SUMMARY OF INVESTIGATION REPORT[1] Public Version

Microsoft Windows 10 Home and Pro investigation by the Autoriteit Persoonsgegevens (Dutch DPA), August 2017

1. SUMMARY

The Dutch DPA has investigated several versions of Windows 10, the operating system of Microsoft that has been available since the end of July 2015. There are more than 4 million active devices in the Netherlands (such as pc's, laptops and tablets) with Windows 10 Home and Pro. The Dutch DPA has found a number of violations during the investigation. During the investigation Microsoft has changed the data processing, by introducing the Creators Update in April 2017. This however has not ended the violations found in the investigation.

Telemetry

Microsoft continuously collects technical data from and about each device on which Windows 10 is installed. These data are called 'telemetry data'. Through telemetry, Microsoft for example collects a number of unique identifiers, in combination with data about hard and software on the device, and hardware connected to the device (such as routers and printers). Until April 2017 (in the Anniversary Update version), Microsoft offered three levels of telemetry: basic, enhanced and full. Since the launch of the Creators Update, on 11 April 2017, Microsoft only offers two levels of telemetry: basic and full.

The AP found during its investigation of the Anniversary Update that Microsoft collected data of a sensitive nature at the most limited (basic) level of telemetry, for example about the use of apps. At the enhanced and full levels of telemetry, Microsoft additionally collected data about the websurfing behaviour via its browser Edge, as well as (parts of the) content of hand written documents (on an inkpad). Microsoft has limited the collection of data at the basic telemetry level since April 2017. In this Creators Update Microsoft no longer collects data about app usage at the basic telemetry level. However, at the full telemetry level, Microsoft does collect detailed information about app usage, as well as data about websurfing behaviour through Edge and (parts of) the content of handwritten documents (via an inkpad).

In both versions of Windows 10 the level of telemetry is by default set to 'full', and the user is asked to accept these default settings. Microsoft also has switched 'On' that it may process the telemetry data to show personalised advertisements and recommendations in Windows and in Edge, including for all apps for sale in the Windows store, and that Microsoft and app developers may use the unique Advertising ID to show personalised advertisements in apps.

Data about behaviour

An operating system, such as Windows, can obviously not function without processing data. Some data are for example necessary to be able to access information on the Internet. But such data are not telemetry data. With telemetry Microsoft - as it were - takes pictures of the behaviour of Windows 10 users, and continuously sends these pictures to itself.

[1] This informal translation in English, provided by the Dutch DPA, is not legally binding. The public version of the full investigation report (in Dutch) contains 158 pages, and 3 annexes, with summaries of the written views of Microsoft on the report, with the response of the Dutch DPA.

Included in the telemetry data that Microsoft collects with the default setting of 'full telemetry', are personal data of a sensitive nature, data that reveal something about a person's behaviour. The AP has found that Microsoft (through the default setting of full telemetry) systematically charts information about app usage of users. This for example concerns the use of an app of an online casino, of a Turkish newspaper, of a magazine targeted at gay people, an app that indicates Islamite prayer times, an app collection details about a woman's pregnancy and an app targeted at diabetes patients. Microsoft can use these data to treat a person in a certain way or influence the behaviour of that person. And Microsoft factually does that, by showing people personal recommendations and advertisements.

Purposes Anniversary Update

Based on Article 7 of the Dutch data protection act (hereinafter: Wbp) a company may only process personal data for specified, explicit and legitimate purposes. During the investigation of the Anniversary Update, Microsoft processed the telemetry data (at all three levels of telemetry) for one or more of the following purposes:
1. Keeping Windows up-to-date;
2. Keeping Windows secure, reliable and performant;
3. Improve Windows (by means of aggregated analysis);
4. Showing personalised recommendations and advertisements within Windows and Edge.
These purposes were not explicitly described. Microsoft didn't have a full overview of the (categories of) personal data that the company processed through telemetry. It concerned a *big data* type of processing, in which engineers could continuously add new researches and could collect new categories of personal data. Therefore Microsoft was unable to determine, prior to the collection, what personal data it wanted to process for what purposes, and to inform users about these purposes. The AP therefore concluded that Microsoft acted in breach of Article 7 of the Wbp.

