bB

SUMMONS

Today, _____ at the request of:

1. The **CONSUMENTENBOND** (the Dutch Consumers' Association, hereinafter referred to as the "**Consumentenbond**"), an association with full legal capacity having its registered office in The Hague, the Netherlands, and its principal place of business at Enthovenplein 1, (2521 DA) The Hague;

   Electing as its address for service in this matter the offices of bureau Brandeis, at Apollolaan 151, (1077 AR) Amsterdam, the Netherlands, of which firm Chr. A. Alberdingk Thijm, C.F.M. de Vries and S.C. van Velze have been appointed as lawyers in this matter and will appear as such,

I,

HAVE SUMMONED:

1. **Samsung Electronics Benelux B.V.**, a private limited company with its registered office in Delft, the Netherlands, and its principal place of business at Evert van de Beekstraat 310, (1118 CX) Schiphol, the Netherlands, electing as its address for service in this matter the offices of F. Gerritzen, at Appollolaan 15, (1077 AB) Amsterdam,

   and have served a copy and the original writ at the address stated above:

   - ❑ with:

   - ❑ in a sealed envelope on which the information prescribed by law is stated, as there was no one present with whom I could leave a copy of the writ in a legally valid manner,

2. **Samsung Electronics Co. Ltd.**, a company incorporated according to foreign law, with its principal place of business at Maetan 3-Dong, Paldal-Ku 416, Suwon City, Kyungki-Do (Korea), electing as its address for service in this matter the offices of F. Gerritzen, at Apollolaan 15, (1077 AB) Amsterdam (hereinafter jointly referred to as: "**Samsung**")

   and have served a copy and the original writ at the address stated above:

bB

- ❑ with:

- ❑ in a sealed envelope on which the information as prescribed by law is stated, as there was no one present with whom I could leave a copy of the writ in a legally valid manner,

TO:

appear on **Wednesday [date] (the "Cause-list Date") at 10:00 a.m.**, not in person but represented by counsel in the legal proceedings before the District Court of The Hague, to be held in the court building at Prins Clauslaan 60, (1076 AV) The Hague,

WITH NOTIFICATION THAT:

- ✓ if a defendant fails to appoint an attorney on the Cause-list Date or on a different cause-list date to be specified by the court, or if a defendant fails to pay the court fee to be specified below on time, and the prescribed terms and formalities have been observed, the court will grant a default judgment against the defendant and allow the claims set out below unless it deems them to be unlawful or unfounded;
- ✓ that if at least one of the defendants appears in court and has paid the court fee due on time, one judgment will be issued for all parties, which will be regarded as a judgment in a defended action;
- ✓ upon each of the defendants' appearance in the proceedings, a court fee will be levied which is to be paid within four weeks of the defendant's appearance; the amounts of the court fees are stated in the most recent annex to the Dutch Court Fees (Civil Cases) Act (*Wet griffierechten burgerlijke zaken*), which can be found inter alia on the website www.kbvg.nl/griffierechtentabel;
- ✓ a court fee determined by or pursuant to the law will be charged to a person of limited means if, at the time the court fee is charged, he or she has submitted:
  - a copy of the decision granting legal aid as referred to in section 29 of the Dutch Legal Aid Act (*Wet op de rechtsbijstand*) or, if this is not possible on account of circumstances that are not reasonably attributable to that defendant, a copy of the application referred to in section 24(2) of the Dutch Legal Aid Act, or
  - a statement issued by the board referred to in Section 1(b) of that Act showing that that defendant's income does not exceed the amounts referred to in section 35(3) and (4), paragraphs a to d in each case, or in those subsections, paragraph e in each case, of that Act, on the understanding that as a result of an amendment to the Dutch Legal Aid Act that has come into force, the board of the Legal Aid Council, referred to in section 2 of that Act, will now issue this statement, while the amounts with which the income is compared are stated in Article 2(1)(2) of the Dutch Legal Aid (Personal Contributions) Decree (*Besluit eigen bijdrage rechtsbijstand*).
- ✓ that, pursuant to Section 15 of the Dutch Court Fees (Civil Cases) Act, a single joint court fee will be levied on defendants who appear with the same lawyer and file identical statements of case;

IN ORDER TO:

respond to the following claims by the Consumentenbond:

INTRODUCTION

1. This case turns on whether Samsung must provide the software in its smartphones in a timely manner with the (available) updates and upgrades, and the information that Samsung must provide to the consumer about its policy on updates and upgrades.

2. The purpose of these proceedings is to acquire two declaratory decisions that, put briefly, Samsung is acting in conflict with the due care that can be expected of it according to generally accepted standards and/or is acting in conflict with a number of specific statutory obligations by (i) not providing updates and/or upgrades and/or not providing them in a timely manner, and by (ii) not informing consumers in a clear manner of the policy on updates and upgrades.

3. The Consumentenbond requests that this Court also orders Samsung to provide software updates and upgrades within one month after these become available, for a period of four years after the introduction to the market and/or two years after the time of the sale.

4. The Consumentenbond also requests that this Court, in summary, orders Samsung to inform consumers clearly and unambiguously of its policy on updates and upgrades with regard to each model that Samsung has introduced or will introduce to the market.

5. These proceedings are ongoing against the background of the increasing importance of smartphones in our society and their inherent security risks: security risks that Samsung can avoid by updating the software in its devices in a timely manner. Furthermore, due to the absence of proper information regarding Samsung's policy, the consumer cannot make an informed purchase decision.

6. The Consumentenbond earlier conducted provisional relief proceedings against Samsung (**Exhibit 1**) with regard to the 'Stagefright bug'. The judge in provisional relief proceedings of the Amsterdam District Court dismissed the Consumentenbond's claims at that time due, inter alia, to the absence of an urgent interest.[1] The Consumentenbond is issuing these proceedings on the merits to ensure that Samsung provides its smartphones with updates and upgrades for their entire lifespan.

FACTS

Consumentenbond

7. The Consumentenbond is an association with full legal capacity that has the objective of looking after the interests of consumers in general and of the members of the association in the Netherlands in particular, and insofar as possible and necessary abroad (**Exhibits 2 and 3**).

[1] Provisional relief judge, Amsterdam District Court 8 March 2016, ECLI:NL:RBAMS:2016:1175

8. In the context of this objective the Consumentenbond informs consumers, of the quality of products and services, including smartphones, and it emphasises the importance of security and privacy, as is inter alia evident from the *Update!*, *Stop DigiDwang!* and *Helder over Online Privacy campaigns* (**Exhibit 4**).

The smartphone market and Samsung's market position

9. Four out of five Dutch people own a smartphone, i.e. a phone that offers extensive computer options. A smartphone combines the characteristics of a mobile phone with those of a personal computer.

10. The basis of each smartphone is the operating system, the software that drives the hardware (the smartphone) and that functions as the medium between the smartphone and the user, the consumer. The consumer mainly recognises the operating system by its design.

11. The most frequently used operating systems are Android by Google, iOS by Apple and Windows Phone by Microsoft.

12. Android and iOS together cover the lion's share (more than 90%) of the smartphone market. Android is the market leader, both worldwide and in the Netherlands. In 2013 more than 75% of all phones sold worldwide operated on Android. Android is also dominant in the Netherlands. According to GfK's recent figures for January-June 2016, the Android share of the total number of smartphones was 66%. (**Exhibit 5 a**)

13. Samsung is a worldwide market leader in the field of smartphones and the largest offeror of smartphones with the Android operating system. Samsung represents more than 45% of the market worldwide. In the Netherlands, Samsung's share of all smartphones is 41.7%.[2] Samsung's share in Android represents 63.1%. This means that Samsung is the market leader in the Netherlands in the field of smartphones. These figures are confirmed by the Global Mobile Consumer Survey for 2015 from Deloitte (**Exhibit 5**).

14. Samsung sells a large product range of smartphones, inter alia through its website.[3] In addition, Samsung phones can be purchased through other web shops, such as CoolBlue and Bol.com and through telecom provider (web)shops such as KPN and Vodafone.

Android

15. The Android operating system was developed by Google and has been offered since 2007 as *open source* **(Exhibit 6**). Google offers the operating system free of charge and everyone is allowed to use it.

16. Android is the most frequently used operating system for smartphones. In addition to Samsung manufacturers such as HTC, LG, Sony and Huawei also use Android as their operating system.

---

[2] In 2015 this was 40.5%, see the Deloitte Global Mobile Consumer Survey 2015.

[3] http://www.samsung.com/nl/consumer/mobile-phone/smartphones/smartphones/.

17. Android is therefore the basis of each Samsung smartphone.

Updates and Upgrades

Updates

18. It is inherent to software and therefore also to the Android operating program that these contain or will contain vulnerabilities which open them up to the possibility of exploitation. That is the reason why Google continuously works to improve the security and protection of Android. On the security page of the Android website, Google describes the measures it takes to safeguard the security of Android (**Exhibit 7**).[4]

19. The Google Android Security Team continuously checks the software for vulnerabilities and bugs ("security vulnerabilities"). As soon as such a vulnerability is discovered in Android, Google checks the nature of the vulnerability and classifies this in accordance with the severity of the potential consequences in the event of exploitation.

> *The first task in handling a security vulnerability is to identify the severity of the bug and which component of Android is affected. The severity determines how the issue is prioritised, and the component determines who fixes the bug, who is notified, and how the fix gets deployed to users.* [...] *The severity of a bug generally reflects the potential harm that could occur if a bug was successfully exploited.*[5]

20. The most severe vulnerabilities (*bugs*) are classified as "critical", which means that in the case of successful exploitation, those with malicious intent get a "remote root" option. [6] This means that those with malicious intent can gain full remote control of the device.

21. The other classifications are "high", "moderate" and "low". In the event of a "high" classification, those with malicious intent can still obtain access to data that is not usually freely accessible.

22. Vulnerabilities in the software are remedied with a "patch", a piece of software that remedies the error. As soon as Google finds a vulnerability or bug in Android it makes a "patch" for this (hereinafter referred to as: "Update"), and subsequently informs its partners that use Android and simultaneously makes the Update available.

23. In any event, Google makes Updates for Android versions that have appeared over the past three years.

---

[4] https://source.android.com/security/ and https://source.android.com/security/overview/updates-resources.html.

[5] https://source.android.com/security/overview/updates-resources.html#triaging_bugs.

[6] Google describes this as follows on the website: "*A remote attack vector indicates the bug could be exploited without installing an app or without physical access to the device. This includes bugs that could be triggered by browsing to a web page, reading an email, receiving an SMS message, or connecting to a hostile network*".

> *When a moderate or higher severity security vulnerability in AOSP* [Android Open Source Project, lawyer] *is fixed, we'll notify Android partners of issue details and provide patches for a minimum of the most recent three Android releases. The Android security team currently provides patches for Android versions 4.4 (KitKat), 5.0 (Lollipop), 5.1 (Lollipop MR1), and 6.0 (Marshmallow). This list of backport-supported versions changes with each new Android release.*[7]

24. Google provides Updates monthly through *Android Security Bulletins* (**Exhibit 7**). According to the "Security program overview" the provision of these monthly security Updates is one of the "key components" of the Android security program and "an important tool used to make and keep Android users safe". [8] In the *Security Bulletins* Google describes the vulnerabilities that have been found, their severity and the Updates (and their functioning).

25. Google makes Updates available for Google Pixel (until recently: Nexus) devices, Google's personal smartphone,[9] and for all manufacturers with whom it cooperates ("all our device manufacturing partners"). It is then up to these manufacturers, such as Samsung, to customise these Updates and install them in the smartphones they offer.

26. Since 2014, in the context of transparency, Google has been publishing, every year, *Android Security Reports*, (**Exhibit 7**), which once again describe the security process used by Google relating to Android. [10] It is evident from this that Google encourages the implementation of monthly updates by manufacturers, inter alia by introducing an Android Security patch level.

> *We continued to provide device manufacturers with ongoing support for fixing security vulnerabilities in devices, and have expanded the program to include monthly public security bulletins with security patches released to the Android Open Source Project (AOSP). In addition to the updates that we release for Nexus devices, several device manufacturers and network providers are also working toward monthly updates of their devices and services for users. As part of this process, we introduced the Android security patch level, which makes checking if an Android device is up-to-date with all security patches as simple as knowing today's date.*

Upgrades

27. Since Android's first introduction in 2008, many new functionalities have been added and many changes have been made. In the meantime 24 versions of Android have appeared, similarly to Apple which regularly issues new versions (from the iOS 4 in 2010 to the iOS 10 in 2016). In this manner in 2012 "Jelly Bean" was launched, followed by "KitKat" in 2013,

---

[7] https://source.android.com/security/overview/updates-resources.html.

[8] https://source.android.com/security/bulletin/index.html.

[9] Google Pixel (until recently: Nexus) is a series of mobile devices manufactured by Google in cooperation with various hardware manufacturers. The manufacture changes each time.

