Latest reference: 2019-03-29

  Tesla cars collect lots of personal data, and when they go to a junkyard the driver's personal data goes with them.

- Added: 2019-04-01 — Latest reference: 2019-03-25

The British supermarket Tesco sold tablets which were tethered to Tesco's server for reinstalling default settings. Tesco turned off the server for old models, so now if you try to reinstall the default settings, it bricks them instead.

- Added: 2019-03-28 — Latest reference: 2019-03-20

  A study of 24 “health” apps found that 19 of them send sensitive personal data to third parties, which can use it for invasive advertising or discriminating against people in poor medical condition.

  Whenever user “consent” is sought, it is buried in lengthy terms of service that are difficult to understand. In any case, “consent” is not sufficient to legitimize snooping.

- Added: 2019-03-28 — Latest reference: 2019-03-20

  Volvo plans to install cameras inside cars to monitor the driver for signs of impairment that could cause an accident.

  However, there is nothing to prevent these cameras from doing other things, such as biometrically identifying the driver or passengers, other than proprietary software which Volvo—or various governments and criminals—could change at any time.

- Added: 2019-03-26 — Latest reference: 2017-04-13

  Low-priced Chromebooks for schools are collecting far more data on students than is necessary, and store it indefinitely. Parents and students complain about the lack of transparency on the part of both the educational services and the schools, the difficulty of opting out of these services, and the lack of proper privacy policies, among other things.

  But complaining is not sufficient. Parents, students and teachers should realize that the software Google uses to spy on students is nonfree, so they can't verify what it really does. The only remedy is to persuade school officials to exclusively use free software for both education and school administration. If the school is run locally, parents and teachers can mandate their representatives at the School Board to refuse the budget unless the school initiates a switch to free software. If education is run nation-wide, they need to persuade legislators (e.g., through free software organizations, political parties, etc.) to migrate the public schools to free software.

- Added: 2019-03-23 — Latest reference: 2017-01-27

  A cracker would be able to turn the Oculus Rift sensors into spy cameras after breaking into the computer they are connected to.

  (Unfortunately, the article improperly refers to crackers as “hackers”.)

- Added: 2019-03-13 — Latest reference: 2018-11-30

  In China, it is mandatory for electric cars to be equipped with a terminal that transfers technical data, including car location, to a government-run platform. In practice, manufacturers collect this data as part of their own spying, then forward it to the government-run platform.

- Added: 2019-03-11 — Latest reference: 2019-03-08

  Malware installed into the processor in a hard drive could use the disk itself as a microphone to detect speech.

  The article refers to the “Linux operating system” but seems to mean GNU/Linux. That hack would not require changing Linux itself.

- Added: 2019-03-10 — Latest reference: 2015-07-29

  Game Of War: Fire Age is an iPhone game with addictive features which are based on behavioral manipulation techniques, compounded with group emulation. After a fairly easy start, the game slows down and becomes more difficult, so gamers are led to spend more and more money in order to keep up with their group. And if they stop playing for a while, the equipment they invested in gets destroyed by the “enemy” unless they buy an expensive “shield” to protect it. This game is also deceptive, as it uses confusing menus and complex stats to obfuscate true monetary costs.

- Added: 2019-03-04 — Latest reference: 2019-02-27

  The Ring doorbell camera is designed so that the manufacturer (now Amazon) can watch all the time. Now it turns out that anyone else can also watch, and fake videos too.

  The third party vulnerability is presumably unintentional and Amazon will probably fix it. However, we do not expect Amazon to change the design that allows Amazon to watch.

- Added: 2019-03-04 — Latest reference: 2019-02-14

  The AppCensus database gives information on how Android apps use and misuse users' personal data. As of March 2019, nearly 78,000 have been analyzed, of which 24,000 (31%) transmit the Advertising ID to other companies, and 18,000 (23% of the total) link this ID to hardware identifiers, so that users cannot escape tracking by resetting it.

  Collecting hardware identifiers is in apparent violation of Google's policies. But it seems that Google wasn't aware of it, and, once informed, was in no hurry to take action. This proves that the policies of a development platform are ineffective at preventing nonfree software developers from including malware in their programs.

- Added: 2019-02-28 — Latest reference: 2019-02-23

  Facebook offered a convenient proprietary library for building mobile apps, which also sent personal data to Facebook. Lots of companies built apps that way and released them, apparently not realizing that all the personal data they collected would go to Facebook as well.