Purposes Creators Update

In the Creators Update, Microsoft distinguishes the purposes for which telemetry data are being processed. The basic telemetry data are always processed for the following three purposes:
1) Fixing errors;
2) Keeping devices up to date and secure, and;
3) Improving Microsoft products and services.
Microsoft offers users the possibility during installation to opt-out from the data processing for two other purposes, namely:
4) Showing personalised advertisements in Windows and Edge, including for all apps for sale in the Window store, and;
5) Showing personalised advertisements in apps, with the help of the Advertising ID.
Since the launch of the Creators Update, Microsoft offers an overview of the categories of data that it collects through basic telemetry, but only informs in a general way (with examples) about the categories of personal data it collects through full telemetry. The way Microsoft collects data at the full telemetry level, remains unpredictable. Notwithstanding [CONFIDENTIAL] internal review board, engineers may still add new kinds of data, and the collected data can be used for at least 3 purposes, or for 5 purposes (if the user has not actively opted out from the two kinds of personalised advertising)
Because of the combination of purposes for which the collected data may be processed, in combination with the lack of transparency, Microsoft can not obtain a legal ground for the data processing, such as consent or necessity for a legitimate interest. Therefore, the purposes for which Microsoft collects telemetry data can not be *legitimate*. Added to that, the description of the first four purposes is very broad, and does not meet the requirement of Article 7 that purposes need to be specific and explicit.

Therefore Microsoft still acts in breach of Article 7 of the Wbp, in combination with Article 6 of the Wbp (fair and lawful processing) with the collection of telemetry data, even after the introduction of the Creators Update.

Legal grounds

An organisation may only process personal data if it has a legal ground for it. The possible legal grounds are summed up in Article 8 of the Wbp. Microsoft has stated that the processing of telemetry data is based on three different legal grounds, namely: consent, necessity for its legitimate interest, and (in some cases) necessity for the performance of the contract. Microsoft also argues that it can rely on exceptions on the consent requirement from Article 11.7a of the Dutch Telecommunications Act (hereinafter: Tw, consent prior to the reading from or placing of information on the devices of end-users).

Consent for accessing information on a device

Article 11.7a Tw stipulates that users must give consent for the storing on or reading of information from their devices, after they have been provided with clear and complete information, at least about the purposes for which the information will be processed. Microsoft did and does not obtain this consent, because the information about the purposes was and is insufficiently clear. Microsoft therefore could and can not rely on consent.

Consent Wbp

Microsoft could not and can not successfully appeal to the legal ground of unambiguous consent of the data subject (the person whose personal data are being processed) for the processing of his or her data (article 8, under a, of the Wbp). Consent must namely comply with four criteria to be valid (specific, informed, unambiguous and free). The AP concluded that Microsoft did not comply with any of these criteria with the Anniversary Update. Based on the investigation of the Creators Update, the AP concludes that Microsoft still does not comply with three of the demands: informed, specific and unambiguous.

Informed and specific

Consent can only be given if it is informed, for specific kinds of data processing. That means that people should know precisely to what they say yes. But the (improved) information that Microsoft gives in the installation screen of the Creators Update about the different kinds of personal data the company processes, still falls short. The information does not make it sufficiently clear that at the full telemetry level, Microsoft continuously collects data about the usage of apps and websurfing behaviour through Edge, including for example specific news articles that have been read and locations entered into an app. After the installation, it is impossible, even for technically advanced system operators, to trace what personal data Microsoft is actually collecting via telemetry. Let alone for average users. They are not required to have to figure out themselves what personal data a company is collecting, they should be given clear and understandable information. Because Microsoft does not provide such information regarding the full telemetry level, the company does not obtain informed and specific consent.