[10] https://static.googleusercontent.com/media/source.android.com/and/us/devices/tech/security/reports/Google_Android_Security_2014_Report_Final.pdf and http://static.googleusercontent.com/media/source.android.com/nl//security/reports/Google_Android_Security_2015_Report_Final.pdf.

"Lollipop" in 2014 and "Marshmallow" in 2015. The most recent version of Android is dated 22 August 2016 and is known by the name "Nougat". The new version of the operating system will hereinafter also be referred to by the term "Upgrades".

28. Upgrades usually contain new functionalities (e.g. notification screens and options such as finger print scanners), applications, performance improvements (such as speed and battery recharge time) and/or new design elements.

29. However, Upgrades can also contain security updates and settings. In this manner Android offered Marshmallow consumers for the first time the option to give (individual) permission for each app for the sharing of (personal) data instead of (for the entirety) in the Google Play Store,[11] as was still the case for Lollipop (**Exhibit 8**).[12] Due to this change, by which consumers can determine themselves what data they share and when, and by which they can switch the app authorisations on or off at any time, the privacy of consumers has been significantly improved. With this Android acknowledges that apps do not require continuous access to the (location) data of consumers.

The importance of Updates and Upgrades

30. Updates and Upgrades are of essential importance to guaranteeing information security (*cyber security*) and the protection of personal data of consumers. All parties agree on this.

31. In its Protection of Personal Data Guidelines the Dutch Data Protection Authority (the "Dutch DPA") sets out what an "appropriate security level" means. The supervisory authority applies as the starting point a number of security measures that are customary and necessary in the field of information security. Keeping the operating system up to date is one of these measures. According to the Authority the controllers who process personal data (such as Samsung) must furthermore install in a timely manner the solutions issued by the supplier (in this case: Google) for the security breaches in the software.

> *Software, such as browsers, virus scanners and operating systems, kept up to date. The controller will also install in a timely manner the solutions that are issued by the supplier for security breaches in this software. More in general the controller will acquire in a timely manner information about technical vulnerabilities of the information systems used. The extent to which the organisation is exposed to such vulnerabilities is assessed and the controller will take suitable measures for dealing with the risks attached thereto.*[13]

---

[11] Users can find apps through the Google Play Store, which are either free of charge or paid for. Google Play is comparable with the IOS App Store.

[12] https://nl.wikipedia.org/wiki/Android_(besturingssysteem).

[13] Protection of Personal Data Guidelines of the Dutch DPA, February 2013. To be found at: https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf.

32. The standards that the Dutch DPA refers to are further detailed in the Code for Information Security (NEN-ISO / IEC 27002:2007 nl). This Code is a technology-neutral standard that is applied broadly for the purpose of information security during the formulation and implementation of security measures. The Code describes standards and measures that are important for achieving an adequate level of information security. This Code also prescribes that security patches (Updates) must be implemented as soon as possible.

33. The importance of issuing "patches' (i.e.: Updates) in a timely manner was also underlined by the Rotterdam District Court in a case which concerned the question of whether KPN had taken sufficient measures to fix a vulnerability in its network in a timely manner. According to the court KPN must take measures to fix vulnerabilities in the software, inter alia, by issuing "patches". KPN was in breach of its duty of care because KPN had not patched the software involved during a specified period of time.

> *Furthermore, it has not been refuted that the claimant at the time of the proceedings did not execute any central coordination with regard to patch management, that work concerning the finding of vulnerabilities was only executed for a part of that part of the network which the Netherlands Authority for Consumers & Markets had focused on in its investigation and that the software referred to in para. 1.5 was not patched during a certain period.*[14]

34. According to the District Court, patch management is an essential component of a proper security policy. The fact that in that case ultimately no personal data were taken by those with malicious intent (and the vulnerability had therefore not resulted in exploitation), did not affect the opinion that KPN had breached its duty of care. The fact that, as KPN put forward, patching is a labour intensive process as it is carried out manually, did not affect this decision either. In the opinion of the District Court, the Netherlands Authority for Consumers & Markets had rightly imposed a financial penalty on KPN for the insufficient protection of customer data.[15]

35. The importance of Updates in mobile devices is also evident from research that the Federal Communications Commission (FCC) and the Federal Trade Commission (FTC) are currently conducting in the United States concerning the (inadequate) upgrade and update processes of manufacturers of smartphones (**Exhibits9 and 9 b**).[16] The supervisory authorities are concerned that Updates for smartphones are made available following considerable delay and that some older devices do not receive any Updates at all. The supervisory authorities asked Samsung and Google, among others, to explain their update policy.

> *Consumers may be left unprotected, for long periods of time or even indefinitely, by any delays in patching vulnerabilities once they are discovered. To date, operating system providers, original equipment manufacturers, and mobile service providers have*

---

[14]Rotterdam District Court 8 January 2015, ECLI:NL:RBROT:2015:22 (*KPN/ACM*), para. 4.7.

[15]Rotterdam District Court 8 January 2015, ECLI:NL:RBROT:2015:22 (*KPN/ACM*).

[16] http://www.bloomberg.com/news/articles/2016-05-09/apple-google-and-wireless-carriers-asked-by-u-s-about-security.

> *responded to address vulnerabilities as they arise. There are, however, significant delays in delivering patches to actual devices—and that older devices may never be patched.*[17]

36. The manufacturers were given 45 days to complete an extensive questionnaire (**Exhibit 9 c**) regarding their Update process and the selection of devices that receive Updates.

> *In order to gain a better understanding of security in the mobile ecosystem, the Federal Trade Commission has issued orders to eight mobile device manufacturers requiring them to provide the agency with information about how they issue security updates to address vulnerabilities in smartphones, tablets, and other mobile devices.*[18]

37. In 2013 the FTC had already formulated a complaint with regard to HTC, in which it concluded that HTC had "failed to employ reasonable and appropriate security in the design and customization of the software on its mobile devices" (**Exhibit 10, para. 7**). The complaint ultimately resulted in a settlement. Part of this settlement is not only that HTC must issue patches (Updates) in a timely manner but also that HTC is placed under intensive supervision for the next 20 years.[19]

38. The National Cyber Security Centre (NCSC) too emphasises the importance of Updates. The NCSC recommends installing Updates as soon as possible in order to fix vulnerabilities in the software (**Exhibit 11**). Software, the "End-of-Life" date of which has expired, i.e. the date following which the software is no longer supported by Upgrades and Updates, is according to the NCSC no longer tenable and can no longer be regarded as secure.

39. These are only examples. Numerous parties and authorities too emphasise the importance of Updates and Upgrades. For example, in October 2016, Europol started a campaign to counter the consequences of "mobile malware" i.e. harmful software that is focused on smartphones **(Exhibit #**). Updates are an important resource in this context.[20] Alert Online also recommends updating all software as quickly as possible to prevent viruses making use of vulnerabilities in older versions.[21]

Incidents

40. The fact that all these parties underline the importance of Updates and Upgrades is not surprising. Smartphones and their software are continuously exposed to vulnerabilities and security bugs, with all the ensuing risks for the privacy of consumers. Updates are there to fix these vulnerabilities.

---

[17] http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0509/DOC-339256A1.pdf.

[18] https://www.ftc.gov/news-events/press-releases/2016/05/ftc-study-mobile-device-industrys-security-update-practices.

[19] https://tweakers.net/nieuws/87458/htc-schikt-met-amerikaanse-overheid-over-slechte-beveiliging.html.

[20] https://www.europol.europa.eu/content/mobile-malware.

[21] https://www.alertonline.nl/.

41. An example of a well-known vulnerability in Android software is the Stagefright security bug made known by Zimperium in July 2015 (**Exhibit 13 a**). This bug was found in all Android versions from Android 2.2 (Froyo from 2010) onwards, which means that virtually all the millions of Android smartphones that are currently in circulation are or were exposed to this bug.

42. Those with malicious intent can, by means of the Stagefright bug, potentially have full remote access to an Android smartphone, without the requirement of any action on the part of the consumer and without the consumer even noticing anything. This is the reason why the Stagefright bug was classified as "critical" by Google (**Exhibit 13 b**). The risks of Stagefright are the highest for devices that run on Android 4.0 or lower, which underlines the independent importance of Upgrades in addition to Updates.

43. It was this Stagefright bug that led Google to tighten up the Android security policy and to introduce the monthly Updates, as is, inter alia, described in an article in Bloomberg (**Exhibit 14**).

44. Other vulnerabilities are *Fake ID*, *TowelRoot*, *ObjectInputStream deserializable*, *One class to rule them all*[22] and the very recent bug *Drammer*.[23]

45. Having regard to the fact consumers nowadays save all kinds of (sensitive) information in their phone - for example, in addition to contact persons and text messages, also photos, (work) emails, agendas, notes, health applications, internet banking and social media - the risks are high. This is also exactly the reason for the aforementioned research of mobile updates conducted by the FTC and FCC.

> *As consumers and businesses turn to mobile broadband to conduct ever more of their daily activities, the safety of their communications and other personal information is directly related to the security of the devices they use. There have recently been a growing number of vulnerabilities associated with mobile operating systems that threaten the security and integrity of a user's device, including "Stagefright" in the Android operating system, which may affect almost 1 billion Android devices globally.*[24]

Google and Samsung

46. As set out above (paras. #) Google regards Updates as an important resource with which to safeguard the security of users, which is the reason why they offer these on a monthly basis to manufacturers who use Android.

---

[22] These recent bugs (2014-2015) have also been used in research conducted by the University of Cambridge, see http://androidvulnerabilities.org/graph.

[23] http://www.nu.nl/mobiel/4339484/nederlandse-onderzoekers-vinden-opnieuw-groot-lek-in-android.html/.

[24] http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0509/DOC-339256A1.pdf.

47. Samsung itself appears to acknowledge the importance of Updates and Upgrades of the mobile devices it sells. It undertakes to provide these in the "end user licence agreement" (the "EULA") that it concludes with consumers when they install their smartphone (**Exhibit 15**).

48. Clause 4 of this licence agreement ("Updates for Samsung software") concerns Updates and Upgrades. According to this article Samsung is authorised to make updates, upgrades, additions and add-ons for Samsung software available after the date on which the consumer acquired the original copy of the Samsung software. According to clause 4 the licence agreement also applies to these later Updates.

> *Samsung is authorised to make updates, upgrades, additions and add-ons (if applicable) for the Software of Samsung, including bugfixes, service upgrades (wholly or in part) and service updates, improvements and functionality improvements, or removal of Software of Samsung (including entirely new versions) (jointly referred to as the 'Update'), available to you after the date on which you have acquired the original copy of the Software of Samsung. This licence agreement for end users applies to all parts of the Update […]* (**Exhibit 15, p.11**).

49. Samsung emphasises in the same clause the importance of Updates for the security of smartphones. This is the reason why Updates can also be automatically downloaded and installed without permission from the consumer. Samsung moreover recommends that consumers regularly check if there are new Updates for the purpose of security.

> *Having regard to the fact that it is most important that you receive Updates for security software in good time to protect the system against new threats, the security updates can be downloaded and installed without your permission, even if you have switched off the functionality "download updates automatically". This secures your mobile device of Samsung and every Samsung mobile device that is used through the "herd" or "community immunity" concept. We recommend checking regularly for new updates for the best possible use of your device.* (**Exhibit 15, p.11**)

50. On its website and Mobile Security Blog Samsung also emphasises "the importance of protecting our users' security and privacy" and makes the commitment to deliver Updates to consumers as soon as possible. (**Exhibit 16 c**).

Updates and Upgrade performance data

51. Unfortunately these promises made by Samsung are rarely realised in practice. The reality is that it often takes months before Updates are available for installation by the consumer in the various Samsung smartphones. These Updates are not available at all for some devices, as was also flagged up by the FTC and FCC.

52. In July 2015 the Consumentenbond started the "Update!" campaign (**Exhibit 4**). The Consumentenbond is using this campaign to urge manufacturers to support smartphones for

longer with updates. The reason for the campaign was a survey conducted by the Consumentenbond in July 2015 **(Exhibit #** Digitaalgids (Dutch Digital Guide)). It was evident from this survey that many Android devices of Samsung are not supported by new software and that a large number of the devices even run on an unsafe version of Android.

53. The Stagefright bug illustrates this. Although Google made an Update available to its partners within one week after the discovery of the bug, it subsequently took around 3 to 4 months before Samsung actually started to implement this in its devices.

Data about Updates

54. The manner in which Samsung implements Updates, within which period and through which processes is insufficiently transparent.

55. It can be read on a FAQ page on Samsung's website with the title "Software support Samsung" (**Exhibit 16 b**)[25] that Samsung makes efforts to roll out Updates as quickly as possible for as many devices as possible, but that it is also possible a specific device may not receive any Updates.

