BEST BEFORE DATE POLICY BRIEF: Device sustainability through long-term software support

September 2021

privacyinternational.org

ABOUT PRIVACY INTERNATIONAL

Governments and corporations are using technology to exploit us. Their abuses of power threaten our freedoms and the very things that make us human. That's why Privacy International campaigns for the progress we all deserve. We're here to protect democracy, defend people's dignity, and demand accountability from the powerful institutions who breach public trust. After all, privacy is precious to every one of us, whether you're seeking asylum, fighting corruption, or searching for health advice.

So, join our global movement today and fight for what really matters:
our freedom to be human.

Privacy International
62 Britton Street, London EC1M 5UY, United Kingdom
Phone +44 (0)20 3422 4321

privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).

BEST BEFORE DATE POLICY BRIEF:

DEVICE SUSTAINABILITY THROUGH LONG TIME SOFTWARE SUPPORT

Our environment is increasingly populated by devices connected to the Internet, from computers and mobile phones to sound systems and TVs to fridges, kettles, toys, or domestic alarms. There has been research into the negative safety and privacy impacts of inadequate security provided by the software in such devices[1]. This is also the case with **outdated security, a risk enabled by software support periods that are shorter than a product's usable life cycle and an industry focused on selling its future products.** Additionally, this common practice contributes to the growing pile of global electronic waste and damage to our environment.

Introduction and problem

The global generation of electrical and electronic waste (e-waste) is growing exponentially. Every year more and more consumers buy new devices, or replace their malfunctioning, broken or out-of-date phones, computers, TVs and other electronics, generating e-waste at a huge scale - an increase of 2.5 million metric tons (Mt) on average every year globally.

Around the world, people generated some 53 million tons of e-waste in 2019, projected to grow to a staggering 74.7 million tons by 2030[2]. Recycling cannot

1 For example, as far back as 2016 Norway Consumer Council found serious security flows in a doll named Cayla that triggered IoT safety concerns round the world; a second investigation into children's smart watches showed similar concerning results: https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws. Recently, a UK report by the STEaPP department of the University College London highlighted the dangers posed by lack of connected device security in cases of domestic abuse, fitness apps as well as connected children's toys: https://bit.ly/3hgVH0N.

keep up, even where infrastructures are developed: only 17.4% of 2019's global e-waste was collected and recycled formally[3]. In fact, much of e-waste is exported illegally from high income to lower income countries or is mixed up with other waste and ends up improperly disposed of in landfills where toxins common in electronics like lead, mercury and cadmium can leach out and contaminate surrounding soils and groundwater.

Although it has the highest collection and recycling rate in the world, at 42.5% of total waste, **Europe ranks first worldwide in terms of e-waste generation per capita** (16.2 kg), so its mandated recycling schemes, however efficient, simply cannot keep up with the rate of new e-waste generation which is fuelled not just by increased consumption, but also by in-built short life cycles of devices (so called 'planned obsolescence') and few repair options[4].

In the face of this problem, consumers and environmental organisations, movements such as the Right to Repair,[5] demand that manufacturers are mandated to improve device sustainability and to tackle this acute environmental threat. And there is increased realisation amongst policy makers and legislators, that such measures cannot be left to producer initiatives and voluntary codes or guidelines alone, but must be tackled by adopting legally binding measures, developed holistically and cooperatively, given that this is a global problem.

2 Forti V., Baldé C.P., Kuehr R., Bel G. The Global E-waste Monitor 2020: Quantities, flows and the circular economy potential. United Nations University (UNU)/United Nations Institute for Training and Research (UNITAR) – co-hosted SCYCLE Programme, International Telecommunication Union (ITU) & International Solid Waste Association (ISWA), Bonn/Geneva/Rotterdam: https://www.itu.int/en/ITU-D/Environment/Documents/Toolbox/GEM_2020_def.pdf.

3 Ibid.

4 Ibid.

5 Right to repair: https://repair.eu.

What is Hardware and Software

Modern electronic devices require two main parts to function: the hardware and the software. The hardware usually refers to physical electronic pieces inside a device (usually a collection of microchips, logic gates and specialised processing chips, such as those to process radio waves for communication, or process audio for sound) while the software is the set of instructions that tells the device what to do. Hardware without software don't do anything (a computer without an Operating System such as Windows or MacOS can't run anything) and software without hardware have nothing to send instructions to (a copy of windows or MacOS is useless without a computer to run it on).