Unambiguous consent

Consent must be provided unambiguously. That a person does not actively change the default settings during installation, does not mean he or she therefore gives consent for the use of his or her personal data. There may not be any doubt about the question whether a person has consented. Unambiguous consent can never be deduced from a lack to perform an opt-out. Additionally, the AP has established that with regard to some Windows 10 users in the Netherlands, Microsoft has not respected their existing privacy choices when they upgraded from the Anniversary Update to the Creators Update. Both for new users of the Creators Update, and for users that choose to install the new upgrade themselves, the telemetry level was set to full, and the use for advertisement purposes switched on, even if users had chosen basic telemetry in a prior Windows 10 version, and switched off the Advertising ID.

Other legal grounds

Microsoft could and cannot successfully base the processing of telemetry data on the legal grounds of 'necessary for a legitimate interest' (Article 8, under f, of the Wbp) or 'necessary for the performance of an agreement' (Article 8, under b, of the Wbp). Firstly, because Microsoft infringes on the Telecommunications Act, by not obtaining consent prior to the collection of data that are stored in the device. Because of this, Microsoft can not claim a *legitimate* interest. Secondly, Microsoft processes the telemetry data for different purposes and has not demarcated what personal data the company processes for each of those purposes. Because the data processing at the full telemetry level also involves data of a sensitive nature, and the interest of Microsoft does not outweigh the right to protection of the private life of data subjects, the company does not comply with the necessity requirement. Microsoft could possibly obtain a legal ground for the limited data processing at the basic telemetry level, if this were to be the default setting during installation, and users were enabled to give separate consent for the processing of telemetry data for the improvement of products and services of Microsoft, and the two advertising purposes.

Infringements of the law

In sum, Microsoft acts in breach of the law, because the company violates articles 7 and 8 of the Wbp. Microsoft also violates article 6 of the Wbp, because of the lack of specific purposes and transparency. Article 6 of the Wbp stipulates that personal data may only be processed in accordance with the law, in a fair and careful manner.

2. Investigation Method

Microsoft does not provide users access to the telemetry data collected on the device or sent to Microsoft. The network traffic is encrypted and protected with certificate pinning. Therefore the Dutch data protection authority (Dutch DPA) has collected information about telemetry in four other ways.

1. During the on site inspection on 22 June 2016 at the premises of Microsoft B.V. an engineer of Microsoft demonstrated a tool on his own laptop. This tool has been developed internally for Microsoft engineers to establish what telemetry data are being collected .
2. Between 4 and 8 July 2016, the Dutch DPA used Windows 10 as a regular user, and performed some activities on a research pc. This was a virtual machine, tests were conducted both on Windows 10 Home and Pro. A week later, the Dutch DPA asked Microsoft for a full overview of all telemetry data collected in that period. Microsoft was able to retrieve and combine all data from that user.
3. In July 2016, Microsoft provided a general overview of all telemetry data collected at the 'basic' level, that is, data Microsoft collected from actual Windows 10 users in the Netherlands in May 2016. Microsoft warned that this set may change over time. Microsoft stated that it had no overview of data collected on the enhanced and full level, because these were dynamic streams, created by different teams of engineers depending on their product needs.
4. In September 2016 and at the end of December 2016, the Dutch DPA obtained its own temporary copy of the tool, and performed a number of activities in 8 (December 2016: 12) different scenario's (that is, with or without Microsoft account, basic, enhanced or full telemetry, device *in* or *out* sample). In December 2016, the Dutch DPA also specifically tested switching off other settings after installation. The Dutch DPA performed these activities on the Anniversary update version of Windows 10 Pro. This way the Dutch DPA could record what data were being stored on the device (having testimony that all these data were actually transferred to Microsoft servers, either immediately or in batches of 15 minutes or 4 hours). The collection of data by the Dutch DPA however was limited in time (1 x 4 days, 1 x 3 days, about 1 hour per day), and only reflects the limited activities the Dutch DPA undertook (some app usage, some browsing). Microsoft has

testified the tool does not capture all telemetry data transferred to Microsoft. The tool doesn't capture telemetry data collected during start-up and install.