> *Google makes a patch (remedy software) if a bug or security vulnerability is found in Android. We will test this patch as quickly as possible and submit this to our partners (mobile providers). We only want to roll out a patch after we are certain that our devices will continue to meet the high requirements of user experience and security after the installation of this patch. However, it may be that specific updates will not become available for your device.*

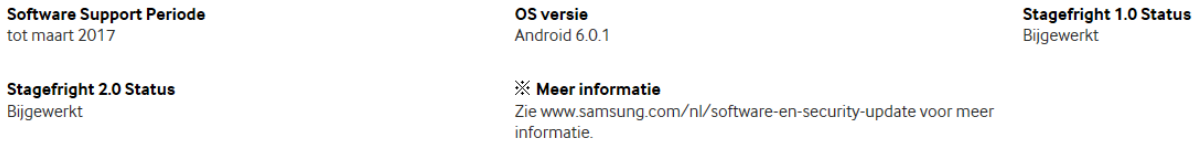
56. Reference is made on this page to a worldwide monthly update program, which was started by Samsung in October 2015 for "selected devices", such as the Galaxy S7, S7 edge, S6, S6 edge, S6 edge+, S5, Note 4 and Tab S2. This monthly cycle therefore only applies to a select number of popular devices. According to the information page, the security Updates option for other devices is checked quarterly.

57. On its Mobile Security Blog (in English) (**Exhibit 16 c**), which it has kept updated since October 2015, Samsung lists the available patches from the monthly patch cycle. The blog states which bugs have been fixed in the (Android) software, but does not state which bugs have not (yet) been fixed.

58. The Blog does not state for how long the Samsung smartphones are generally provided with Updates. This must be checked for each model on the Samsung website. However, it seems that in the Netherlands Samsung proceeds from a maximum period of 2 years to be calculated from the time when the smartphone was introduced to the market. Thus the website states that the Samsung Galaxy s6, a smartphone, which is still available in the shops, and can also be purchased through the Samsung website, will receive software support for another 5 months, until March 2017.

---

[25] http://www.samsung.com/nl/support/skp/faq/1097862.



59. Having regard to the opaque process of Samsung security updates, it is not clear if Samsung makes Updates available and, if so, when it makes the Updates available.

60. This uncertainty led the American FTC to issue an information order to a number of manufacturers, including Samsung. Samsung must provide detailed information within 45 days concerning the question of whether it provides Updates and, if so, when, and for which specific devices.

> *In order to gain a better understanding of security in the mobile ecosystem, the Federal Trade Commission has issued orders to eight mobile device manufacturers requiring them to provide the agency with information about how they issue security updates to address vulnerabilities in smartphones, tablets, and other mobile devices.*
> *[…]*
> *Among the information recipients must provide under the orders are:*
> • *the factors that they consider in deciding whether to patch a vulnerability on a particular mobile device;*
> • *detailed data on the specific mobile devices they have offered for sale to consumers since August 2013;*
> • *the vulnerabilities that have affected those devices; and*
> • *whether and when the company patched such vulnerabilities.* (**Exhibit 9 b,** press release FTC**,** see the full questionnaire **in Exhibit 9 c**).

61. The data on Updates that *is* made available to third parties does not paint a positive picture. It is evident from worldwide research conducted by the University of Cambridge in October 2015 (**Exhibit 18**) that only a small number of Android devices receive Updates in a timely manner.[26] According to this research 87.7% of the Android devices are vulnerable to serious security bugs in Android.[27] The research was conducted with the "Device Analyzer", an application that can monitor the status of an Android device.

62. The research gives manufacturers a score out of 10 depending on the security that they could guarantee to their customers in the past years. Samsung was given a score of 2.81. The score is based on a formula that takes account of the number of devices that are free of vulnerabilities, the number of devices that are updated to the most recent version of the operating system and the number of vulnerabilities that have not yet been remedied with an Update.

---

[26] Security metrics for the Android ecosystem by Daniel R. Thomas, Alastair R. Beresford and Andrew Rice in ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM) 2015.

[27] http://androidvulnerabilities.org/.

63. According to the research, the "bottleneck" in the implementation of Updates does not rest with Google as the provider of Android, but with manufacturers which do not implement Updates in a timely manner. The report also concludes that there is an information asymmetry between the manufacturer and the consumer, because only the manufacturer knows whether there is any vulnerability present and whether an Update has been or will be issued for this. The consumer simply does not know whether his or her device is secure.

> *The security of Android depends on the timely delivery of updates to critical vulnerabilities. Unfortunately few devices receive prompt updates, with an overall average of 1.26 updates per year, leaving devices unpatched for long periods. We showed that the bottleneck for the delivery of updates in the Android ecosystem rests with the manufacturers, who fail to provide updates to critical vulnerabilities. This arises in part because the market for Android security today is like the market for lemons: there is information asymmetry between the manufacturer, who knows whether the device is currently secure and will receive updates, and the consumer, who does not. Consequently there is little incentive for manufacturers to provide updates.*[28]

64. A recent Bloomberg article of May 2016 (**Exhibit 14**) shows, once more, that the bottleneck in the update process does not rest with Google but with the manufacturers. In fact, Google considers the lack of timely installations of Updates and Upgrades by partners as "the weakest link in Android security" and is taking all kinds of measures to ensure that manufacturers update and upgrade quicker.

> *The issue -- a mishmash of different smartphones running outdated software lacking the latest security and features -- has plagued Android since its debut in 2007. But Google has stepped up its efforts recently, accelerating security updates, rolling out technology workarounds and reducing phone testing requirements.* [...]
>
> *Google is making progress persuading phone makers and carriers to install security updates quicker "for the good of users," Lockheimer* [Senior Vice president Android, lawyer] *said. The same expedited process may then be used to send operating system updates to phones, he explained.*[29]

65. The article confirms existing rumours that Google intends to start publishing Update performance data in the foreseeable future. The reason for this is to persuade manufacturers to install Updates and Upgrades quicker.

> *Google is using more forceful tactics. It has drawn up lists that rank top phone makers by how up-to-date their handsets are, based on security patches and operating system versions, according to people familiar with the matter. Google shared this list with*

---

[28] Security metrics for the Android ecosystem by Daniel R. Thomas, Alastair R. Beresford and Andrew Rice in ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM) 2015, p. 11.

[29] https://www.bloomberg.com/news/articles/2016-05-25/google-steps-up-pressure-on-partners-tardy-in-updating-android.

Android partners earlier this year. It has discussed making it public to highlight proactive manufacturers and shame tardy vendors through omission from the list [...].

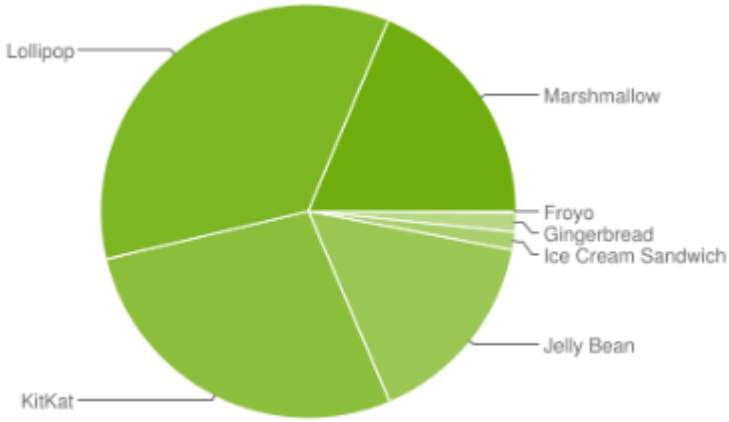
Data about Upgrades

66. Data about Android Upgrades is easy to find.

67. The Google Developers Dashboard, the page that provides information about the Android versions that run on the devices that use Android as their operating system, shows that still only 18.7% of Android devices are equipped with Marshmallow.[30] By far the largest number of the devices are still running on Lollipop dating from 2014 and even KitKat dating from 2013. And no fewer than 15.6% of them still run on the old Jelly Bean system. And this is despite the fact that Marshmallow has been available since 5 October 2015. Meanwhile yet another new version has become available: Nougat.

Version	Codename	API	Distribution
2.2	Froyo	8	0.1%
2.3.3 - 2.3.7	Gingerbread	10	1.5%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	1.4%
4.1.x	Jelly Bean	16	5.6%
4.2.x		17	7.7%
4.3		18	2.3%
4.4	KitKat	19	27.7%
5.0	Lollipop	21	13.1%
5.1		22	21.9%
6.0	Marshmallow	23	18.7%

Data collected during a 7-day period ending on September 5, 20
Any versions with less than 0.1% distribution are not shown.



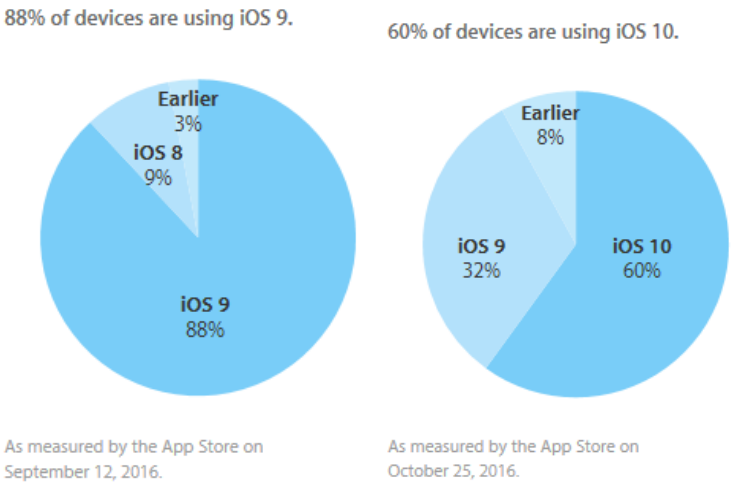
68. The survey conducted by the Consumentenbond (**Exhibit 17**) shows similar results. During the period 2013-2015 the Consumentenbond tested 171 smartphones and found that 84% of these smartphones did not run on the most recent (at that time) Android version.

69. iOS, the operating system developed by Apple for the iPhone and the iPad, shows an entirely different picture (**Exhibit 27 b**). According to the Developers Dashboard of Apple, 88% of the devices ran on iOS 9 in September 2016.[31] Meanwhile in September 2016 the new operating system of iOS was introduced, i.e. iOS 10. After five weeks this most recent version was installed in more than half of all devices (namely in 60%). The devices therefore receive Upgrades for iOS

[30] https://developer.android.com/about/dashboards/index.html.

[31] https://developer.apple.com/support/app-store/.

much faster. What's more, iOS in practice appears to provide Upgrades up to 4 years after the introduction of the device.[32]



70. With regard to Upgrades, Samsung states on its website that during the software and support period it seeks to "provide devices with the most recent Android version as much as possible", but that it cannot promise that the consumer will always receive the most recent version in his or her phone. It is evident from research conducted by the Consumentenbond that eight months after the release of Android 6 still only 20% of all Samsung devices had received the most recent version (**Exhibit 17**).[33]

Comparison

71. Many manufacturers are, like Samsung, equally vague about their policy and implement Updates and Upgrades with considerable delays. There are however also examples of how to do it better. Pixel phones (formerly Nexus) of Google receive Updates for at least for 3 years after being launched in the market (or for at least 18 months after the last sale, depending on which period is longer) and Upgrades for at least two years (**Exhibit 19**). iOS of Apple appears in practice to receive Updates up to five years after the introduction of the device and Upgrades for up to four years.[34]

Consultation between the Consumentenbond and Samsung

72. By now, this case has a long history to it.

73. On 2 July 2015, following the research conducted by the Consumentenbond, which shows that most Samsung smartphones run on an old version of Android (**Exhibit 17**), the Consumentenbond asked Samsung what measures it will take to ensure that consumers are not

[32] https://www.statista.com/chart/5824/ios-iphone-compatibility/.

[33] https://www.consumentenbond.nl/acties/updaten/nauwelijks-updates-naar-android-6.0.

[34] https://www.statista.com/chart/5824/ios-iphone-compatibility/.

exposed to security bugs (**Exhibit 20 a**). Samsung has not responded substantively to this.

74. On 16 July 2015, the Consumentenbond then sent an overview of the most recent Android versions in Samsung smartphones (**Exhibit 20 b**). On 22 July 2015 Samsung replied that these smartphones do indeed often receive recent Updates to fix the security bugs . Apparently only Upgrades are not available for these devices (**Exhibit 20 c**).

75. On 22 July 2016 Samsung stated in an email that it was making efforts to make the most recent system updates available in the Galaxy models. For the models that are not capable of receiving Upgrades, Samsung is doing all it can *"to still provide these devices with regular updates"* (**Exhibit 20 d**).

76. By email of 8 September 2015 the Consumentenbond requested that Samsung inform consumers about its upgrade policy with regard to the most recent version of Android 6.0 Marshmallow (**Exhibit 20 e**). In this email the Consumentenbond also referred (once again) to the Stagefright bug and noted that this bug still had not been fixed.

77. On 29 September 2015 the Consumentenbond had still not received a reply. The Consumentenbond then invited Samsung to its office to discuss Samsung's update policy (**Exhibit 20 f**). This discussion took place on 8 October 2015. Samsung did not make any specific promises at this meeting. In the opinion of the Consumentenbond the discussion was therefore inadequate.