  It shows that no one can trust a nonfree program, not even the developers of other nonfree programs.

- Added: 2019-02-28 — Latest reference: 2019-02-08

  The HP “ink subscription” cartridges have DRM that constantly communicates with HP servers to make sure the user is still paying for the subscription, and hasn't printed more pages than were paid for.

  Even though the ink subscription program may be cheaper in some specific cases, it spies on users, and involves totally unacceptable restrictions in the use of ink cartridges that would otherwise be in working order.

- Added: 2019-02-22 — Latest reference: 2019-01-07

  Vizio TVs collect “whatever the TV sees,” in the own words of the company's CTO, and this data is sold to third parties. This is in return for “better service” (meaning more intrusive ads?) and slightly lower retail prices.

  What is supposed to make this spying acceptable, according to him, is that it is opt-in in newer models. But since the Vizio software is nonfree, we don't know what is actually happening behind the scenes, and there is no guarantee that all future updates will leave the settings unchanged.

  If you already own a Vizio “smart” TV (or any “smart” TV, for that matter), the easiest way to make sure it isn't spying on you is to disconnect it from the Internet, and use a terrestrial antenna instead. Unfortunately, this is not always possible. Another option, if you are technically oriented, is to get your own router (which can be an old computer running completely free software), and set up a firewall to block connections to Vizio's servers. Or, as a last resort, you can replace your TV with another model.

- Added: 2019-02-21 — Latest reference: 2019-02-20

  Some portable surveillance devices (“phones”) now have fingerprint sensors in the display. Does that imply they could take the fingerprint of anyone who operates the touch screen?

- Added: 2019-02-20 — Latest reference: 2019-02-04

  Twenty nine “beauty camera” apps that used to be on Google Play had one or more malicious functionalities, such as stealing users' photos instead of “beautifying” them, pushing unwanted and

often malicious ads on users, and redirecting them to phishing sites that stole their credentials. Furthermore, the user interface of most of them was designed to make uninstallation difficult.

Users should of course uninstall these dangerous apps if they haven't yet, but they should also stay away from nonfree apps in general. *All* nonfree apps carry a potential risk because there is no easy way of knowing what they really do.

- Added: 2019-02-13 — Latest reference: 2019-02-06

  Many nonfree apps have a surveillance feature for recording all the users' actions in interacting with the app.

- Added: 2019-02-08 — Latest reference: 2019-02-01

  An investigation of the 150 most popular gratis VPN apps in Google Play found that 25% fail to protect their users' privacy due to DNS leaks. In addition, 85% feature intrusive permissions or functions in their source code—often used for invasive advertising—that could potentially also be used to spy on users. Other technical flaws were found as well.

  Moreover, a previous investigation had found that half of the top 10 gratis VPN apps have lousy privacy policies.

  (It is unfortunate that these articles talk about “free apps.” These apps are gratis, but they are *not* free software.)

- Added: 2019-02-07 — Latest reference: 2019-02-04

  Google invites people to let Google monitor their phone use, and all internet use in their homes, for an extravagant payment of $20.

  This is not a malicious functionality of a program with some other purpose; this is the software's sole purpose, and Google says so. But Google says it in a way that encourages most people to ignore the details. That, we believe, makes it fitting to list here.

- Added: 2019-02-03 — Latest reference: 2019-01-23

  Google is modifying Chromium so that extensions won't be able to alter or block whatever the page contains. Users could conceivably reverse the change in a fork of Chromium, but surely Chrome (nonfree) will have the same change, and users can't fix it there.

- Added: 2019-02-02 — Latest reference: 2018-12-29

  Around 40% of gratis Android apps report on the user's actions to Facebook.

  Often they send the machine's “advertising ID,” so that Facebook can correlate the data it obtains from the same machine via various apps. Some of them send Facebook detailed information about the user's activities in the app; others only say that the user is using that app, but that alone is often quite informative.

  This spying occurs regardless of whether the user has a Facebook account.

- Added: 2019-02-02 — Latest reference: 2018-11-02

  Foundry's graphics software reports information to identify who is running it. The result is often a legal threat demanding a lot of money.

  The fact that this is used for repression of forbidden sharing makes it even more vicious.

  This illustrates that making unauthorized copies of nonfree software is not a cure for the injustice of nonfree software. It may avoid paying for the nasty thing, but cannot make it less nasty.