5. On 11 April 2017 Microsoft launched the Creators Update version of Windows 10 Home and Pro. With the release, Microsoft published two new information sources about basic[2] and full telemetry.[3]
6. Between May and June 2017, the Dutch DPA obtained a new temporary copy of the tool, and performed a number of activities in 9 different scenario´s in the Creators Update (with or without Microsoft account, basic or full telemetry, device *in* or *out* sample, and 1 privacy paranoid setting, with all options manually turned off, including 'Smartscreen' in the browser Edge).

3. Definition telemetry data

The Dutch DPA uses the following definition of telemetry data. All technical data that are collected from and about devices with Windows 10 Home and Pro through the Universal Telemetry Client. This includes the Advertising ID and data about inking and typing. Telemetry does not include the data that are necessarily sent from devices to allow for communication on the Internet, such as transferring your location to a weather app to determine the weather in your location. Telemetry is a separate registration of metadata about the use of software and the functioning of the device.

Based on the last investigation of the Creators Update (May-June 2017) with the Data Viewer Tool, and the new information published by Microsoft about information collected at the basic and at the full telemetry level, Microsoft collects the following data through telemetry at the '**basic**' level:

Local account	**Microsoft account**
	CDNId - ID for the used Content Delivery Network. [CONFIDENTIAL][4]
	PCFP - unique computer hardware ID. Concerns a hexadecimal number range, based on a hash of certain unique data about the device, for example [CONFIDENTIAL]. The value of this identifier is identical to the InventoryId;[5]
	UserGuid - unique global User ID. The value is a hexadecimal number range;[6]
	CustomUserID - user ID. The AP has only observed this identifier with an empty value;[7]
	IMEI - If a laptop or tablet has a GSM modem, the IMEI will be read, the globally unique hardware

[2] Microsoft, 5 April 2017, URL: https://docs.microsoft.com/en-us/windows/configuration/basic-level-windows-diagnostic-events-and-fields

[3] Microsoft, 5 April 2017, URL: https://docs.microsoft.com/en-us/windows/configuration/windows-diagnostic-data

[4] Microsoft mentions a different description in her overview of basic telemetry, but has announced to the AP it will correct this description. [CONFIDENTIAL]. The AP has only observed this identifier at basic telemetry via the Microsoft account. At full telemetry the AP has also observed this identifier in the local account. See Appendix 3 [CONFIDENTIAL].

[5] Microsoft mentions in her overview of basic telemetry: ***PCFP**: An ID for the system that is calculated by hashing hardware identifiers*. Microsoft also mentions *InventoryId: The device ID used for compatibility testing*. The value of this item is identical to the PCFP identifier. This is likely another name for the DeviceDataId recorded by the AP in previous investigations with the Data Viewer Tool. The AP did not observe these two identifiers (PCFP and InventoryID) via the local account. See Appendix 3, [CONFIDENTIAL].

[6] Microsoft mentions in her overview of basic telemetry: ***UserGuid:** The CEIP user ID*. With the abbreviation CEIP Microsoft means: *Customer Experience Improvement Program*. In a different telemetry message, Microsoft provides another description, namely: *UserGuid: A unique global user identifier*. See Appendix 3, [CONFIDENTIAL].

