www.theguardian.com/technology/2015/may/22/malware-viruses-companies-preinstall

Malware is not only about viruses – companies preinstall it all the time

Richard Stallman

Since I started free software in the 80s, developers have grown to routinely mistreat users by shackling behaviour and snooping – but we have ways to resist.

09.33 EDT 04.52 EDT

In 1983, when I started the free software movement, malware was so rare that each case was shocking and scandalous. Now it's normal.

To be sure, I am not talking about viruses. Malware is the name for a program designed to mistreat its users. Viruses typically are malicious, but software products and software preinstalled in products can also be malicious – and often are, when not free/libre.

In 1983, the software field had become dominated by proprietary (ie nonfree) programs, and users were forbidden to change or redistribute them. I developed the GNU operating system, which is often called Linux, to escape and end that injustice. But proprietary developers in the 1980s still had some ethical standards: they sincerely tried to make programs serve their users, even while denying users control over how they would be served.

How far things have sunk. Developers today shamelessly mistreat users; when caught, they claim that fine print in EULAs (end user licence agreements) makes it ethical. (That might, at most, make it lawful, which is different.) So many cases of proprietary malware have been reported, that we must consider any proprietary program suspect and dangerous. In the 21st century, proprietary software is computing for suckers.

What sorts of wrongs are found in malware? Some programs are designed to snoop on the user. Some are designed to shackle users, such as Digital Rights Management (DRM). Some have back doors for doing remote mischief. Some even impose censorship. Some developers explicitly sabotage their users.

What kinds of programs constitute malware? Operating systems, first of all. Windows snoops on users, shackles users and, on mobiles, censors apps; it also has a universal back door that allows Microsoft to remotely impose software changes. Microsoft sabotages Windows users by showing security holes to the NSA before fixing them.

Apple systems are malware too: MacOS snoops and shackles; iOS snoops, shackles, censors apps and has a back door. Even Android contains malware in a nonfree component: a back door for remote forcible installation or deinstallation of any app.

www.theguardian.com/technology/2015/may/22/malware-viruses-companies-preinstall

What about nonfree apps? Plenty of malware there. Even humble flashlight apps for phones were found to be reporting data to companies. A recent study found that QR code scanner apps also snoop.

Apps for streaming services tend to be the worst, since they are designed to shackle users against saving a copy of the data that they receive, as well as making users identify themselves so their viewing and listening habits can be tracked.

The Free Software Foundation reports on many more cases of proprietary malware.

Microsoft tightens privacy policy after admitting to reading journalist's emails

What about other digital products? We know about the smart TV and the Barbie doll that transmit conversations remotely. Proprietary software in cars that stops those we used to call "car owners" from fixing "their" cars. If the car itself does not report everywhere you drive, an insurance company may charge you extra to go without a separate tracker. Meanwhile, some GPS navigators save up where you have gone in order to report back when connected to update the maps.

Amazon's Kindle e-reader reports what page of what book is being read, plus all notes and underlining the user enters; it shackles the user against sharing or even freely giving away or lending the book, and has an Orwellian back door for erasing books.

Should you trust an internet of proprietary software things?
Don't be an ass.

The companies that sell malware are skilled at spinning the malfunctionalities as services to the consumer but they could offer most of these services with freedom and anonymity if they wanted to.

It is fashionable to recognise the viciousness of today's computing only to declare resistance unthinkable. Many claim that no one could resist gratification for mere freedom and privacy. But it's not as hard as they say. We can resist:

Individually, by rejecting proprietary software and web services
that snoop or track.

Collectively, by organising to develop free/libre replacement systems and web services that don't track who uses them.

Democratically, by legislation to criminalise various sorts of malware practices. This presupposes democracy, and democracy requires defeating treaties such as the TPP and TTIP that give companies the power to suppress democracy.