- Added: 2019-01-28 — Latest reference: 2019-01-11

  Samsung phones come preloaded with a version of the Facebook app that can't be deleted. Facebook claims this is a stub which doesn't do anything, but we have to take their word for it, and there is the permanent risk that the app will be activated by an automatic update.

Preloading crapware along with a nonfree operating system is common practice, but by making the crapware undeletable, Facebook and Samsung (among others) are going one step further in their hijacking of users' devices.

- Added: 2019-01-21 — Latest reference: 2019-01-10

  Until 2015, any tweet that listed a geographical tag sent the precise GPS location to Twitter's server. It still contains these GPS locations.

- Added: 2019-01-15 — Latest reference: 2016-12-29

  In the game Fruit Pop, the player buys boosts with coins to get a high score. The player gets coins at the end of each game, and can buy more coins with real money.

  Getting a higher score once leads the player to desire higher score again later. But the higher score resulting from the boost does not give the player more coins, and does not help the player get a higher score in subsequent games. To get that, the player will need a boost frequently, and usually has to pay real money for that. Since boosts are exciting and entertaining, the player is subtly pushed to purchase more coins with real money to get boosts, and it can develop into a costly habit.

- Added: 2019-01-14 — Latest reference: 2016-12-14

  The Microsoft Telemetry Compatibility service drastically reduces the performances of machines running Windows 10, and can't be disabled easily.

- Added: 2019-01-13 — Latest reference: 2019-01-10

  Amazon Ring “security” devices send the video they capture to Amazon servers, which save it long-term.

  In many cases, the video shows everyone that comes near, or merely passes by, the user's front door.

  The article focuses on how Ring used to let individual employees look at the videos freely. It appears Amazon has tried to prevent that secondary abuse, but the primary abuse—that Amazon gets the video—Amazon expects society to surrender to.

- Added: 2019-01-06 — Latest reference: 2019-01-05

  The Weather Channel app stored users' locations to the company's server. The company is being sued, demanding that it notify the users of what it will do with the data.

  We think that lawsuit is about a side issue. What the company does with the data is a secondary issue. The principal wrong here is that the company gets that data at all.

  Other weather apps, including Accuweather and WeatherBug, are tracking people's locations.

- Added: 2019-01-01 — Latest reference: 2018-12-30

  New GM cars offer the feature of a universal back door.

  Every nonfree program offers the user zero security against its developer. With this malfeature, GM has explicitly made things even worse.

- Added: 2018-12-11 — Latest reference: 2018-12-06

  Facebook's app got “consent” to upload call logs automatically from Android phones while disguising what the “consent” was for.

- Added: 2018-12-04 — Latest reference: 2018-11-27

  Many web sites use JavaScript code to snoop on information that users have typed into a form but not sent, in order to learn their identity. Some are getting sued for this.

  The chat facilities of some customer services use the same sort of malware to read what the user is typing before it is posted.

- Added: 2018-11-13 — Latest reference: 2018-11-10

  Corel Paintshop Pro has a back door that can make it cease to function.

  The article is full of confusions, errors and biases that we have an obligation to expose, given that we are making a link to them.

  - Getting a patent does not “enable” a company to do any particular thing in its products. What it does enable the company to do is sue other companies if they do some particular thing in their products.
  - A company's policies about when to attack users through a back door are beside the point. Inserting the back door is wrong in the first place, and using the back door is always wrong too. No software developer should have that power over users.
  - “Piracy” means attacking ships. Using that word to refer to sharing copies is a smear; please don't smear sharing.

  - The idea of “protecting our IP” is total confusion. The term “IP” itself is a bogus generalization about things that have nothing in common.

    In addition, to speak of “protecting” that bogus generalization is a separate absurdity. It's like calling the cops because neighbors' kids are playing on your front yard, and saying that you're “protecting the boundary line”. The kids can't do harm to the boundary line, not even with a jackhammer, because it is an abstraction and can't be affected by physical action.

- Added: 2018-11-04 — Latest reference: 2018-10-30

  Nearly all “home security cameras” give the manufacturer an unencrypted copy of everything they see. “Home insecurity camera” would be a better name!

  When Consumer Reports tested them, it suggested that these manufacturers promise not to look at what's in the videos. That's not security for your home. Security means making sure they don't get to see through your camera.

- Added: 2018-10-30 — Latest reference: 2018-10-24

  Some Android apps track the phones of users that have deleted them.