Motherboards, graphic cards, monitors and hard disk drives are all examples of hardware contained in a computer that are useless without software. On the other hand, Microsoft Windows (or any other operating system like macOS or Linux), internet browsers (like Mozilla Firefox or Safari), applications like Instagram or Spotify, and drivers for sound- or graphic cards are all examples of software.

Software - key to device sustainability

While initiatives to extend the useful life of the hardware are crucial in addressing this problem, our devices aren't only made of hardware. Software, from the operating system (such as Android, iOS, Windows etc.) to the microchip firmware (low-level software for specific hardware such as a smartphone camera), is what keeps our devices secure, functional, compatible with the latest apps and protected against known security vulnerabilities.[6]

6 See Annex A: Software update explainer.

Out-of-date software on devices leave people vulnerable to hackers and cyber-attacks, often depriving them of critical services and resulting in significant financial losses and emotional distress. Consumers' digital data is also at risk.

An out-of-date software on an otherwise functioning device can be a door to one's bank account or the intimacy of one's life, render a device unusable, or worst still endanger safety and life even.[7] Such a risk is enabled by software support periods that are shorter than the product's usable life cycle, and an industry focused only on selling its latest products rather than supporting earlier models. In other words, current market economics merely encourage the replacement of perfectly functioning devices. This does not only create extra e-waste, but it also puts people at risk. Both can be avoided.

When purchasing devices and services, it is often unclear until when these will be supported with software updates. We found reported examples of only a few companies being upfront and disclosing how many years a device will receive software and security updates for (see Principles, below), including Apple and Google.[8]

But even when this information is public it is not easily accessible to the consumer. An investigation by Which?, the UK consumer organisation, into how long major smart home appliance manufacturers will provide updates for the connected products, revealed that none published their update policies for consumers to see.[9] And even if disclosed, this information can still be vague or confusing, allowing manufacturers to sell devices with "out-of-date" software, often at a discount, at the expense of consumers' rights.

7 See, for example, UK report (note 1) which, inter alia, investigates Internet of Things (IoT) facilitated Tech abuse, lack of (or outdated) security allowing perpetrators to control, coerce and abuse: https://bit.ly/3hgVH0N.

8 Google devices include Nexus smart phones, Pixel phones, Chromebooks and Google Home.

9 Which?, Security updates for smart appliances could end after just two years, finds Which? (8 June 2020): https://www.which.co.uk/news/2020/06/the-truth-behind-smart-appliance-security-updates.

What is an Operating System (OS)?

An operating system is a core programme that manages the interactions between other programmes and the hardware. It usually consists of a core (also known as kernel) which enumerates the available hardware. It provides a scheduler which tries to balance the contention of multiple tasks (applications) being run simultaneously around the ability of the processor (the brain of the device) usually only being able to run one task at a time. For example, the Operating System will make sure that launching an app such as the web browser won't interrupt the sound being played by another application. Modern operating systems like Windows, Android, iOS or Linux also usually bundle a number of ancillary services such as the user interface and basic utilities for the device. This includes for example a sound managing interface to set the volume of applications playing on the device or a network interface to easily connect to WIFI networks.

The concerns around the impact of software updates on electronics' sustainability is increasingly on the radar of campaigners and policymakers. A few point out to the important distinction between security and functionality updates,[10] and the need to differentiate between the two when mandating policy measures related to the lifetime of devices. Security updates are always essential and subject to cybersecurity guidelines or legislative measures, whereas functionality updates are not necessarily essential to the functioning of an 'older' device; they may in fact slow it down and therefore actively encourage users to replace it. Apple, for example, was famously subject to multiple class actions in the US and litigation and fines in the EU for its slowing down of older iPhone 6 and 7 via software functionality updates.[11]

10 For example, the French organisation HoP (Stop planned Obsolescence) in its White Paper: https://www.halteobsolescence.org/wp-content/uploads/2020/11/Livre-Blanc-europeen.pdf (Proposal 02).

11 BBC News, Apple fined for slowing down old iPhones (7 February 2020): https://www.bbc.co.uk/news/technology-51413724; BBC News, Apple settles iPhone slowdown case for $500m (2 March 2020): https://www.bbc.co.uk/news/technology-51706635; Kim Lyons, Apple faces yet another lawsuit over throttling iPhones (The Verge, 25 January 2021): https://www.theverge.com/2021/1/25/22248408/apple-class-action-suit-throttling-iphone-europe.

