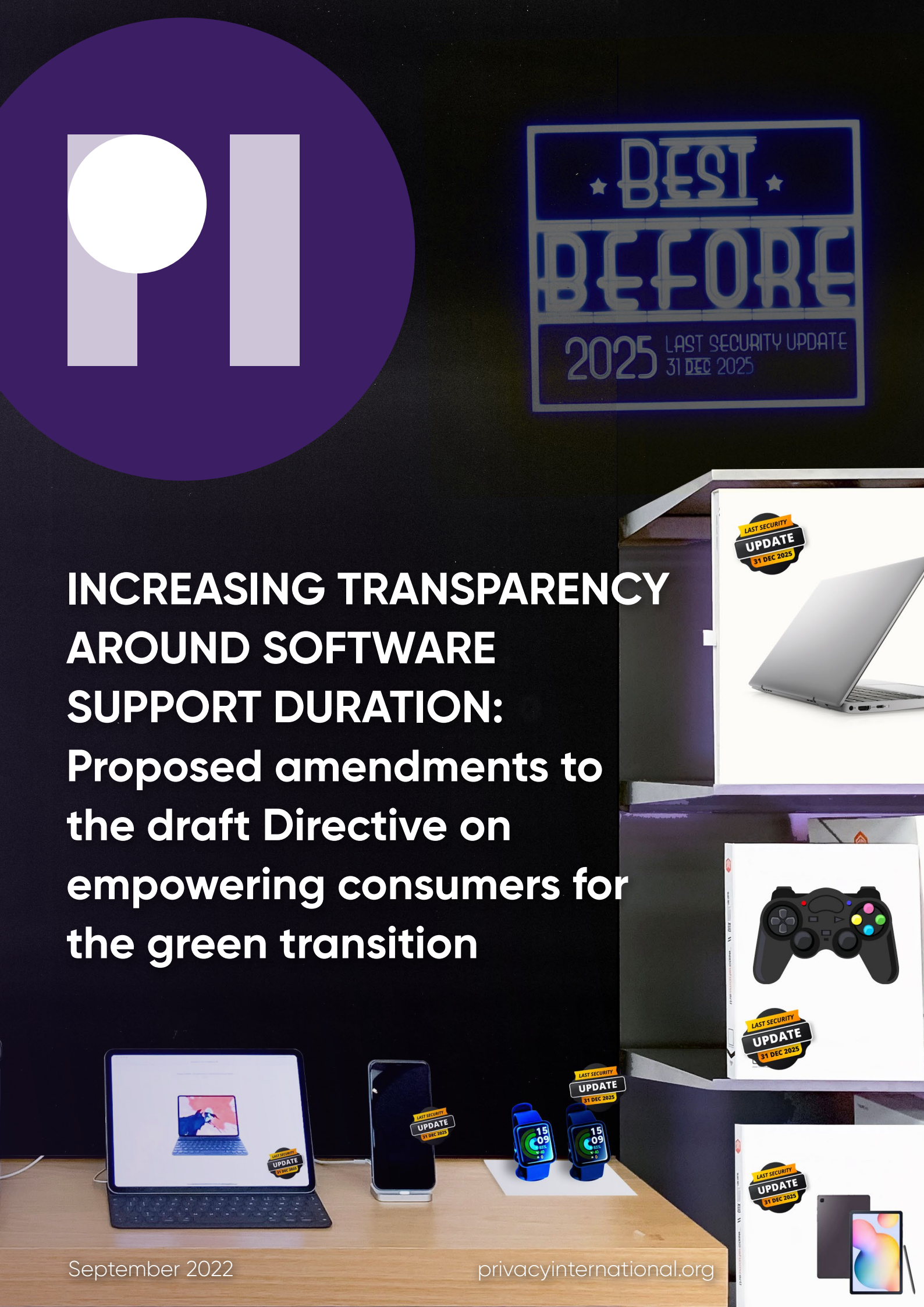

INCREASING TRANSPARENCY AROUND SOFTWARE SUPPORT DURATION: Proposed amendments to the draft Directive on empowering consumers for the green transition

September 2022

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.

Open access. Some rights reserved.