[7] Microsoft does not mention this identifier in her overview of basic telemetry. See Appendix 3 [CONFIDENTIAL]. The content was empty during the investigation by the AP.

	number of the modem;[8]
	Microsoft processes several unique device identifiers (Device Ids) in the telemetry messages: • **WUDeviceID/wuDeviceid/WUMachineId**: a unique device identifier that is used for updates. The value is a hexadecimal number range;[9] • **DUID**: a unique device identifier. The observed value was #;[10] • **customDeviceId**. The value is a hexadecimal number range;[11] • **XboxLiveDeviceId / did**. The value is a hexadecimal number range. This device identifier is used to identify an Xbox console or device that uses the Xbox app / network; names are XboxLiveDeviceID -also XBL - did or xid;[12] • **OneDriveDeviceId**. The value is a hexadecimal number range;[13]
Information about **crashes**, such as a crash of an app, revealing the name of the app;[14]	
deviceID - a device identifier. Microsoft does not mention this identifier in her overview of basic telemetry. The value is a hexadecimal number range, for example: [CONFIDENTIAL].[15]	
(User) LocalId - a unique user identifier created on the device. The value is a hexadecimal number range, for example: [CONFIDENTIAL]. This ID is not the same as the account ID;[16]	

[8] Microsoft mentions in her overview of basic telemetry: ***IMEI***: *Represents the International Mobile Station Equipment Identity. This number is usually unique and used by the mobile operator to distinguish different phone hardware.* See Appendix 3 [CONFIDENTIAL]. The AP has only observed the IMEI with a Microsoft account, not with a local account. The content is empty, because the investigation VM did not contain a telephone card.

[9] Microsoft mentions these identifiers in her overview of basic telemetry in the categories: SoftwareUpdateClientTelemetry, Microsoft.Windows.Update and Census.WU, with the following descriptions: ***WUDeviceID***: *The unique identifier of a specific device, used to identify how many devices are encountering success or a particular issue; UniqueDeviceID; The unique device ID controlled by the software distribution client; The Windows Update device ID.* ***wuDeviceid***: *The Windows Update device GUID; Unique device ID used by Windows Update; UniqueDeviceID; Device id on which the reboot is restored.* ***WUMachineId***: *Retrieves the Windows Update (WU) Machine Identifier.* See Appendix 3 [CONFIDENTIAL]. Observed at basic telemetry via the Microsoft account. At full telemetry observed both via the local and the Microsoft account.

[10] Microsoft mentions this identifier in her overview of basic telemetry in the category Census.Hardware, with the description: *The device unique ID.* See Appendix 3 [CONFIDENTIAL].'.

[11] Not mentioned by Microsoft in her overview of basic telemetry. Observed by the AP in the category: [CONFIDENTIAL]. Recorded by the AP on 2 and 7 June 2017, see Appendix 3 [CONFIDENTIAL]. Observed via the Microsoft account both at basic and full telemetry, not via the local account.

[12] Microsoft mentions these identifiers in her overview of basic telemetry in the category Census.Xbox and for 'did' in Common Data Extensions.XBL, with the descriptions: *Retrieves the unique device id of the console* and *XBOX device ID.* Recorded by the AP on 2 and 13 June 2017, see Appendix 3 [CONFIDENTIAL]. The AP has only observed [CONFIDENTIAL]. via the Microsoft account, not via the local account.

[13] Microsoft mentions these identifiers in her overview of basic telemetry in the category: Microsoft.OneDrive.Sync.Updater, with the description: *The OneDrive device ID.* Recorded by the AP on 2 and 13 June 2017, see Appendix 3 [CONFIDENTIAL]. Observed via the Microsoft account, not via the local account.

[14] Microsoft mentions these identifiers in her overview of basic telemetry in the category: Microsoft.Windows.FaultReporting.AppCrashEvent, with the description: *This event sends data about crashes for both native and managed applications, to help keep Windows up to date. The data includes information about the crashing process and a summary of its exception record (…)* , see Appendix 3 [CONFIDENTIAL]..

[15] Not mentioned by Microsoft in her overview of basic telemetry. Observed by the AP in the category: [CONFIDENTIAL]., both with the local and the Microsoft account. Recorded by the AP on 2 and 7 June 2017, see Appendix 3 [CONFIDENTIAL]'.