What are software updates and what do they do?

A software update (also known as patch) is a set of changes to a software to update, fix or improve it. Changes to the software will usually either fix bugs, fix security vulnerabilities, provide new features, or improve performances and usability. Depending on the software, updates can either be installed manually or automatically if the device is connected to the internet and has the appropriate capabilities (for instance, an Android phone that updates its software on its own). Software updates are particularly important when applied to the Operating System given the reliance of other software (such as apps or drivers) on it. For example, a major release of an Operating System such as Android or iOS might render several apps obsolete, if all version released after the update aren't compatible with the previous version of the OS. This could prevent people from accessing important services as illustrated with some covid-19 track and track apps which were only compatible with specific versions of iOS and Android. From a security standpoint, software updates have important implications. When an update includes a fix for security vulnerabilities, any device running an out-of-date version of the software is particularly vulnerable. This allows malicious actors to know what vulnerabilities exist on a given system and, consequently, puts devices running this software (version) more at risk. For example, using an outdated version of Android (such as version 4) means that all the security vulnerabilities spotted and fixed in following versions still exist on any device that uses the older version 4.

We believe that security and protecting the environment should go hand in hand, and consumers should not be forced to sacrifice the latter to achieve the former. This means a synchronized relationship between the expected lifespan of a device hardware and its security software, with functionality updates clearly explained and left to user choice if not essential for older devices.

It is the responsibility of manufacturers and software vendors to enable long time software support and be transparent about their own practices, but this responsibility needs to be mandated as evidence shows that it is not being done voluntarily.

Five principles for software update

Privacy International is proposing a set of principles that should govern the software update policy of connected devices. These principles aim to encompass and add an additional layer to existing environmental impact standards. We believe that they should be legally mandated and enforceable, upheld by manufacturers and be effectively overseen and enforced:

1. Devices should be designed in an environmentally sustainable manner

Known as eco-design or design for sustainability (D4S) and defined as "the integration of environmental aspects into the product development process, by balancing ecological and economic requirements. Eco-design considers environmental aspects at all stages of the product development process, striving for products which make the lowest possible environmental impact throughout the product life cycle".[12]

Eco-design in the case of connected digital products should include essential elements, such as in-built durability, repairability, reusability and re-cyclability using minimum resources, and crucially have key functionalities maintained and be secure to use.

12 European Environment Agency (after UNEP), eco-design: https://www.eea.europa.eu/help/glossary/eea-glossary/eco-design.

Good practice example:

Fairphone produces entirely repairable and upgradable phones (obtaining 10/10 repairability score from the independent organisation iFixtIt) while using fairer, recycled, and responsibly mined materials to increase industry and consumer awareness. They prove that designing and selling such device is possible and a viable business model.[13]

2. Device manufacturers, software vendors and service providers at a minimum should provide software security and key functionality updates for the expected lifespan of a product, while the nature and purpose of non-essential functionality updates and their impact on the performance of the device should be clearly stated and left to user choice.

This shall include:

- providing support for OS updates.
- providing security updates for drivers and firmware.

Lack of software updates might also negatively impact device functionality, for example, by making some functions obsolete (e.g., a browser that does not support the latest security protocols and thus can't display websites properly). It might also mean that identified bugs or problems might not be fixed (e.g., poor battery).

13 Georgina Guiney, E-Waste Nightmare: Cell Phones Getting Greener But Not There Yet (EarthTalk, 9 June 2017): https://earthtalk.org/e-waste.

Need for extended software support

Which? research carried out on Android devices in 2020 revealed that a staggering two in five (40%) of Android users worldwide are no longer receiving security updates from Google, and therefore at risk of data theft, ransom demands and malware attacks. These smartphones are not necessarily old models and still available to buy, but consumers are not aware of the risks.[14]

Older **Apple** Macs' security updates are also unsatisfactory - fixes are provided mainly for the latest version of their operating system, OS X (El Capitan). Older versions receive no security updates, or only for a few known vulnerabilities.[15]

In the meantime, other device manufacturers will only provide an emergency security patch when a particularly damaging bug is in circulation, such as the one known as 'stage-fright' infecting Android phones. Only recent flagship phones were being 'patched' against the virus, but not older and cheaper phones.[16]

However, extended security updates are possible and can be mandated.