Privacy International wants to encourage the circulation of its work as widely as possible while retaining the copyright. Privacy International has an open access policy which enables anyone to access its content online without charge. Anyone can download, save, perform or distribute this work in any format, including translation, without written permission.This is subject to the terms of the Creative Commons Licence Deed: Attribution-Non-Commercial-No Derivative Works 2.0 UK: England & Wales. Its main conditions are:

- You are free to copy, distribute, display and perform the work;
- You must give the original author ('Privacy International') credit;
- You may not use this work for commercial purposes;
- You are welcome to ask Privacy International for permission to use this work for purposes other than those covered by the licence.

Privacy International is grateful to Creative Commons for its work and its approach to copyright.

For more information please go to www.creativecommons.org.

Photo by Aedrian on Unsplash

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).

INCREASING TRANSPARENCY AROUND SOFTWARE SUPPORT DURATION:

Proposed amendments to the draft Directive on empowering consumers for the green transition

September 2022

INTRODUCTION

Privacy International welcomes the aim of the Directive on empowering consumers for the green transition to enhance consumer rights, particularly by ensuring that consumers obtain reliable and useful information on products, including on their lifespan. Nevertheless, we note that the proposal put forward by the European Commission contains certain shortcomings with regard to information on software support duration and the bundling of security with functionality or any other software updates, which are detailed below. It is crucial that these are effectively addressed by the European Parliament through the introduction of specific amendments to ensure that the aim of the Directive is not undermined, and that consumers' devices and data remain secure in our connected world.

Privacy International (PI) is a global, not-for-profit organization that campaigns against companies and governments who exploit our data and technologies. We do not accept any funding from industry, and we have a strict policy about the circumstances under which we accept grants in order to ensure our independence from state actors and private organizations. Given our leading and respected status as a voice on issues of data and privacy, we are frequently called upon to give expert evidence to parliamentary and government committees. Among others, we have advised and reported to the Council of Europe, the European Parliament, the Organisation for Economic Co-operation and Development and the UN Office of the High Commissioner for Human Rights.

Software is what keeps our devices secure, functional, compatible with the latest apps, and protected against known security vulnerabilities. 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. 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 providing long-term software support for their older products.

In March 2022, the European Parliament established a Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware, following a series of revelations that reported NSO Group's Pegasus software was being used against journalists, activists and politicians in numerous countries across the world including in Europe. The use of extremely intrusive surveillance technologies, such as the ones offered by NSO Group, very often rely on the exploitation of vulnerabilities found in out-of-date software.

> *"With Android phones, the main problem is that many of the Android OEMs don't ship patches [i.e., updates] and the majority of Android phones out there at any one time are insecure. The reason for this is the typical Android vendor only keeps on updating Android for so long as that particular model of phone is on sale and as soon as they are selling a new one, they stop shipping updates.* ***The underlying issue here is how long is a particular product going to be patched, and it's the same as the issue the European Parliament was wrestling with 3 years ago. The way to fix this... is mandating 'death dates' on devices…"***
>
> **Ross Anderson, Professor of Security Engineering, University of Cambridge**

Moreover, as our research demonstrates, it is often extremely difficult -or even impossible- for consumers to precisely know how long the software on their digital products will be supported for by manufacturers. **Lack of meaningful information in both online and offline stores, both at the point of purchase or afterwards, is one of the main problems encountered by EU consumers when purchasing a connected product.** This is not a sporadic phenomenon; it is a practice deployed by most dominant actors in the digital markets for various categories of popular products. Therefore, **the text of the draft Directive should be improved with amendments to ensure that current company practices do not result in serious harms for consumers or negatively impact devices' sustainability.**

The remainder of this submission addresses what PI believes to be the two main concerns that the draft Directive raises and consequently require specific amendments.

CONSUMERS SHOULD BE PROVIDED WITH CLEAR INFORMATION ABOUT HOW LONG THEIR DEVICES WILL BE SUPPORTED WITH SECURITY AND SOFTWARE UPDATES

Out-of-date software on devices leaves 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. Therefore, it is essential that the Directive demands that consumers are given clear and specific information about how long the software on their connected products will be supported for by the producer.

Currently, the EU regulatory landscape requires that connected devices receive software updates for the period of time that consumers can reasonably expect, which is often wrongly linked to the legal guarantee period (2 years). In addition, the text of the draft Directive assumes that consumers are familiar with the above obligations of manufacturers and imposes information obligations only for software updates whose duration is more than "the duration of the commercial guarantee of durability, to avoid unnecessary information for consumers". As the Explanatory Memorandum notes, this way the draft Directive hopes to "incentivise producers to offer commercial guarantees of durability longer than two years by obliging traders to provide information at the point of sale on the existence (or absence in the case of energy-using goods) and length of the commercial guarantees of durability provided by producers".