[16] Microsoft mentions in her overview of basic telemetry in the category 'Common Data Extensions.User': *localId: Represents a unique user identity that is created locally and added by the client. This is not the user's account ID.* Observed by the AP in the categories

(Device) LocalId - a unique identifier for the device created on the device. The value is a hexadecimal number range, for example: [CONFIDENTIAL]. The value is equal to the value in the client registry in the map KLM\Software\Microsoft\ SQMClient \MachineId;[17]
OSDeviceName - generic name for the type of device. For example: [CONFIDENTIAL];[18]
Hard and software installed on the device, including manufacturer, drivers installed by the user or manufacturer;[19]
Installed apps (name, publisher, language);[20]
Use and amount of (processing) **memory, processor and BIOS** on the device;[21]
Region- and language settings;[22]
Information about **other devices connected to the device** (such as printers or routers, or the inkpad used by the AP); [23]
What browser is set as favourite (default) and changes to the default browser, plus **favourite programs to open web, pictures, movies, music and PDF files**.[24]

[CONFIDENTIAL]. see Appendix 3 [CONFIDENTIAL].

[17] Microsoft mentions in her overview of basic telemetry in the category 'Common Data Extensions.Device' *localId: Represents a locally defined unique ID for the device, not the human readable device name. Most likely equal to the value stored at HKLM\Software\Microsoft\SQMClient\MachineId.* De AP has observed this identifier in almost every telemetry message, see Appendix 3 [CONFIDENTIAL].

[18] Microsoft mentions in her overview of basic telemetry in the category 'Microsoft.OneDrive.Sync.Updater.CommonData' *OSDeviceName: Only if the device is internal to Microsoft, the device name.* Microsoft also mentions this identifier in the category 'Census.Hardware', with a different description: *The device name that is set by the user.* Last but not least Microsoft mentions this identifier in her overview of basic telemetry in the category: 'Microsoft.Windows.Update.UpdateStackServicing.CheckForUpdates' *DeviceName: The name of the device.* De AP has found the same value in an item with the name, [CONFIDENTIAL].' in the message: [CONFIDENTIAL].De AP notes that in the telemetry messages with the OSDeviceName, also the identifier OSUserName has been found, with as value asterixes ("*****"). Recorded by the AP in basic telemetry and Microsoft account, on 2 and 13 June 2017, see Appendix 3 [CONFIDENTIAL].

[19] Microsoft mentions in her overview of basic telemetry for example in the category Microsoft.Windows.Inventory.Core.InventoryDriverBinaryAdd: *This event sends basic metadata about driver files running on the system to help keep Windows up-to-date.* Recorded by the AP on 2 and 13 June 2017 in basic telemetry. See Appendix 3 [CONFIDENTIAL]..

[20] Microsoft mentions these data in her overview of basic telemetry in the category Microsoft.Windows.Inventory.Core.InventoryApplicationAdd, with the description: *This event sends basic metadata about an application on the system to help keep Windows up to date.* This includes for example: *Name: The name of the application. Location pulled from depends on 'Source' field* and *Publisher: The Publisher of the application. Location pulled from depends on the 'Source' field* and *objectInstanceId: ProgramId (a hash of Name, Version, Publisher, and Language of an application used to identify it).* Additionally, the AP has recorded the names of the apps Candy and Solitaire on 8 and 9 May, 2 and 6 June 2017 in a category not mentioned by Microsoft in her overview of basic telemetry. See Appendix 3 [CONFIDENTIAL]. These data are also being collected via basic telemetry in the category [CONFIDENTIAL]. See Appendix 3 [CONFIDENTIAL].

[21] Microsoft mentions in her overview of basic telemetry for example in the category Microsoft.Windows.Appraiser.General.InventorySystemBiosAdd: *This event sends basic metadata about the BIOS to determine whether it has a compatibility block.* The AP has not observed any telemetry messages in this category. However, the AP has found comparable information in telemetry messages from the category [CONFIDENTIAL]. See Appendix 3 [CONFIDENTIAL].