Recent updates of EU eco-design regulations for televisions mandates manufacturers to provide firmware and security updates for eight years from the last unit of a model being put on the market; consumers must be informed re period of updates.[17]

14 Which?, Void Android: More than one billion Android devices at risk of hacking attacks (6 March 2020): https://press.which.co.uk/whichpressreleases/void-android-more-than-one-billion-android-devices-at-risk-of-hacking-attacks.

15 CERN, Computer Security: Mac security: nothing for old versions (1 April 2016): https://home.cern/news/news/computing/computer-security-mac-security-nothing-old-versions.

16 Chris Hoffman, Android's Stagefright Exploit: What You Need to Know and How to Protect Yourself (How-to Geek, 12 August 2015): https://www.howtogeek.com/225834/stagefright-what-you-need-to-know-and-how-to-protect-yourself.

17 Commission Regulation (EU) 2019/2021 of 1 October 2019 laying down ecodesign requirements for electronic displays pursuant to Directive 2009/125/EC of the European Parliament and of the Council, amending Commission Regulation (EC) No 1275/2008 and repealing Commission Regulation (EC) No 642/2009 (Text with EEA relevance), OJ L 315: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:OJ.L_.2019.315.01.0241.01.ENG.

3. Device manufactures, and software vendors should explicitly and prominently announce their end-of-life date for software support when sold (Best by Date or BBD), on the packaging, as well as in the product description available to users before they buy, online or in-store.

The date of expiry should be clear on purchase, as well as the defining factor for such date, i.e., the precise date rather than "1 year update support", and precise factor such as security or functionality updates e.g. "End of OS support".

Current BBD practices:

The current situation is patchy, with practices varying among manufacturers and software vendors, and very few give clear, or any, information to consumers. We searched but struggled to find update policies for different kind of devices, and most often we could not find any clear ones.

- Older Apple iPhones receive security updates for up to seven years after they go out of production. The software update was released in December 2020 to ensure support for its Covid-19 Bluetooth contact tracing function. The iPhone 5S ceased sales in 2014.[18]
- In August 2020 Samsung has announced that it will be providing at least three major Android updates to its flagship smartphones. Even then this information was reportedly hidden in the fine print.[19]
- Fitbit Legacy Device Policy states that "Our devices typically receive software updates for at least two years after the device is last sold on Fitbit.com" and provide a list of legacy products. Looking at this list, the life of expectancy of the product can be placed between 5 and 8 years.

18 Nicole Lee, Apple's iOS 12.5 adds COVID-19 exposure notifications for older iPhones (Engadget, 14 December 2020): https://www.engadget.com/apple-ios-125-adds-covid-19-exposure-notification-older-iphones-213616636.html?guccounter=2.

19 Ben Schoon, Samsung will provide at least 3 major Android updates to every flagship since the Galaxy S10 (9TO5Google, 5 August 2020): https://9to5google.com/2020/08/05/samsung-android-updates-3-year-promise/

4. Device manufacturers and software vendors should design the software running on the devices they sell to be sustainable and maintainable

Software and OS compatibility should not be the determining factor in the end of life of a product. Modern operating systems provide solutions for updates for an extended period and such solutions should be preferred and implemented.

Modern solutions for software updates

Google project **Treble for Android** (first available with Android 8) is a way to separate the implementation of Android drivers or software from the main Android codebase. This effectively makes it easier for manufacturers to update their devices as they don't need to recompile Google's entire Android code every time an update is released by Google.[20]

The operating system **Windows 10** is said to run on "the broadest range of devices ever," from small Internet of Things gadgets set up in offices and homes, to game consoles, to handheld tablets and phones, to computer servers that drive websites and other business software inside massive data centres. This would mean that, contrary to Apple, for example, which provides Mac OS for desktops and iOS for mobile devices, all different types of devices (e.g., wearables, consoles, tablets, laptops, phones, desktops and servers) will be running on the same core operating system code. While the latter will be the same for all devices, each device would still require an individualised software version, due to its unique characteristics.[21] This translates into the real world with a variety of versions of MS Windows 10 running on a very high number of devices ranging from most commercial computers to Windows Server running on cloud infrastructures to Windows 10 IoT Core, which runs on very limited hardware such as Raspberry Pi, a low cost, credit-card sized computer that plugs into a computer monitor or TV, and uses a standard keyboard and mouse.[22]

20 Iliyan Malchev, Here comes Treble: A modular base for Android (Android Developers Blog, 17 May 2017): https://android-developers.googleblog.com/2017/05/here-comes-treble-modular-base-for.html; JR Raphael, What is Project Treble? The Android upgrade fix explained (Computerworld, 1 April 2020): https://www.computerworld.com/article/3306443/what-is-project-treble-android-upgrade-fix-explained.html.