While the introduction of such information obligations is, generally, in favour of consumers, it relies on the fact that consumers are already aware that their

devices will be supported for a minimum of 2 years, which does not appear to be the case. For example, a 2015 European Commission study on legal and commercial guarantees found that only 41% of respondents knew that the length of the legal guarantee period is 2 years, while "in about half of the Member States, respondents who thought that the legal guarantee period was one year outnumbered those knowing that the length of the legal guarantee period is two years". In a similar vein, a 2020 document by Consumer PRO, a European Commission initiative underlines:

> *"There is a great deal of confusion for consumers between the legal guarantee of conformity and the so-called commercial guarantees. In practice, very often, traders do not inform consumers about the legal guarantee of conformity even though it is an obligation..".*

When purchasing devices and services, it is often unclear how long these will be supported with software updates. The current landscape is characterised by varying and inconsistent approaches between either security or functionality updates, as well as with software support periods that differ with regard both to product category as well as among the same connected devices. In addition, information about how long connected devices will be supported with either functionality or security updates, or both, is rarely provided to consumers at the point of purchase and will very often be missing from the companies' website. However, even when this information is disclosed it is not always easily accessible to the average consumer. This practice allows manufacturers to sell devices with "out-of-date" software, often at a discount, at the expense of consumers' rights. Therefore, the text of the Directive should be amended to ensure that consumers are aware of manufacturers' obligation to provide software support for their devices for a minimum of two years from the point of sale.

AMENDMENT 1
PROPOSAL FOR A DIRECTIVE

Article 2(2), point ec

Text proposed by the Commission	**Amendment**
(ec) for goods with digital elements, where the producer makes such information available, the minimum period in units of time during which the producer provides software updates, unless the contract provides for a continuous supply of the digital content or digital service over a period of time. Where information about the existence of a commercial guarantee of durability is provided in accordance with point (ea), the information on the updates shall be provided if those updates are supplied for a longer period than the commercial guarantee of durability;	(ec) for goods with digital elements, the minimum period ***from the point of sale*** in units of time during which the producer provides software updates, unless the contract provides for a continuous supply of the digital content or digital service over a period of time. Where information about the existence of a commercial guarantee of durability is provided in accordance with point (ea), the information on the updates shall be provided ***regardless of whether*** those updates are supplied for a longer period than the commercial guarantee of durability;

AMENDMENT 2
PROPOSAL FOR A DIRECTIVE

Article 2(3), point mc

Text proposed by the Commission	**Amendment**
(mc) for goods with digital elements, where the producer makes such information available, the minimum period in units of time during which the producer provides software updates, unless the contract provides for a continuous supply of the digital content or digital service over a period of time. Where information about the existence of a commercial guarantee of durability is provided in accordance with point (ma), the information on the updates shall be provided if those updates are supplied for a longer period than the commercial guarantee of durability;	(mc) for goods with digital elements, the minimum period ***from the point of sale*** in units of time during which the producer provides software updates, unless the contract provides for a continuous supply of the digital content or digital service over a period of time. Where information about the existence of a commercial guarantee of durability is provided in accordance with point (ma), the information on the updates shall be provided ***regardless of whether*** those updates are supplied for a longer period than the commercial guarantee of durability;

INFORMATION ABOUT SECURITY UPDATES SHOULD BE DECOUPLED FROM INFORMATION ON FUNCTIONALITY UPDATES AND SHOULD BE PROVIDED BY PRODUCERS TOO

The current wording of the Draft Directive only partially addresses the issue of unfair practices and puts consumers' digital safety at risk. By allowing companies to bundle functionality and security updates, it imposes a choice for consumers between performance degrading updates and lack of security. At the same time, manufacturers are excluded from the scope of the information obligations, although they are usually the ones responsible for providing connected products with updates.

The draft Directive treats security updates the same as functionality updates, under the term "software updates" (see, for example, Recital 15 and Article 1(1)(w)). Recital 15 prohibits traders from omitting to inform consumers "that a software update, including a security update, will negatively impact the use of goods with digital elements or certain features of those goods, even if the update improves the functioning of other features", when they invite them to update their software. Finally, the Annex of the draft Directive seeks to amend current EU laws on commercial practices that are considered unfair (Directive 2005/29/EC) to include "omitting to inform the consumer that a software update will negatively

impact the use of goods with digital elements or certain features of those goods even if the software update improves the functioning of other features".