[22] Microsoft mentions in her overview of basic telemetry for example *InstallLanguage: The first language installed on the user machine.* Microsoft also mentions the category Census.UserNLS: *This event sends data about the default app language, input, and display language preferences set by the user, to help keep Windows up to date.* With regard to the region/locale, Microsoft describes: *locale: Represents the locale of the operating system.* Recorded by the AP on 2 and 13 June 2017. See Appendix 3 [CONFIDENTIAL].

[23] Microsoft mentions in her overview of basic telemetry for example in the category Microsoft.Windows.Inventory.Core.InventoryDeviceContainerAdd: *This event sends basic metadata about a device container (such as a monitor or printer as opposed to a PNP device) to help keep Windows up-to-date.* That Microsoft collects these data can also be observed from the telemetry category [CONFIDENTIAL]. Recorded by the AP on 2 June 2017, see Appendix 3 [CONFIDENTIAL]. The AP has only tested the inkpad with a Microsoft account.

[24] Microsoft mentions in her overview of basic telemetry in the category Census.Userdefault: *DefaultBrowserProgId :The ProgramId of the current user's default browser* and *DefaultApp: The current user's default program selected for the following extension or protocol: .html,.htm,.jpg,.jpeg,.png,.mp3,.mp4, .mov,.pdf.* Observed by the AP with the Microsoft account, see Appendix 3 [CONFIDENTIAL]. Only tested with a Microsoft account by the AP, not with a local account. The identifiers [CONFIDENTIAL].were also observed in the message: [CONFIDENTIAL]. The AP has changed the default browser from Edge to Firefox during the investigation.

Additionally, at the full telemetry level, Microsoft collects:

The user chosen name of the device[25], and for owners of a Microsoft account identifiers such as the Microsoft Office ID[26] and the Microsoft Account ID. For owners of a local account: a similar unique identifier for the local account[27];
The MAC address of network equipment such as routers (BSSID), and and user chosen names (SSID) of connected hardware such as routers and printers; [28]
When using the browser Edge: URL of every website visited, regardless of TLS.[29] Microsoft also collects the content belonging to a hyperlink (the DOM-content) if a user clicks on a hyperlink. [30] Microsoft also collects the URL of the start page and the favourite (default) search engine.[31] Microsoft also collects the referrer URLs[32] and when tabs are closed;[33]
Information about successful TLS handshakes from apps and the browser Edge;[34]
Data about usage of all installed apps, such as frequency, how often they are active (in the foreground), amount of seconds usage of mouse, keyboard, pen or touch screen[35];

[25] Microsoft mentions in her overview of full telemetry the *User-provided device name*, without description. As remarked above, Microsoft describes that she also collects the device name at basic telemetry. See Appendix 3 [CONFIDENTIAL].

[26] Microsoft does not mention this identifier in her overview of full telemetry. Recorded by the AP on 1, 7 and 8 June 2017, , see Appendix 3 [CONFIDENTIAL].

[27] Microsoft mentions in her overview of full telemetry as a general explanation under 'Common Data' that she adds to most telemetry messages: *User ID -- a unique identifier associated with the user's Microsoft Account (if one is used) or local account. The user's Microsoft Account identifier is not collected from devices configured to send Basic diagnostic data*. Not recorded by the AP, but Microsoft herself states that she only *adds* this identifier after receipt of the telemetry data on her servers.

[28] Microsoft mentions in her overview of full telemetry, in the category 'Device network info': *Available SSIDs and BSSIDs*. The BSSID is the MAC address of the device, the SSID is the user chosen username of the device. The AP did not connect a modem or router to the VM research machine, and has therefore not observed these telemetry messages.

[29] Microsoft describes in her overview of full telemetry in the category 'Microsoft browser data', that she collects information from the address bar and search queries, such as:
Text typed in address bar and search box
Text selected for Ask Cortana search
Service response time
Auto-completed text if there was an auto-complete
Navigation suggestions provided based on local history and favorites
Browser ID
URLs (which may include search terms)
Page title
Recorded by the AP on 3 May 2017. See Appendix 3 [CONFIDENTIAL].