78. On 2 December 2015 the Consumentenbond demanded that Samsung place material information on its website and provide Updates for the Samsung smartphones with a critical security bug (**Exhibit 20 g**). The Consumentenbond once again offered to enter into talks. These talks took place on 17 December 2015.

79. Following these talks Samsung was to come up with a proposal to comply with the demand from the Consumentenbond. Samsung requested an extension of the deadline for this, which request was granted by the Consumentenbond.

80. However, on 24 December 2015, without informing the Consumentenbond, Samsung published a press release in which it stated that it was tightening up its policy on updates and upgrades (**Exhibit 28**). The Consumentenbond did not receive any further proposal from Samsung after this press release.

81. Because it found that the policy that Samsung introduced in the press release was inadequate and did not meet the essential elements in the demand it had made, the Consumentenbond decided to institute provisional relief proceedings. On 16 February 2016 the provisional relief proceedings took place.

82. In a judgment of 8 March 2016 the provisional relief judge of the Amsterdam District Court dismissed the claims of the Consumentenbond, due in particular to the lack of an urgent

interest.[35]

83. On 4 November 2016 talks once again took place between Samsung and the Consumentenbond. These talks did not result in Samsung adjusting its conduct either.

84. It follows from the factual context that Samsung is currently still failing in its policy on updates and upgrades. This is the reason why the Consumentenbond has no choice but to institute the present proceedings on the merits.

LEGAL FRAMEWORK

85. It follows from the factual context that:

- many Samsung devices do not run on the most recent version (or even on the previous version) of Android;
- Samsung only makes monthly Updates available for a select number of devices;
- the other Samsung devices only receive Updates following long delays, or they do not receive them at all;
- there are presently Samsung devices for sale that still only receive a few months of software support (Updates and Upgrades); and
- Samsung does not make any specific promises whatsoever to consumers about whether they can expect Updates and Upgrades, and, if they can, within what time frame.

86. By not making Updates and Upgrades available and/or by not making them available in a timely manner, or at least not for the entire lifespan of the devices, Samsung exposes consumers to potential exploitation by persons acting with malicious intent, and Samsung is acting contrary to various statutory obligations and contrary to the due care that is expected of it according to generally accepted standards.

87. The Consumentenbond takes the position that Samsung must provide all its devices during their lifespan with monthly Updates that fix the vulnerabilities in the software, and that this must be for a period of four years after the introduction of the device to the market, or for at least two years after the time of the sale of the device to the consumer (depending on which period is longer). In addition Samsung must provide all its devices during their normal lifespan with Android Upgrades as soon as these are available.

88. Lastly, Samsung must inform the consumer in advance, clearly and unambiguously, about its Policy on Updates and Upgrades.

89. Samsung's conduct is in conflict with several statutory provisions. Samsung is also acting in conflict with that what is proper according to generally accepted standards. In what follows the Consumentenbond will explain that Samsung's conduct is in conflict with the doctrine of non-

[35] Provisional Relief Judge of the Amsterdam District Court 8 March 2016, ECLI:NL:RBAMS:2016:1175

conformity (Article 7:17 of the Dutch Civil Code ("BW"), the duty of care with regard to the protection of personal data (Section 13 of the Dutch Personal Data Protection Act (*Wet bescherming persoonsgegevens*) ("Wbp"), the prohibition of unfair commercial practice (Article 6:193b BW), the Radio Equipment Directive, and the due care that can be expected from Samsung according to generally accepted standards (Article 6:162 BW). The claims take issue with these infringements of statutory provisions and seek, where possible, to halt the actions that are in conflict with due care according to generally accepted standards. In summary, the claims seek to ensure that Samsung has an obligation to update and an obligation to provide information.

Non-conformity (Article 7:17 BW)

90. A consumer who purchases a Samsung smartphone, whether or not through the Samsung website, purchases a smartphone in which the Android operating system (modified by Samsung) has been installed. When Samsung becomes aware of a vulnerability in the software, as a result of which it is less secure and consumers are exposed to exploitation, and Samsung does not fix this vulnerability, this software will not contain the characteristics that the consumer can expect of it and it will be non-conforming.

Licence agreement

91. When a consumer sets up a smartphone, he must agree to Samsung Electronics Co. Ltd's "End User Licence Agreement for Software" (**Exhibit 15**). If the consumer does not do this he will not be permitted to use the smartphone, as is determined by the opening paragraph of the agreement. The consumer therefore must first click on "agree" before he can use the smartphone. When the consumer does this he enters into a contractual relationship with Samsung.

> *This licence agreement for end users is a legally binding agreement between you (an individual or an entity) and Samsung Electronics Co Ltd ('Samsung') for software owned by Samsung and its affiliated companies and its external suppliers and licensors […].*
> *By using this device or any other Samsung mobile product, including mobile phones and tablets, running on Android operating system ("Samsung Mobile Device"), you accept the terms of this End User Licence Agreement. If you do not accept these terms, do not use the Samsung Mobile Device or the Samsung Software.*

92. Clause 1 of the agreement grants the consumer w a limited, non-exclusive licence for installing, using, accessing, displaying and running Samsung software in the smartphone.

93. As set out above (paras. #), clause 4 of the licence agreement concerns the Updates and Upgrades that Samsung will provide.

94. Clause 5 states that if the consumer wishes to receive Updates he must agree that Samsung may collect and use o a certain amount of (personal) data.

95. Pursuant to clause 8 the licence agreement is for an indefinite duration. The licence is in principle provided for the entire lifespan of the device, unless the consumer does not comply with the conditions of the licence agreement. The same applies to the licence in the Privacy Policy (**Exhibit 21**, clause 7.1).

Applicable purchase regime

96. The consumer therefore concludes a separate licence agreement with Samsung for the (permanent) use of the software and for receiving Updates and Upgrades. Samsung is the party that the consumer is contracting with in this context and Samsung is the party that is independently responsible for the supply and the updating of the software. Samsung is also the party that determines whether or not Updates and Upgrades will be provided.

97. In the *Beeldbrigade* judgment the Dutch Supreme Court confirmed that a contract of sale (as provided by Article 7:1 BW) also applies to agreements for the purchase of standard software.[36] The Supreme Court deduced this from Article 7:47 BW, which determines that a purchase can also relate to property rights, and from which it is evident that the legislature intended to give contracts of sale a broad scope with regard to the subject-matter of purchase agreement. The Dutch Supreme Court further found it important that the licence provides the acquirer with "use that is not limited in duration" of the software. The Supreme Court deemed it desirable that the contract of sale also applies to such agreements.[37]

98. The European Court of Justice (CJEU) has classified the provision of an unlimited, non-exclusive and non-transferable right of use by a copyright owner of a copy of a computer program to a customer as the "sale" of that program.[38]

99. Since Samsung's licence agreement also grants the consumer a right of use that is unlimited in time, the provisions of the law on purchase also apply to that.

100. This follows from Article 7:5(5) BW, which declares the provisions on a consumer sale applicable to the supply of digital content which is not supplied on a tangible medium. The law (Article 6:230g BW and Article 1(11) of the Consumer Protection Directive)[39] defines digital content as "data which are produced and supplied in digital form". In recital 19 of the Consumer Protection Directive, as in the Explanatory Memorandum to the Dutch implementation act, software is expressly referred to as an example of digital content.[40]

---

[36] Dutch Supreme Court 27 April 2012, ECLI: NL: HR: 2012:BV1301 (*Beeldbrigade*).

[37] Dutch Supreme Court 27 April 2012, ECLI: NL: HR: 2012:BV1301 (*Beeldbrigade*), para. 3.5.

[38] CJEU 3 July 2012, case C 128/11, ECLI: EU: C: 2012:407 (*UsedSoft*).

[39] Directive 2011/83/EU

[40] Parliamentary Papers II 2012/13, 33 520, no. 3, page 19.

101. Having regard to the independent nature of the contractual relationship between the consumer and Samsung, and the independent economic value that is represented by Samsung software, the software in a smartphone must be regarded as digital content which is not supplied on a tangible medium. This also applies to Updates that the consumer must download onto the smartphone.

Non-conformity

102. Samsung must, on the basis of Article 7:17(1) and (2) BW, deliver a smartphone with software that meets consumer expectations, also having regard to the nature of that software and Samsung's announcements about it.

103. What can the consumer reasonably expect of his Samsung smartphone and the software on it??[41] He can indeed expect that he will receive a smartphone that is secure, equipped with the most recent version of the operating system, that it is up to date, and that the software included will not contain any vulnerabilities that can be exploited by those with malicious intent. If these vulnerabilities do occur (will occur) he can expect that Samsung will fix these vulnerabilities within a foreseeable period by providing Updates and/or Upgrades. This applies fully to Updates that fix "critical" security breaches i.e. that are regarded by Google as "critical" having regard to the (potential) seriousness of the consequences (see paras. 19-21 above).

104. It must be noted that conformity problems may, inter alia, concern the quality and security of digital content, such as vulnerabilities in the software, with resulting security risks. This has been accepted in the relevant literature.

> *One may think of the situation where software contains a defect or bug, with security risks as a result. Such a problem can be classified as a security matter, but also as a quality problem.*[42]

105. The fact the consumer's aforesaid expectations are justified is also evident from an assessment of the relevant circumstances. The following and other matters are significant: i) the normal lifespan of a smartphone and the licence issued by Samsung, ii) the announcements made by Samsung and Google, iii) the nature of the thing, iv) the price, v) the potential risks and vi) the standards observed in practice.[43]

Lifespan and licence

---

[41] One must take into account the expectations of an average consumer who is reasonably well-informed and reasonably observant and circumspect,. ECJ EC 16 July1998, no. C-210/96, Jur. 1998, page I-4657, *Dutch Law Reports* 2000/374 (*Gut Springenheide*).

[42] M.B.M. Loos, N. Helberger, L. Guibault, C. Mak, L. Pessers, K.J. Cseres, B. van der Sloot & R. Tigner, *Analysis of the applicable legal frameworks and suggestions for the contours of a model system of consumer protection in relation to digital content contracts*, FINAL REPORT: Comparative analysis, Law & Economics analysis, assessment and development of recommendations for possible future rules on digital content contracts, 2011, p. 108 and 121.

[43] M.B.M. Loos *Consumentenkoop ('Consumer sale')* (Monographs on the Dutch Civil Code no. B65b), Deventer: Kluwer 2014, no. 30.

106. The consumer expects that he will be able to use his Samsung smartphone, and therefore also the software on it, securely for an extended longer period. The average expected duration of use by a consumer is 2.26 years (**Exhibit 22**). Many consumers conclude a two-year contract. However, the expected *lifespan* is still much longer than that, which is also evident from the lively trade in used smartphones without contract and the fact that many consumers switch to sim card only contracts after two years.

107. This alone means that Samsung's obligations do not end after the time of the purchase. This also follows from the fact that the consumer gets a licence from Samsung, which is not limited in time, for the extended use of the software (**Exhibit 15**) and that in this licence agreement Samsung also promises that it will provide Updates and Upgrades. This licence therefore assumes, in conformity with generally accepted practice, that the software in the smartphone must be updated. If Samsung does not do that, there will be non-conformity.

108. This is where the difference is from - for example - a washing machine or television set. Using these examples, the seller can only be expected to take an active role once the consumer makes a complaint about a specific defect. By contrast, with regard to the software in a smartphone, the supplier may be expected to play a pro-active role to prevent non-conformity. Having regard to the nature of the defects, a consumer cannot be required to first make a complaint, for the simple reason that he generally does not know that the software in his smartphone contains a vulnerability.

109. It is a generally known fact that the supplied software as well as a consumer's digital environment are subject to changes. Samsung knows that its software will be unavoidably exposed to vulnerabilities and that it will have to remedy these security defects.

110. A consumer's expectation that Samsung will provide Updates and Upgrades for his smartphone is also justified on the basis of the licence agreement. However, even if parties had not agreed to Samsung having an obligation to regularly provide Updates and Upgrades, Samsung is indeed obliged to do so. If this were different, that would undermine the mandatory protection provided to the consumer by Article 7:17 BW. Loos and others confirm this:

> *Express arrangements about the supply of digital content can be made for other agreements for the supply of digital content. If such arrangements have not been made, then the consumer can in my opinion nevertheless expect the supplier to ensure that the consumer can make use of the digital content for a reasonable period, to be determined according to the circumstances of the case, and that the supplier if necessary will support this use by means of providing updates free of charge.*[44]

Announcements made by Samsung and Google

---

[44] M.B.M. Loos, 'Europese harmonisatie van online en op afstand verkoop van zaken en de levering van digitale inhoud ('European harmonisation of online and distance sale of goods and the delivery of digital contents (II), *NtER* June 2016, no. 4, page 153. See also M.B.M. Loos, 'Consumentenovereenkomsten tot levering van digitale inhoud na de implementatie van de Richtlijn consumentenrechten, ('Consumer agreements for the supply of digital content after the implementation of the consumer rights Directive' *Mediaforum* 2015-3, p. 100) .