First, the text of the draft Directive makes no reference to producers of connected products. Instead, it provides that traders will be responsible for providing information about the duration of software support that devices will receive. As well as having responsibility for failing to inform consumers about the negative impact of software updates on a device's functionality, **it is necessary that such information obligations are imposed not only on traders but also on producers of digital products, as it is the producer who is responsible for providing devices with software updates.**

Second, it is vital that the Directive draws a distinction between security and functionality updates. Security updates are essential and subject to cybersecurity guidelines or legislative measures, whereas functionality updates can negatively impact on the functionality of the device by, for example, effecting the speed at which the device functions. This distinction is necessary as security software should not be expected to degrade the performance or functionality of a device. PI's research has further illustrated that "bundling" updates has become commercial practice and has been largely embraced by big tech companies. This is particularly evident in the context of data privacy. Most recently, Apple's iOS 15.6 update for iPhones included both enhancements and security patches, which were installed by virtue of the same update. Likewise, Google's Android December 2021 update for Google Pixel phones included both security patches as well as performance improvements for devices.

While not within the scope of this Directive, PI believes **security updates should be offered separately from any other software updates, including functionality updates**. Security updates are essential to keep consumers safe and do not degrade the functionality or performance of devices.

AMENDMENT 3
PROPOSAL FOR A DIRECTIVE

Recital 15

Text proposed by the Commission	**Amendment**
(15) It should be prohibited to omit to inform the consumer that a software update, including a security update, will negatively impact the use of goods with digital elements or certain features of those goods, even if the update improves the functioning of other features. For example, when inviting consumers to update the operating system on their smartphone, the trader will have to inform the consumer if such an update will negatively impact the functioning of any of the features of the smartphone.	(15) It should be prohibited to omit to inform the consumer that a software update, including a security update, will negatively impact the use of goods with digital elements or certain features of those goods, even if the update improves the functioning of other features. For example, when inviting consumers to update the ***producer should provide consumers with the option to only download the security updates, if the entire update will negatively impact the functioning of any of the features of their device.***

AMENDMENT 4
PROPOSAL FOR A DIRECTIVE

Recital 22

Text proposed by the Commission	**Amendment**
(22) In order for consumers… before concluding the contract. Moreover, as regards goods with digital elements, digital content and digital services, consumers should be informed about the period of time during which free software updates are available. Therefore, Directive 2011/83/EU… and of the Council.	(22) In order for consumers… before concluding the contract. Moreover, as regards goods with digital elements, digital content and digital services, consumers should be informed about the period of time during which free software updates are available, ***including both security and other, functionality or features updates, which should be provided independently.*** Therefore, Directive 2011/83/EU… and of the Council.

AMENDMENT 5
PROPOSAL FOR A DIRECTIVE

Article 1(1) point w

Text proposed by the Commission	**Amendment**
(w) 'software update' means a free update, including a security update, that is necessary to keep goods with digital elements, digital content and digital services in conformity in accordance with Directives (EU) 2019/770 and (EU) 2019/771;	(w) 'software update' means a free update, ***either a security update or any other functionality or feature update***, that is necessary to keep goods with digital elements, digital content and digital services in conformity in accordance with Directives (EU) 2019/770 and (EU) 2019/771;

AMENDMENT 6
PROPOSAL FOR A DIRECTIVE

Article 2(1) point (14e)

Text proposed by the Commission	**Amendment**
(14e) 'software update' means a free update, including a security update, that is necessary to keep goods with digital elements, digital content and digital services in conformity in accordance with Directives (EU) 2019/770 and (EU) 2019/771;';	(14e) 'software update' means a free update, ***either a security update or any other functionality or feature update,*** that is necessary to keep goods with digital elements, digital content and digital services in conformity in accordance with Directives (EU) 2019/770 and (EU) 2019/771;';

AMENDMENT 7
PROPOSAL FOR A DIRECTIVE

Point 4(23j)

Text proposed by the Commission	**Amendment**
(23j)	(23j) ***Bundling security updates with functionality, feature or other software updates, especially when the functionality or feature software update is likely to negatively impact the use of goods with digital elements or certain features of those goods***

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+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).