21 Cade Metz, Windows 10 Will Run Everywhere. But What Does That Mean? (Wired, 10 January 2014): https://www.wired.com/2014/10/windows-10-will-run-everywhere-mean.

22 Rapsberry Pi: https://www.raspberrypi.org.

5. Open-source practices should be encouraged to allow consumers to maintain devices, however not at the expense of commercial support

Devices may have a hardware life expectancy longer that the announced software BBD. Manufacturers should enable any potential use of the device after the BBD by allowing users and other third parties to access and maintain the device's software.

Examples of Open Source and alternative software support to product lifespan

webOS is an Operating System that was originally developed by Palm for its Personal Digital Assistant (PDA) devices. After acquiring Palm in 2010, HP announced that it would release webOS under an open-source license. HP later sold webOS to LG Electronics for them to use it on their web-enabled smart TVs. Today, LG has expanded the use of the webOS from smart TVs to IoT devices.[23] And to further expand its reach and lure developers, LG has launched an open-source version of webOS called webOS OSE (Open Source Edition).[24]

The **Pinephone** is one of the latest attempts at creating an entirely open-source phone. The purpose of the PinePhone isn't only to deliver a functioning Linux phone to end-users, but also to actively create a market for such a device, as well as to support existing and well-established Linux-on-Phone projects. All major Linux Phone-oriented projects, as well as other FOSS OS', are represented on the PinePhone and developers work together on our platform to bring support this this community driven device.[25]

OpenWRT is an open-source Linux-based Operating System designed for commercial routers. It has found success not only because of its features and stability, but also because it provides a secure and maintained alternative to the Operating System that might come pre-installed on commercial routers. OpenWRT will usually receive updates long after a device default OS has stopped receiving updates.

23 LG, A World of Premium Content: https://www.lg.com/us/experience-tvs/smart-tv/use.

24 WebOS OSE, On-ramp to the Future of Smart Devices: https://www.webosose.org.

25 Pine64, PinePhone: https://www.pine64.org/pinephone.

Recommendations for EU institutions:

A number of important policy initiatives are in progress at an EU level, which have the potential to address the sustainability of connected devices[26].
Relevant pieces of planned legislation over the next two years include: a planned review of the Eco-design Directive; setting rules for electronics and ICT (under the Circular Electronics Initiative); as well as setting rules for environmental information for consumers via "Empowering consumers for the green transition" proposed legislation. Enhanced software security will also be addressed in an all-encompassing horizontal regulation for Internet-connected devices, being considered under the EU cybersecurity strategy.[28]

26 The European Commission published the Green Deal in 2019, with the aim of reaching carbon-neutrality by 2050: https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal/actions-being-taken-eu_en. The Circular Economy Action plan and the Sustainable Products Initiative are part of this plan: https://ec.europa.eu/environment/pdf/circular-economy/new_circular_economy_action_plan.pdf; https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12567-Sustainable-products-initiative_en.

27 European Commission, Sustainable product policy & ecodesign: https://ec.europa.eu/growth/industry/sustainability/product-policy-and-ecodesign_en.

28 European Commission, The EU's Cybersecurity Strategy in the Digital Decade: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade.

Rules on software sustainability reflecting the above principles must be included in these forthcoming legislative proposals. In particular, the proposed legislation should:

- Mandate an extended software security support period, at a minimum for the expected lifespan of a connected device or product.
- Mandate provision of extended operating system (OS) updates to the latest version, at a minimum for the expected lifespan of a connected device or product.
- Include obligation for software vendors to separate security and functionality updates, with clear information re the necessity or effect of each. Users should have the option to reject or uninstall functionality updates that may affect the performance of their device.
- Mandate Best Before Date labelling: explicit and prominent information on the product and at the point of sale regarding the period of time the software of the device or IoT product will be supported; explicit means a finite date both for the security and the OS updates.
- Request manufacturers and software vendors to permit lifespan extension or repair options at the end of their support period, either by publishing the source code (open source) or by allowing for alternative software to be installed on the device at the end of support.
- Ensure manufacturers and software vendors give clear, simple and accessible information for users to include installation of updates, reason for the updates, impacts on functionality and possible repair or disposal options once the support period ends.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org