111. Not only the licence agreement that but also Samsung's announcements lead a consumer to legitimately expect that he will continue to receive Updates and Upgrades for his device in a timely manner. The fact is that, in its website, Samsung announces that the security of data and the protection of privacy enjoy the "highest priority" and that it makes endeavours to fix security breaches as quickly as possible.

> "*For Samsung the protection of privacy and the security of consumer data are of the highest priority. As the worldwide market leader in the field of mobile devices we also endeavour to be at the forefront in this field. We continuously work with our software suppliers, mobile providers and consumer associations on the process of maximising the efficiency of software updates and security updates .*" (**Exhibit 16 b**)

112. For its part Google writes that "Android seeks to be the most secure and usable operating system for mobile platforms" (**Exhibit 7 a**).[45] This announcement also has a bearing on the consumer's legitimate expectation that he has bought a smartphone with the securest operating system in existence.

The nature of smartphones

113. For many consumers a smartphone is an essential product in their daily life. Dependence on smartphones is high and, for a long time, consumers have not only been using their smartphones for communication. They also save large amounts of (sensitive) (personal) data in their phones, such as their diaries, contacts, photos, email etc. This important functionality means that consumers also have high expectations with regard to the security of their smartphones.

114. This expectation is also legitimate when one considers the high cost of a smartphone for consumers. Samsung's market position as the worldwide market leader also raises expectations.

(Potential) damage

115. The fact that consumers save large quantities of (sensitive) personal data in their smartphones means that the potential consequences of exploitation are serious, certainly in the event of critical security breaches. Also having regard to these risks, the consumer's expectation that Samsung will provide the smartphone with Updates and Upgrades during the lifespan of the device is legitimate.

Standards and duty of care that apply in the market to security and protection

116. As w set out in the body of facts, the importance of Updates and Upgrades is emphasised by supervisory authorities and courts, and "patches" form an essential part of the standards pertaining to information security.

117. Consumers are also guided by advice from the government and experts as regards their expectations of the security of their phones. Given that much of the advice from these parties places the emphasis on Updates and Upgrades (see paras. 30-39), the consumer's expectation is

---

[45] https://source.android.com/security/.

that his smartphone will also continue to receive them.

118. The fact that suppliers such as Apple (iOS) and Google (Nexus and Pixel) provide long-term Updates and Upgrades for similar smartphones in the same price range also has a bearing on consumer expectations.

Performance

119. The consumer is entitled to the repair of defective software on the basis of Article 7:21 (1) in conjunction with (3) BW. This "repair" can be carried out by providing Updates and Upgrades, thus repairing the software. This must be done within a reasonable period on the basis of Article 7:21(3) BW. A period of one month is reasonable and realistic because Samsung presently issues monthly updates for a number of models.

Section 13 of the Dutch Personal Data Protection Act ("Wbp")

120. Under this Act it also obligatory to provide Upgrades and Updates, and in any event Updates for critical security breaches.

121. Section 13 Wbp provides that the controller must take appropriate technical and organisational measures for the protection of personal data during the processing of personal data.

> *The controller implements appropriate technical and organisational measures to protect personal data against loss or any unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures will guarantee a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. These measures also seek to prevent the unnecessary collection and further processing of personal data.*

122. This duty of care applies directly to Samsung, as Samsung processes the personal data of its smartphone users, as is evident from clause 5 of the licence agreement (**Exhibit 15, p. 12**) and the privacy policy (**Exhibit 21**). Samsung collects location data, data on the device (such as the unique IMEI number), the IP address, the telephone number and contact details et cetera. These (partially sensitive) data is traceable to a natural person (the user of the device) and therefore must be regarded as personal data within the meaning of Section 1 Wbp. Samsung is the controller as regards this processing.

123. In addition, it is a generally known fact that consumers are increasingly saving (sensitive) personal data in their smartphones, e.g. in their diaries, address files and email.

124. In the aforementioned Protection of Personal Data Guidelines of the Dutch DPA referred to above, the Dutch DPA also details the duty to protect personal data in Section 13 Wbp. According to this supervisory authority, keeping software such as operating systems up to date by installing patches in a timely manner, is one of the measures that the controller must take. [46]

[46] Guidelines p. 23.

125. Other generally accepted information security standards, such as the Dutch Information Security Code (*Code voor Informatiebeveiliging*), or the IT security guidelines of the Dutch National Cyber Security Centre (*ICT-beveiligingsrichtlijnen van het Nationaal Cyber Security Centrum*), refer to the timely remedy of technical vulnerabilities by means of patches as an important security measure (see also paras. 30-39 above).

126. The supervisory authority the Netherlands Authority for Consumers & Markets (ACM) has identified patch management as an essential part of information security. According to the ACM, the presence of vulnerabilities in software means "security risks are always present". That is why companies must ensure that the necessary patches are implemented.

> *Lastly, the ACM points out that it also has ascertained that adequate patch management is a generally applicable and accepted part of information security. It is regularly noted that virtually all software contains vulnerabilities. These vulnerabilities make it possible to use the software in a manner other than what is intended, and, for example, makes it possible to breach the protection of sensitive data such as personal data. This means that security risks are always present.*
>
> *Thousands of vulnerabilities in software are discovered worldwide every year. Suppliers regularly publish security patches to fix vulnerabilities in software. […]*
> *In addition there must be a process for dealing with the patches that have appeared (analysing the risks of the vulnerability, testing the patch, deciding whether to install the patch, and the time frame within which all this must take place forms part of this). It must also be recorded which patches have or have not been installed in which systems.*
> *A company with proper patch management has a clear idea of the current state of the vulnerabilities of the software and systems it uses and the patches already applied by the company. In this regard a company must ensure that it implements the necessary patches and it must ensure that this patching causes as few disruptions as possible, or for example entails a minimum number of security risks to the protection of personal data.*[47]

127. This was the opinion of the ACM in its review of Section 11.3 of the Dutch Telecommunications Act (*Telecommunicatiewet*) ("Tw"). This section contains an obligation, which corresponds with Section 13 Wbp, for providers of public communication networks and services.[48] Section 11.3 Tw reads as follows:

---

[47] ACM decision on an objection by KPN B.V. against the decision dated 16 December 2013 imposing a penalty of EURO 364,000 was imposed on KPN B.V. for breaches of Section 11.3(1) in conjunction with Section 11.2 and Section 18.7(3) and (5) Tw, as well as against the decision dated 14 February 2014 ruling, on the basis of Section 8 of the Government Information (Public Access) Act, that the first mentioned decision would be published, paras. 91-92. See: https://www.acm.nl/nl/publicaties/publicatie/14313/Beslissing-op-bezwaar-KPN-zorgplicht/.

[48] The fact that both obligations of duty of care mean the same follows from Section 11.2 Tw and recital 20 of the e-Privacy Directive; this has also been repeatedly emphasised in the parliamentary history. See inter alia *Parliamentary Papers II* 2010/11, 32 549, no. 7, p. 42 and *Parliamentary Papers II* 2010/11, 32 549, no. 3, p. 73.

> *In the interest of the protection of personal data and the protection of privacy of the subscribers and users, the offerors referred to in Section 11.2 implement appropriate technical and organisational measures with regard to the security and protection of the networks and services offered by them. Having regard to the state of the art and the cost of their implementation, such measures will guarantee a level of security that is proportionate to the risk concerned.*

128. The ACM decided that KPN had breached this duty of care by insufficiently securing its systems and, in December 2013, it imposed a penalty. Among other things, the ACM accused KPN of not having patched the vulnerability in the software for 2 months after becoming aware of it, while the supplier had already made an Update available. [49] According to the ACM, KPN should have immediately installed the patch. [50]

129. The ACM upheld the decision when it ruled on the objection in June 2014. The three-judge division of the Rotterdam District Court also upheld the penalty on appeal.[51] The District Court also held that KPN had breached its duty of care, inter alia because the software concerned had not been patched for a period of time. According to the District Court Section 11.2 Tw and Section 13 Wbp purport to provide a "far-reaching obligation to use best endeavours". According to the District Court patch management is an important component of a proper security policy. The fact that in this case no personal data had in the end been removed by those acting with malicious intent did not affect the finding that the duty of care had been breached.

130. Samsung is therefore obliged, on the basis of Section 13 Wbp, to immediately fix the vulnerabilities in the software after becoming aware thereof, by installing Updates. This applies fully to vulnerabilities that Google classifies as "critical". By not providing its devices with these Updates in a timely manner, or by not at all providing its devices with Updates, Samsung takes insufficient technical and organisational measures to secure the personal data that it processes. As a result of this, users run the real risk that persons acting with malicious intent will gain access to their personal data.

131. On the basis of Section 50 Wbp in conjunction with Article 3:305a BW, the Consumentenbond may claim measures to remedy actions that are in conflict with Section 13 Wbp, such as in this case by in fact providing Updates and Upgrades.

Radio Equipment Directive

---

[49] ACM decision to impose a penalty on KPN B.V. for breaches of the duty of care provisions set out in Section 11.3(1) in conjunction with Section 11.2 Tw, 16 December 2013, para. 102. See: https://www.acm.nl/nl/publicaties/publicatie/14312/Boete-KPN-voor-onvoldoende-beveiliging-klantgegevens/.

[50] ACM decision to impose a penalty on KPN B.V. for breaches of the duty of care provisions set out in Section 11.3(1) in conjunction with Section 11.2 Tw, 16 December 2013, para. 111.

[51] Rotterdam District Court 8 January 2015, ECLI:NL:RBROT:2015:22 (*KPN v ACM*).

132. Samsung's conduct is also in conflict with the Radio Equipment Directive,[52] recently implemented in chapter 10 Tw. The Directive contains "essential requirements" that radio equipment – including smartphones[53] – must fulfil. These "essential requirements" include the obligation to secure equipment to ensure the protection of personal data and the privacy of the user and the subscriber and to prevent fraud.[54]

133. On the basis of Article 10 of the Radio Equipment Directive, manufacturers of radio devices such as Samsung must ensure that the equipment that they place on the market complies with the essential requirements. In this context Recital 27 of the Directive clarifies that all economic operators who play a role in the supply and distribution chain must take suitable measures to ensure that they only make available on the market radio equipment which is in conformity with this Directive.[55]

134. The implementation period of the Radio Equipment Directive has expired (12 June 2016). The envisaged amendment to the Dutch Telecommunications Act will take place at a time to be determined by Royal Decree. However, given that the implementation period has expired, the provisions of the Directive do indeed apply to the Dutch legal order because the courts must interpret Dutch law in accordance with the Directive.[56]

135. However, even without this interpretation in accordance with the Directive, Samsung as a manufacturer of the smartphone must ensure the protection of the personal data and the privacy of the user and prevent fraud. The fact is that the predecessor of the Radio Equipment Directive, Directive 1999/5/EC on radio equipment and telecommunication terminal equipment,[57] contained comparable "essential requirements" that are contained in the current Section 10.3 Tw and the Dutch Peripherals and Radio Equipment Decree 2007 (*Besluit randapparaten en radioapparaten 2007*).[58]

Not providing Updates and Upgrades (in a timely manner) is an unfair commercial practice.

136. During the smartphone's lifespan Samsung is also obliged to provide Updates and Upgrades in a timely manner on the basis of the prohibition of unfair commercial practices provisions of Article 6:193b(2)BW and Article 5 of Directive 2005/29/EC ("Unfair Commercial Practices Directive").On the basis of Article 11 of the Unfair Commercial Practices Directive, the

---

[52] Directive 2014/53/EU of the European Parliament and the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC.

[53] *Parliamentary Papers II* 2014–2015, 34 260, no. 3; Parliamentary Papers II 2015-2016, 34 260, no. 6.

[54] Article 3(1)(a) in conjunction with Article 3(3)(e) and (f) of the Radio Equipment Directive.

[55] Recital 27 of the Radio Equipment Directive.

[56] CJEU 5 April 1979, no. C-148/78 (*Tullio Ratti*).

[57] Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity.

[58] Article 3(3)(c) and (d) of Directive 1999/5/EC on radio equipment and telecommunications terminal equipment.

Consumentenbond has a lawful interest in combating unfair commercial practices for the benefit of consumers.

137. A commercial practice is unfair on the basis of this article if a trader acts in conflict with the requirements of professional diligence and the economic conduct of the average consumer whom the trader reaches, or on whom the trader is focused, is or could be materially disrupted.

138. On the basis of Article 3(1) in conjunction with Article 2(c) of the Unfair Commercial Practice Directive, the "commercial practice" concept also relates to acts of companies performed *after* commercial transactions and therefore also to acts carried out while a contract is being performed.[59]

139. The "professional diligence" concept in essence concerns the due care that can be expected from a reasonably competent and reasonably acting professional colleague.[60] According to the CJEU in the recent Sony judgment, it must be verified to what extent a trader's conduct is contrary to fair market practices, also having regard to the legitimate expectation of the average consumer.