[30] Not mentioned by Microsoft in the overview of full telemetry. Recorded by the AP on 3 May 2017. See Appendix 3 [CONFIDENTIAL].

[31] Microsoft mentions in her overview of full telemetry, in the category 'Device preferences and settings': *Default browser choice'*. Recorded by the AP on 1 and 7 June 2017, see Appendix 3 [CONFIDENTIAL]. The URL of the start page is recorded in the items [CONFIDENTIAL], the favorite search engine in the items [CONFIDENTIAL].

[32] Not mentioned by Microsoft in the overview of full telemetry. Recorded by the AP on 3,8 May, 1, 7 and 8 June 2017. See Appendix 3 [CONFIDENTIAL].

[33] Not mentioned by Microsoft in the overview of full telemetry. Recorded by the AP on 3,8 May, 1, 7 and 8 June 2017. See Appendix 3 [CONFIDENTIAL].

[34] Not mentioned by Microsoft in the overview of full telemetry. Recorded by the AP on 3 May 2017, full telemetry, local account, *out of sample.* . See Appendix 3 [CONFIDENTIAL]..

[35] Microsoft mentions in her overview of full telemetry, in the category 'Product and Service Usage data', the sub category *App usage*, with the description: *Information about Windows and application usage such as:*
OS component and app feature usage
User navigation and interaction with app and Windows features. This could potentially include user input, such as name of a new alarm set, user menu choices, or user favorites.
Time of and count of app/component launches, duration of use, session GUID, and process ID
App time in various states – running foreground or background, sleeping, or receiving active user interaction
User interaction method and duration – whether and length of time user used the keyboard, mouse, pen, touch, speech, or game controller (...)
Content searches within an app
(...).
Recorded by the AP on 3, 8 May and 1, 7 and 8 June 2017, see Appendix 3 [CONFIDENTIAL] (including the 7 apps specifically installed by the AP).

Content of activities in apps (such as location[36] and read news article[37])
When using an electronic pen: handwritten text, suggested words and (unencoded) pre and post context of written text;[38][39]
Additional information about errors/failures;
Advertising ID.[40]

[36] Microsoft mentions in her overview of full telemetry, in the category 'Product and Service Usage data', in the sub category *App usage* the item 'Content searches within an app'. Recorded by the AP on 3, 8 May and 1, 7 and 8 June 2017, see Appendix 3 [CONFIDENTIAL].
[37] Not specifically mentioned by Microsoft in her overview of full telemetry. Recorded by the AP on 3 and 8 May 2017, with a local account. , see Appendix 3 [CONFIDENTIAL].
[38] Microsoft describes in her overview of full telemetry in the category 'Inking Typing and Speech Utterance data' that she collects the following data related to a digital pen:
Type of pen used (highlighter, ball point, pencil), pen color, stroke height and width, and how long it is used
Pen gestures (click, double click, pan, zoom, rotate)
Palm Touch x,y coordinates
Input latency, missed pen signals, number of frames, strokes, first frame commit time, sample rate
Ink strokes written, text before and after the ink insertion point, recognized text entered, Input language - processed to remove identifiers, sequencing information, and other data (such as names, email addresses, and numeric values) which could be used to reconstruct the original content or associate the input to the user.
[39] Recorded by the AP on 1, 7 and 8 June 2017. See Appendix 3 [CONFIDENTIAL]. The AP has created a fictive medical file in Microsoft Word for the purpose of the investigation, similar to investigations into earlier versions of Windows 10. The AP has opened this file, changed words, and stored the file with the help of an inkpad and digital pen..
[40] Recorded by the AP only in full telemetry, with Microsoft account, on 8 May, 1 and 7 June 2017. See Appendix 3 [CONFIDENTIAL].