- Added: 2018-10-29 — Latest reference: 2018-10-24

  Apple and Samsung deliberately degrade the performance of older phones to force users to buy their newer phones.

- Added: 2018-10-26 — Latest reference: 2018-10-23

  GM tracked the choices of radio programs in its “connected” cars, minute by minute.

  GM did not get users' consent, but it could have got that easily by sneaking it into the contract that users sign for some digital service or other. A requirement for consent is effectively no protection.

  The cars can also collect lots of other data: listening to you, watching you, following your movements, tracking passengers' cell phones. *All* such data collection should be forbidden.

  But if you really want to be safe, we must make sure the car's hardware cannot collect any of that data, or that the software is free so we know it won't collect any of that data.

- Added: 2018-10-22 — Latest reference: 2018-10-15

  Printer manufacturers are very innovative—at blocking the use of independent replacement ink cartridges. Their “security upgrades” occasionally impose new forms of cartridge DRM. HP and Epson have done this.

- Added: 2018-10-11 — Latest reference: 2018-07-31

  A nonfree video game, available through the nonfree Steam client, included a “miner”, i.e. an executable that hijacks the CPU in users' computers to mine a cryptocurrency.

- Added: 2018-10-11 — Latest reference: 2018-05-08

  A cracker used an exploit in outdated software to inject a “miner” in web pages served to visitors. This type of malware hijacks the computer's processor to mine a cryptocurrency.

  (Note that the article refers to the infected software as “content management system”. A better term would be “website revision system”.)

  Since the miner was a nonfree JavaScript program, visitors wouldn't have been affected if they had used LibreJS. Some browser extensions that specifically block JavaScript miners are also available.

- Added: 2018-10-01 — Latest reference: 2018-09-26

  Honeywell's “smart” thermostats communicate only through the company's server. They have all the nasty characteristics of such devices: surveillance, and danger of sabotage (of a specific user, or of all users at once), as well as the risk of an outage (which is what just happened).

  In addition, setting the desired temperature requires running nonfree software. With an old-fashioned thermostat, you can do it using controls right on the thermostat.

- Added: 2018-09-25 — Latest reference: 2018-09-24

  Researchers have discovered how to hide voice commands in other audio, so that people cannot hear them, but Alexa and Siri can.

- Added: 2018-09-22 — Latest reference: 2018-09-14

  Android has a back door for remotely changing “user” settings.

  The article suggests it might be a universal back door, but this isn't clear.

- Added: 2018-09-18 — Latest reference: 2018-09-12

  One version of Windows 10 harangues users if they try to install Firefox (or Chrome).

- Added: 2018-09-15 — Latest reference: 2017-12-06

  Learn how gratis-to-play-and-not-win-much games manipulate their useds psychologically.

  These manipulative behaviors are malicious functionalities, and they are possible because the game is proprietary. If it were free, people could publish a non-manipulative version and play that instead.

- Added: 2018-08-24 — Latest reference: 2018-06-24

  Red Shell is a spyware that is found in many proprietary games. It tracks data on users' computers and sends it to third parties.

- Added: 2018-08-24 — Latest reference: 2005-10-20

  Blizzard Warden is a hidden “cheating-prevention” program that spies on every process running on a gamer's computer and sniffs a good deal of personal data, including lots of activities which have nothing to do with cheating.

- Added: 2018-07-15 — Latest reference: 2018-06-25

  The game Metal Gear Rising for MacOS was tethered to a server. The company shut down the server, and all copies stopped working.

- Added: 2018-02-10 — Latest reference: 2018-03-30

  In MacOS and iOS, the procedure for converting images from the Photos format to a free format is so tedious and time-consuming that users just give up if they have a lot of them.

Proprietary malware

By type

- Addictions
- Back doors
- Censorship
- Coercion
- Coverups
- Deception
- DRM
- Fraud
- Incompatibility
- Insecurity
- Interference
- Jails
- Manipulation
- Obsolescence
- Sabotage
- Subscriptions
- Surveillance
- Tethers
- Tyrants
- In the pipe

By product

- Appliances
- Cars
- Conferencing
- EdTech
- Games
- Mobiles
- Webpages

By company

- Adobe
- Amazon
- Apple
- Google
- Microsoft

Articles

- UHD Blu-ray Denies Your Freedom

Copyright © 2018-2024 Free Software Foundation, Inc.

This page is licensed under a Creative Commons Attribution 4.0 International License.