> *It must therefore be ascertained whether the behaviour of the trader entails a possible violation of honest market practices or of the principle of good faith in the trader's field of activity, which in the present case is the manufacturing of computer equipment for the general public, in the light of the legitimate expectations of the average consumer.*[61]

140. As set out above, a consumer who purchases a (an expensive) smartphone expects to receive a device that is equipped with the most recent version of an operating system, which is secure, up to date, and that this will continue to be the case during the device's lifespan. The consumer expects that Samsung will fix vulnerabilities in the software as soon as possible.

141. It therefore can be expected from a reasonably competent and reasonably acting colleague that the smartphones are provided with (critical) Updates and Upgrades. However, in practice devices are traded which do not receive any Updates and Upgrades or receive Updates and Upgrades only for a few months (see paras. 150-153). This means that Samsung delivers software that by its nature will not last as long as the economic and technical lifespan, reasonably expected by the consumer, of the smartphone concerned. This is in conflict with the requirements of professional diligence.

142. This conduct can considerably influence the economic behaviour of the consumer. The fact is that if a consumer had known that his smartphone would no longer be secure after one year (or even in less than one year), that consumer would perhaps - probably - have chosen another device, which does ensure (and will continue to ensure) security. The fact that a smartphone no

---

[59] See also CJEU 16 April 2015, case C-388/13, ECLI:EU:C:2015:225 (*Nemzeti v UPC*), para. 36.

[60] D.W.F. Verkade, *Oneerlijke handelspraktijken jegens consumenten ('Unfair commercial practices in relation to consumers')* (Monographs on the Dutch Civil Code no. B49a), Deventer: Wolters Kluwer 2016, p. 28 .

[61] CJEU 7 September 2016, case C-310/15, ECLI:EU:C:2016:633 (*Deroo-Blanquart v Sony*), para. 34.

longer receives Updates and Upgrades can also be important for the consumer when determining his position on whether or not to retain his smartphone, or whether he can invoke the fact that it is non-conforming.[62]

Unlawful act

143. The fact that Samsung is acting in conflict with the statutory obligations under Article 7:17 BW, Section 13 Wbp, the Radio Equipment Directive and Article 6:193b BW, means it is committing an unlawful act.

144. However, even aside from this, Samsung is acting in conflict with the due care that can be expected from it according to generally accepted standards by not providing its smartphones with Updates and Upgrades, or at least not providing its smartphones with them in a timely manner, thus exposing its users to potential risks. Just as a coffee shop owner is obliged to close a cellar trapdoor as quickly as possible because leaving it open creates a risk for passers-by, Samsung also has a duty of care to remedy the security breaches in its software which are known to it, and thus to prevent users from suffering damage due to defects.[63]

145. In this context it is also relevant that Samsung is aware of the fact that there are new Updates and Upgrades available. Furthermore, Samsung is aware of the possible dangers ensuing from the failure to provide Updates and Upgrades in a timely manner, the (likely) damage to consumers is therefore foreseeable. In addition Samsung has generated the consumer's confidence that it delivers a secure device that will be provided with Updates and Upgrades in a timely manner. Samsung's capacity as the world's largest supplier of Android devices, as well as the Samsung's expertise in relation to consumers, underline the unlawful character of its conduct. In this context it is important that it is solely Samsung as the supplier of the software who is capable of fixing the vulnerabilities it contains. No party other than Samsung can provide Updates and Upgrades, even if it is not Samsung but rather a third party (such as a provider) that sells the smartphone concerned

INTERIM CONCLUSION

146. On the basis of all of the above Samsung is obliged to provide Updates and Upgrades in a timely manner so that the consumer can use his smartphone securely during its normal lifespan. This particularly applies to Updates intended to fix vulnerabilities that Google classifies as "critical" (**Exhibit 23**).

Misleading omission

147. In addition to offering Updates and Upgrades in a timely manner, Samsung must also inform Dutch consumers clearly and unambiguously of what the consumer can expect with regard to Updates and Upgrades. By not providing this information, or at least by providing this information very unclearly, Samsung is (once again) guilty of an unfair commercial practice,

---

[62] Unfair commercial practices in relation to consumers (Mon. Civil Code no. B49a) 2016/28 .

[63] Dutch Supreme Court 5 November 1965, *Dutch Law Reports* 1966/136 (*Kelderluik*) .

more specifically a misleading omission within the meaning of Article 6:193d BW and Article 7 of Directive 2005/29/EC (Unfair Commercial Practices Directive).[64]

148. In order to be able to make a properly informed choice, the consumer must when purchasing a smartphone have clear and reliable information available, inter alia regarding its software and specific characteristics. The CJEU confirmed this in a recent judgment on the sale of Sony computers with pre-installed software. In that case Sony had complied with this standard by clearly informing the consumer in advance.

> *In the present case, it is clear from the order for reference that, inter alia, the sale by Sony of computers with pre-installed software meets the expectations, as revealed by an analysis of the market concerned, of a significant proportion of consumers who prefer to purchase a computer already equipped and ready for immediate use, rather than to purchase a computer and software separately. Moreover, as is also apparent from the order for reference, prior to the purchase of the computer at issue in the main proceedings, Mr Deroo-Blanquart, as a consumer, was duly informed via Sony's retailer of the existence of pre-installed software on that computer and the specific nature of each of those items of software.* [...].[65]

149. According to the CJEU, a consumer must to be able to make an "informed decision" that he is aware of all the terms of a contract and the consequences of concluding it.

> *As regards the clarification provided to the consumer, it must be highlighted that the information, before concluding a contract, on the terms of the contract and the consequences of concluding it is of fundamental importance for a consumer. It is on the basis of that information in particular that the consumer decides whether he wishes to be bound by the terms previously drawn up by the seller or supplier (judgment of 30 April 2014, Kásler and Káslerné Rábai , C26/13, EU:C:2014:282, paragraph 70).*[66]

150. However, Samsung does not provide clear information to consumers about which version of Android is installed on a smartphone and for how long the smartphones will continue to be supported by Upgrades and Updates.

151. A consumer who wishes to know where he stands must do a lot of searching and clicking through the Samsung website. For every device, a consumer must first scroll through to the "Tech Specs" of a selected smartphone where information is provided about inter alia the processor and the resolution of the smartphone. The example below is the Galaxy S6.

---

[64] Directive 2005/29/EC of the European Parliament and the Council dated 11 May 2005 concerning unfair commercial practices in the internal market and amending Directive 84/450/EEC of the Council, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) no. 2006/2004 of the European Parliament and of the Council ("Unfair Commercial Practices Directive")

[65] CJEU 7 September 2016, case C-310/15, ECLI:EU:C:2016:633 (*Deroo-Blanquart v Sony*), para. 35.

[66] CJEU 7 September 2016, case C-310/15, ECLI:EU:C:2016:633 (*Deroo-Blanquart v Sony*), para. 40.

bB

TECH SPECS

Processor	**Kloksnelheid** 2,1GHz, 1,5 GHz	**Processor** Octa Core
Display	**Formaat (Main Display)** 5,1 inch	**Resolutie** 2560 x 1440 (Quad HD)
	Kleurdiepte 16M	**S Pen** Nee

MEER SPECIFICATIES WEERGEVEN +

[Translation:

Processor	CPU Speed	CPU Type
Display	Size (Main Display)	Resolution
	Colour depth	S Pen Support]

152. After that the consumer must click on "show more specs +". The information that then appears relates to inter alia the camera, the memory and the network specifications. When the consumer scrolls all the way down he will ultimately arrive[67] at the heading "software support", where summary information is provided about the software support period, the version of Android and whether the Stagefright bugs 1.0 and 2.0 have been patched.

Software Support Periode tot maart 2017	**OS versie** Android 6.0.1	**Stagefright 1.0 Status** Bijgewerkt
Stagefright 2.0 Status Bijgewerkt	※ **Meer informatie** Zie www.samsung.com/nl/software-en-security-update voor meer informatie.	

[Translation:

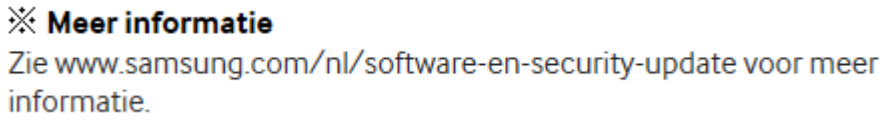
Software Support Period	OS version	Stagefright 1.0 Status
until March 2017	Android 6.0.1	Updated
	Stagefright 2.0 Status	More information
	See www.samsung.com/nl/software-en-security-update for more information.]	

153. A consumer who at this time (November 2016) considers purchasing the Samsung Galaxy s6 will therefore still receive software support for a maximum period of 4 months (until March 2017). The consumer can only find this important information by executing the actions described above on the Samsung website. The average consumer will not do this.

---

[67] The consumer first has to scroll past the headings "camera", "memory", "network", "connectivity", "operating system". "general information", "sensors", "physical specifications", "battery", "audio and video", "services and applications" and "extra information".

154. Reference is made to the following page for further information: www.samsung.com/nl/software-en-security-update. This link is not active so the consumer must copy and paste it into his browser to visit the page concerned.



[Translation:
More information
See www.samsung.com/nl/software-en-security-update
for more information]

155. If the consumer does this he will arrive at the FAQ page entitled "Samsung software support" (**Exhibit 16 b**).[68] It states that Samsung endeavours to roll out Updates as quickly as possible for as many devices as possible, but a particular device may simply not receive Updates.

156. As to whether Upgrades are provided, Samsung states that during the software and support period it endeavours where possible to provide devices with the most recent Android version , but that it cannot promise that the consumer will always receive the most recent version in his phone.

157. Nothing is stated about the guarantee of software support or about the version to which specific devices can be updated. It is absolutely not clear to a consumer how long and how often he can expect such Updates. There is no information whatsoever about Upgrades. Samsung's policy - insofar as Samsung's FAQ page can be classified as such - does not contain s single specific promise.

158. The question of whether a smartphone is equipped with the most recent version of an operating system, or whether a consumer can expect an Upgrade, is essential information for the consumer which can considerably influence his choice of which smartphone to purchase. The fact is that the operating system (and its status) is one of the most important characteristics that determine the choice of a smartphone. Whether a smartphone will be provided with Updates to ensure security and protect privacy during the required period of use and lifespan is also information that can influence a consumer's decision.

159. The omission of this information could induce the consumer to make a decision on a transaction that he would not otherwise have made. The fact is that if the consumer had known that his new Galaxy s6 smartphone would only receive Updates for 4 months instead of for

---

[68] http://www.samsung.com/nl/support/skp/faq/1097862.

approximately the two years for which he wishes to use the device, he would perhaps have chosen another device.

160. This is underlined by the fact that consumers refer to the defective provision of information as one of the most important problems for digital content such as software. This is shown inter alia by research conducted by the European Commission, which points to lack of information and transparency as a "main source of personal detriment" for the consumer.

> *Problems relating to the complexity, transparency and timing of contract agreements represent a source of detriment as information that is, for example, unclear, hidden or lacking, can create problems for consumers where they are not aware of the full contract conditions when interacting with content and services.*[69]

161. The security and safety of hardware and software are also important points of concern for consumers according to this research.[70]

162. The Dutch DPA's Cyber Security risk report (**Exhibit 24**) also flags up the fact that consumers are often ignorant about software vulnerabilities, as a result of which they are often exposed to cyber-attacks for an unnecessarily long time.

> *Cyber criminals often make use of vulnerabilities and errors in software. Errors made by software programmers result in flaws and ignorance about whether modification costs incurred by end users create exposure to cyber-attacks for an unnecessarily long time.*[71]

163. It is evident from recent research conducted by Sammobile (**Exhibit 25)** that the Update policy is information that could considerably affect the choice made by the consumer. 86% of almost 6000 respondents answered the question "*does Samsung's update policy affect your decision to buy a new Galaxy smartphone?*" in the affirmative.[72]

164. Even if it were to be assumed that Samsung will indeed provide information regarding the Policy on Updates and Upgrades, its commercial practice is still unfair. The fact is that, on the basis of Article 6:193d(3) BW, providing information in an unclear, incomprehensible, or ambiguous manner constitutes a misleading omission. Since Samsung's provision of information on Updates and Upgrades is at best minimal, and that this information is also hidden behind links that cannot be followed, and does not contain any specific undertaking, it

---

[69] Digital Content Services for Consumers: Assessment of Problems Experienced by Consumers (Lot 1), Report 4: Final Report, p. 7 and p. 57 et seq. Se: http://ec.europa.eu/justice/consumer-marketing/files/empirical_report_final_-_2011-06-15.pdf.

[70] Digital Content Services for Consumers: Assessment of Problems Experienced by Consumers (Lot 1), Report 4: Final Report, p. 59.

[71] Netherlands Bureau for Economic Policy Analysis (*Centraal Planbureau*) report p. 19.

[72] http://www.sammobile.com/2016/02/17/poll-does-samsungs-update-policy-affect-your-decision-to-buy-a-new-galaxy-smartphone/.

cannot be stated that Samsung provides the information in a manner that is useful and comprehensible to the consumer.[73] In its *UPC v Nemzeti* judgment, the CJEU confirmed that, when assessing unfair commercial practice, ascertaining whether the consumer could himself have obtained the information is irrelevant.

> *In the light of the foregoing considerations, UPC's assertion that the consumer, in this case, could himself have obtained the correct information must therefore be regarded as irrelevant.*[74]

165. When assuming a misleading omission, it is not a requisite that the consumer in question has actually taken note of, or was actually influenced by the commercial practice, but only that the inaccuracy or incompleteness of the commercial practice was of sufficient material importance to *be able* to mislead the average consumer (the "reference person") . It is sufficient that the consumer has been prevented from making an informed choice. This has been confirmed by the CJEU.[75]

166. In addition, in accordance with the Dutch legislature, this requirement will be readily fulfilled, and the requirement that the average consumer makes or has been able to make a decision about an agreement which the consumer would not have taken otherwise, will therefore not be problematic in practice.

> *A condition required for the existence of a misleading commercial practice is that a trader behaves in such a manner "as a result of which the average consumer has made or could make a decision about an agreement which the consumer would not have made otherwise". It is debatable whether this diminishes the legal protection of the consumer, as has been suggested by the persons asking the question. In our opinion this is not the case, because it is not easily imaginable that a commercial practice is unfair where, at the same time, the condition referred to has not been fulfilled. The fact is that the consumer only has to demonstrate that he has made or <u>could</u> make a decision on the basis of the conduct. It is expected that this will not result in many problems for consumers in practice.*[76]

167. The supervisory authority the ACM is of the same opinion:

> *It is not necessary that the consumer has actually been misled. Nor does he have to have made a decision or proceeded with a purchase. The point is that the average consumer might have obtained an incorrect impression due to a misleading commercial practice*

---

[73] Cf. CJEU 5 July 2012, case C-49/11, ECLI:EU:C:2012:419 (*Content Services*), from which it is evident that if information is present on the seller's website and this is only accessible through a link made available to the consumer, the information has not been provided to or received by the consumer.

[74] ECJ 16 April 2015, case C-388/13, ECLI:EU:C:2015:225 (*Nemzeti v UPC*), para. 54.

[75] ECJ 16 April 2015, case C-388/13, ECLI:EU:C:2015:225 (*Nemzeti v UPC*), para. 40.

[76] *Parliamentary Papers II* 2006/07, 30 928, no. 8, p. 6.

and, as a result, could have proceeded with the purchase of a product or service which the consumer would (possibly) not have done otherwise.[77]

168. As explained above, the consumer cannot make a conscious choice on the basis of the information provided by Samsung, and therefore this requirement is fulfilled.

169. In conclusion, the fact that Samsung does not inform users individually that it stops supplying Updates and Upgrades, and, if so, when, even though it has the personal data available, is in conclusion an independent unfair commercial practice. It must be considered that, as a result of this misleading omission, consumers are unable to take additional security measures such as making backups..

SAMSUNG DEFENCES

170. In discussing the facts and the legal framework above we have already partially dealt with and anticipated Samsung's known and expected defences. In addition, the Consumentenbond will briefly respond to the other defences put forward by Samsung's defence counsel during the oral arguments put forward in the earlier provisional relief proceedings.

No exploit yet

171. Samsung takes the position that consumer (information) security is not really in danger, because a requisite for that is that vulnerabilities in the software have been misused. In the earlier provisional relief proceedings Samsung emphasised the fact that there had not yet been any known Stagefright exploits (references).

172. However, the mere fact that no misuse has been made of a critical security breach does not mean that the risk of this is not serious and present and that the consequences could be very serious.

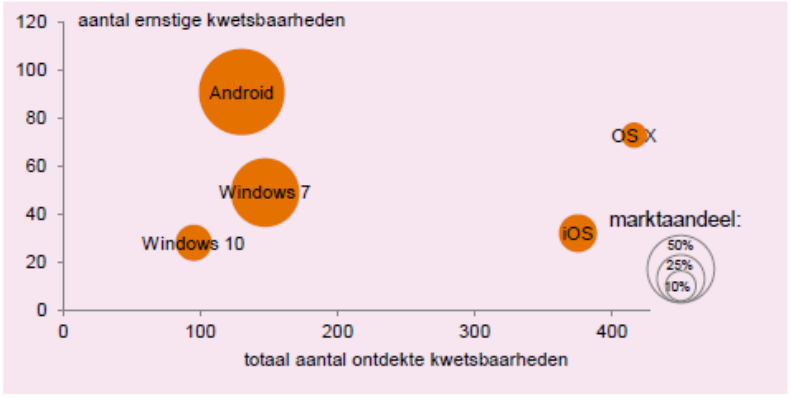
173. This is underlined by the fact that the more users certain software has, the more intensively hackers will search for possible vulnerabilities in it. The most frequently sold operating system worldwide, Android is therefore particularly vulnerable to misuse. This was also the conclusion of the CPB Netherlands Bureau for Economic Policy Analysis (*Centraal Planbureau*) in its most recent risk report based on figures (**Exhibit 24**).[78]

---

[77] https://www.acm.nl/nl/onderwerpen/consumentenrecht/oneerlijke-handelspraktijken/misleidende-handelspraktijken/.

[78] Pp. 17 and 18.

Figuur 2.4: Softwarekwetsbaarheden in besturingssystemen (2015)



Bron softwarekwetsbaarheden: www.cvedetails.com; marktaandelen: www.statistica.com.
Noot: omvang van de cirkel geeft het gemiddelde marktaandeel (wereldwijd) van het besturingssysteem weer in 2015.
Voor Android en iOS is het marktaandeel voor besturingssystemen van smartphones genomen.

[Figure 2.4: Software vulnerabilities in operating systems (2015)
Number of serious vulnerabilities
Market share:
Total number of vulnerabilities discovered
Source for software vulnerabilities: www.cvedetails.com; market share: www.statistica.com.
Note: the dimension of the circle represents the average market share (worldwide) of the operating system in 2015.
The he market share of Android and iOS operating systems in smartphones is shown.]

174. The mere fact that a vulnerability has not (yet) been misused successfully or resulted in a data breach does not mean that these vulnerabilities do not have to be remedied, or remedied more slowly. On the contrary, Samsung has the duty of care to remedy security breaches as quickly as possible to protect its clients and thus remove the risk of damage to the extent possible. As explained above, this is also how the Dutch DPA, the ACM and Rotterdam District Court have interpreted the duty to protect personal data.

Non-conformity

175. In the previous provisional relief proceedings Samsung took the position that the non-conformity rules do not apply. Principally, Samsung takes the position that these rules do not apply to the software in smartphones. Alternatively, Samsung asserts that there is no non-conformity because the vulnerabilities are inherent in software. Samsung also believes that, on the basis of its licence agreement, software is provided "as is", and the consumer therefore has no reason to expect Updates or Upgrades.

Applicability of Article 7:17 BW

176. As also set out above (paras. 47-50), a consumer who purchases a smartphone concludes a separate licence agreement for the (sustained) use of the software and receipt of Updates.

177. Samsung is the party that the consumer contracts with in this regard and Samsung is the party that is independently responsible for supplying software and keeping it up to date. Samsung is also the party that determines whether, how and when Updates and Upgrades will be provided. This is also the case if the smartphone concerned (the hardware) is not sold by Samsung but rather by a third party (such as a provider). The fact is that, in that case, it is still only Samsung who "pushes" the Updates and Upgrades from the cloud to the consumer's smartphone.

178. Samsung therefore cannot be regarded as the "agent" of the provider with regard to the software; on the contrary, it must be regarded as an independent supplier which the consumer can take action against for non-conformity. In accordance with the Beeldbrigade ruling, the contract of sale applies to this licence[79]

179. Samsung's argument (para. 4.7 of its pleading notes) that the Beeldbrigade doctrine does not apply to this case does not affect this, as the consumer does not purchase the software separately. As already stated, the software (and any Updates and Upgrades of it) and the agreement that the consumer concludes with Samsung in that regard, constitutes an independent part of what the consumer purchases. This software licence is separate from the purchase agreement for the hardware.

180. To the extent that "digital content" is required, as Samsung argues (para. 4.11 of its pleading notes), this requirement has automatically been fulfilled. Software is digital content.

181. Having regard to the independent character of the contractual relationship between the consumer and Samsung and the independent economic value represented by Samsung software, the purchase of a smartphone involves a mixed agreement for purchase and digital content. The software must be regarded as digital content which is not supplied on a tangible medium. This also applies to the Updates and Upgrades, which the consumer downloads by the consumer onto his smartphone. Pursuant to Article 7:5(5)BW, the contract of sale applies to them.

182. However, it must be noted that even if it were assumed that this concerns digital content on a tangible medium (in this case: a telephone), the contract of sale - and therefore the conformity rules - also apply to it.[80] In that case the digital content is regarded as movable property within the meaning of Article 7:5(1)BW. Samsung uses the data and personal data of the consumer as consideration to, among other things, analyse the use of the device and to make personalised offers. Samsung also places cookies, beacons and similar technical resources in the consumer's smartphone for analytical and advertising purposes.

Vulnerabilities inherent in software

183. The Consumentenbond disputes Samsung's submission, argued in the provisional relief proceedings (para. 5.7 of Samsung's pleading notes), that minor errors and vulnerabilities are inherent in software. The Consumentenbond also does not take the position that the mere existence of such a vulnerability in itself constitutes non-conformity. On the contrary, the non-conformity lies in the failure to fix the vulnerability in a timely manner, by supplying an Update or Upgrade.

---

[79] Dutch Supreme Court 27 April 2012, ECLI:NL:HR:2012:BV1301 (*Beeldbrigade*).

[80] Parliamentary Papers II 2012/13, 33 520, no. 3, p. 19.

184. Helberger and Loos also note - correctly - that the mere fact that software contains or will contain vulnerabilities still does not mean by definition that it is non-conforming, but it also takes as self-evident that the provider of digital content will in that case supply Updates, which the consumer must also install.

> *"More difficult to answer is the question whether flawed digital content that does not itself cause detriment but that leaves the consumer's hardware or software open to viruses and Trojan horses is also considered not to be in conformity with the contract. From the side of the industry, it is argued that it is normal that complex software has some flaws, defects, or bugs when it is first put on the market. In fact, automatic services updates are also used to address and fix newly discovered flaws as quickly and as efficiently as possible. […] A relevant and yet unresolved question in that context is to what extent consumers must cooperate, e.g., through installing the requested updates, in order to "qualify" for protection. It would seem justified that suppliers of digital content can reasonably expect the consumer to keep her software programmes updated and to allow for repairs of discovered defects, flaws, and bugs through automated services updates. […].*[81]

Agreement

185. The fact that Samsung has drawn up the licence agreement in wording to its maximum benefit, i.e. on an "as is" basis (para. 5.15 of its pleading notes 5.15), and by describing Updates and Upgrades as an "entitlement" of Samsung, does not affect the fact that Samsung is indeed obliged to provide Updates and Upgrades where errors in the software are shown to exist, and that Samsung can be expected to play an active role in this regard. This ensues from the nature and purport of the licence agreement which actually even advises consumers to regularly update their smartphones.

186. Any other interpretation would also be in conflict with the objective of the conformity rules provided to ensure a high level of consumer protection, given that it would then be quite easy to use contracts to void mandatory statutory provisions. On the basis of Articles 7:6(1) and 6:237(b)BW, this is not allowed.[82]

Update process is complicated and expensive

187. Samsung argues that the Update process is complex and expensive, partly because Android is a fragmented system and it supposedly depends on Google for supplying Updates.

188. Even if it were correct that making Updates and Upgrades available for all its devices would be complex and time-consuming, this would not release Samsung from its obligation to make Updates available in a timely manner. Nor may prioritising between devices result in consumers spending prolong periods with devices containing software that potentially could be misused in a serious manner It is self-evident that the fact that Samsung has opted to offer a

---

[81] Helberger, Loos et al., Digital Contracts for Consumers, p. 53.

[82] All this would also be in conflict with the requirements ensuing from the principle of reasonableness and fairness: Article 6:248 BW.

large product range of more expensive (and somewhat) less expensive smartphones is for its own account.

189. The Consumentenbond can be brief about the dependence on Google for the supply of Updates: the fact that Google is not the bottleneck in the Update process has already been explained above in the factual context. Google makes patches available to its partners, including Samsung, rapidly and in any event every month The Consumentenbond's aim in this case is that Samsung implements the patches made available by Google in its devices in a timely manner (within 1 month).

Samsung's performance is above average

190. Samsung will put forward that other products provide even less (clear) information (para. 6.8 of its pleading notes) and/or provide Updates and Upgrades for an even shorter duration. Samsung will presumably also argue that its smartphones score relatively well in consumer tests.

191. However, the fact that the performance of other manufacturers is just as bad or even worse than Samsung's performance does not automatically mean that action cannot be taken against Samsung, the market leader, for its own failures.

192. Nor does the fact that Samsung devices achieve good test results have any relevance to the question of whether Samsung fulfils its duty of care as regards Updates and Upgrades. The fact is that these tests are of the hardware, not the device itself. (The absence of timely) Updates and Upgrades (is) something the consumer experiences after purchasing a device. Furthermore, as stated above in the factual context, the Update performance data are not available to the public and Samsung is not transparent about them, meaning that Update performance cannot be measured in these tests anyway.

CLAIMS

193. The claim for relief defines the terms listed below as follows:

i. "Software": the Android operating system in the smartphone, whether or not provided with an extra Samsung software layer;
ii. "Update": a patch that (temporarily) repairs a vulnerability in the Software;
iii. "Upgrade": a new version of the Android operating system;
iv. "Smartphone": a smartphone that Samsung places or has placed on the market under its brand name
v. "Critical Update": an Update that repairs a vulnerability in the Software which Google regards as critical.

194. The claims can be explained as follows:

195. Claims I and II are for two declaratory decisions that, put briefly, Samsung is acting contrary to the duty of due care according to generally accepted standards and/or contrary to its statutory obligations, by (i) not providing the smartphones that its offers with Updates and/or Upgrades for the normal lifespan of the smartphones and/or not doing so in a timely manner, and (ii) by not informing consumers clearly about the period of protection of the device and - more generally - about its Policy on Updates and Upgrades.

196. With its claims III and V, the Consumentenbond's aim is for Samsung to provide Updates and Upgrades for the Software in its smartphones, for their normal lifespan, in a timely manner. Alternatively, the Consumentenbond is claiming that this order in any event be granted for "critical" Updates.

197. The Consumentenbond has decided on a period of four years following placement on the market and/or two years after the time of the sale by Samsung or through a retail channel. This two-year period meets the average expectation of the consumer, who usually concludes a two year contract. As regards four-year period, the Consumentenbond wishes to ensure that a consumer does not purchase a telephone that will only be supported by Updates and/or Upgrades for a few months, as is presently the case, because consumers also purchase devices that have been on the market for a longer time. This four-year period will therefore ensure that, in practice, consumers do actually receive Upgrades and Updates for (at least) two years. The time of placement on the market is objectifiable and therefore provides a good starting point. Apple also uses this period for its iOS system. The two-year period can be linked to the time when consumers consent to the licence agreement and Samsung's privacy policy.

198. A period of one month prior to the expiry of (critical) Updates, to be calculated from the time that Google informs Samsung about the vulnerability as well as the patch, is reasonable. This is because Samsung will be able to update the Software in its telephones from that time. One month will give Samsung sufficient time to implement the patch. This period is practically feasible for Samsung, as Samsung already applies this period for a select number of devices.[83] The Consumentenbond claims that Samsung should now apply this policy to all its devices, and not just the most recent models. A period of one month is also in line with thinking on the duty of care by supervisors , such as the ACM. The fact is that they have stated that patches must be tested and implemented immediately>

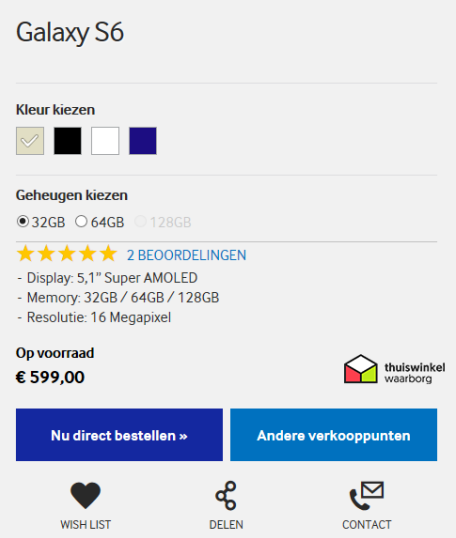
199. A period of three months is reasonable for providing Upgrades. Here we take account of the fact that Upgrades are often provided for the introduction of new functionalities and often involve major changes and, from a security point of view, are less urgent than Updates.

200. Claim V contains an obligation to provide information. As set out above Samsung's current provision of information is incomplete and abstract, and this information is also contained in links that do not open. The aim of this claim is also for Samsung to inform the consumer prior to the sale of a smartphone, the *point of sale*, clearly and unambiguously, about (i) the version of Android used in the smartphone, (ii) the date that the software support for the smartphone

[83] This is evident from statements made on Samsung's website, see http://www.samsung.com/nl/support/skp/faq/109786.

concerned ends and the consequences of this for the consumer, and (iii) its Policy on Updates and Upgrades, including the period for which the consumer can expect (critical) Updates and/or Upgrades.

201. Samsung must include this information about the version of the operating system and the period for which software support will be provided in the most important product specifications of the smartphone ("tech specs") set out on the Samsung website, in the same location that currently provides information about display, memory and resolution.



[Galaxy S6
Choose colour
2 REVIEWS
In stock
Order now Other retail outlets
SHARE]

202. Furthermore, clear reference to the entire policy must be included in the specifications, which must state clearly what the consumer can expect as regards Updates and Upgrades.

203. The same information (specifically for the model and more general information) must also be included in the printed user manual that the consumer receives along with his smartphone. This will ensure that the information also reaches the consumer if he purchases his smartphone somewhere other than through Samsung's website, for example through Bol.com or in a shop.

204. The requested orders are detailed to the extent possible. In deciding on the periods in question, the Consumentenbond has given consideration to Samsung's practical possibilities for taking action. In the unlikely event that this Court sees reason to limit the requested orders and/or to adjust these periods, the Consumentenbond requests that this Court exercises its jurisdiction as determined by the proper administration of justice.

ADMISSIBILITY

205. The Consumentenbond is an association with full legal capacity within the meaning of Article 3:305aBW. This was confirmed by the Dutch Supreme Court in a ruling in 1994.

> *The Consumentenbond is a legal entity which, in accordance with its charter and also in actual fact, is dedicated to representing consumer interests and which, in accordance with general criteria, must be deemed to be sufficiently representative to bring legal proceedings as and when necessary in order to protect collective consumer interests.*[84]

206. The Consumentenbond's object is to represent consumer interests in general, as follows from Article 3 of its Articles (**Exhibit 3**). In representing consumer interests, the Consumentenbond aims to secure "a worthy economic and social position of the consumer with regard to the production, distribution and consumption of private and collective goods and services."

207. As explained in para. 47-48, in pursuing this object the Consumentenbond carries out activities in the interest of protecting privacy and the private life of consumers. The Consumentenbond regularly issues legal proceedings in order to protect consumer interests.[85]

208. In these proceedings the Consumentenbond is acting in the interests of consumers who possess a Samsung smartphone. These interests are similar and therefore are suitable for bundling, because this enables legal protection to be obtained efficiently and effectively.[86] The fact is that Samsung's unlawful act is being committed against all consumers who have a Samsung smartphone and against all consumers who are considering purchasing a Samsung smartphone.

209. On the basis of Article 3:305aBW, the requested claims are also suitable for a collective action.[87]

210. The Consumentenbond has tried to achieve its aims set out in the claims by discussing them with Samsung. The Consumentenbond did so prior to the provisional relief proceedings and has done again during these proceedings on the merits (paras. 72-84). However, Samsung is not prepared to voluntarily satisfy the Consumentenbond's claims.

JURISDICTION

211. The District Court of The Hague has jurisdiction to hear this matter on the basis of Article 99 or Article 102 of the Dutch Code of Civil Procedure ("Rv"). Samsung Electronics Benelux B.V. has its registered office in Delft (**Exhibit 26**). In addition, the unlawful conduct and unfair commercial practices (also) take place through the internet, as Samsung's website (and

---

[84] This was also determined by the Dutch Supreme Court on 2 September 1994, *Dutch Law Reports* 1995/369 (*Consumentenbond v Nuts*).

[85] See the recent case Oost-Brabant District Court, 13 May 2016, ECLI:NL:RBOBR:2016:2425 (*Consumentenbond v Essent*);

[86] Dutch Supreme Court 26 February 2010, *National Case-Law Number (LJN)* BK5756 (*Stichting Baas in Eigen Huis v Plazacasa*); Dutch Supreme Court 9 April 2010, *National Case-Law Number* BK4549, *Dutch Law Reports* (*NJ*) 2010/388 (*Staat and SGP v Clare Wichmann et al.*).

[87] In this regard, compare Dutch Supreme Court 7 November 1997, *NJ* 1998, 268 (*Philips v VEB*).

webshop) are accessible throughout the Netherlands, including The Hague. Since the claims against both defendants are related, this Court also has jurisdiction to hear the claims against Samsung Electronics Co Ltd. on the basis of Article 107 Rv.

OFFER TO PRODUCE EVIDENCE

212. Insofar as the burden of proof on the basis of Article 150 Rv rests on the Consumentenbond, it hereby offers to prove its arguments by all lawful means. It offers in particular to prove the importance of Updates for (information) security and the right of consumers to the protection of personal data, if necessary by having (party-appointed) experts testify. In particular, the Consumentenbond offers evidence of its argument that, as regards information security, it is of the utmost importance that Updates and Upgrades are provided in a timely manner. The following expert is available to it, who can provide further evidence: Prof. Dr. B.P.F. (Bart) Jacobs, professor of Security and correctness of software at Radboud University in Nijmegen, the Netherlands.

213. The exhibits referred to in the summons will be entered into the proceedings on the Cause List Date.

THEREFORE

May it please this Court to issue judgment which, where possible, is provisionally enforceable:

I. containing a declaratory decision that Samsung is acting in conflict with the due care that can be expected of it according to generally accepted standards and/or that it is acting in conflict with the obligations pursuant to Article 7:17BW and section 13 Wbp and/or the Radio Equipment Directive and/or Article 6:193b et seq. BW, all this by acting as described in the body of the summons, in particular by not providing the Software in its Smartphones, for the normal lifespan of the smartphone or at least for a period of four years to be calculated from the time of its placement on the market, with (critical) Updates and/or Upgrades, and/or by not providing its Smartphones with (critical) Updates in a timely manner, or at least not within one month after becoming aware of the vulnerability and the patch (Update) from Google which is intended to eliminate the vulnerability;

II. containing a declaratory decision that Samsung is acting in conflict with the due care that can be expected of it according to generally accepted standards and/or that it is acting in conflict with the obligations pursuant to Article 6:193dBW and/or Article 6:193 BW, by not informing, or at least not clearly and unambiguously informing, consumers prior to their purchasing a Smartphone, about (i) the version of the operating system and/or the question of whether this is the most recent version and/or (ii) the question of whether, the device will receive (critical) Updates and/or Upgrades and, if so, for how long, and/or (iii) the consequences of this for the consumer, and/or (iv) the period for which the consumer can expect such (critical) Updates and Upgrades;

III. ordering Samsung to provide all Smartphones in the Netherlands, for a period of four years after their placement on the market and/or two years after the time of the sale by Samsung or through a retail channel, with Updates that repair these vulnerabilities in the Software, or at least Updates that repair a security breach in the Android operating system that Google regards as "critical", in every instance within one month after Google has made the Update available; alternatively, that this Court issues an order to be determined in the proper administration of justice;

IV. ordering Samsung to provide all Smartphones in the Netherlands, for a period of four years after their placement on the market and/or two years after the time of the sale by Samsung or through a retail channel, with Upgrades within a period of three months after Google issues the Upgrades; alternatively, that this Court issues an order in the proper administration of justice;

V. ordering Samsung to inform consumers, prior to their purchasing a smartphone, clearly and unambiguously about its Policy on Updates and Upgrades, in particular about (i) the version of the operating system in the smartphone and/or whether this is the most recent version and/or (ii) whether the smartphone concerned will receive (critical) Updates and/or Upgrades, and, if so, for how long, and (iii) the consequences of this for the consumer and/or (iv) how long the consumer can expect such (critical) Updates and/or Upgrades, by including the information under (i) and (ii) for each smartphone in the block containing the most important product specifications ("tech specs") in Samsung's website as well as in the (printed) user manual issued with the smartphone, and by including the information under (iii) and (iv) in a clear and easily accessible policy on Samsung's website as well as the (printed) user manual issued with the smartphone, all this in a manner that is adapted to the medium used; alternatively, that is Court issues an order in the proper administration of justice;

VI. ordering Samsung to pay an immediately due and payable penalty, which is not subject to mitigation, of EURO 50,000 in a lump sum for each non-fulfilment of any element described under III, IV and V, as well as EURO 50,000 for each day that such non-fulfilment continues, up to a maximum of EURO 1,000,000;

VII. ordering Samsung to pay the costs of these proceedings.

The costs incurred by me, process server, amount to:

Process Server

bB

T: +31 (0)20 – 760 6505 / F: +31 (0)20 760 6555
info@bureaubrandeis.com / bureaubrandeis.com