Fight to be Forgotten: Exploring the Efficacy of Data Erasure in Popular Operating Systems

Andreas Gutmann[1,3] and Mark Warner[2,3]

[1] OneSpan Cambridge Innovation Centre
[2] University College London Interaction Centre
[3] University College London Information Security Group
{a.gutmann,m.warner}@cs.ucl.ac.uk

Abstract. A long history of longitudinal and intercultural research has identified decommissioned storage devices (e.g., USB memory sticks) as a serious privacy and security threat. Sensitive data deleted by previous owners have repeatedly been found on second-hand USB sticks through forensic analysis. Such data breaches are unlikely to occur when data is securely *erased*, rather than being *deleted*. Yet, research shows people confusing these two terms. In this paper, we report on an investigation of possible causes for this confusion. We analysed the user interface of two popular operating systems and found: (1) inconsistencies in the language used around delete and erase functions, (2) insecure default options, and (3) unclear or incomprehensible information around delete and erase functions. We discuss how this could result in data controllers becoming non-compliant with a legal obligation for erasure, putting data subjects at risk of accidental data breaches from the decommissioning of storage devices. Finally, we propose improvements to the design of relevant user interface elements and the development of official guidelines for best practice on GDPR compatible data erasure procedures.

Keywords: Privacy Evaluation · Data Erasure · GDPR · Cognitive Walkthrough

1 Introduction

The right to erasure (or 'right to be forgotten') in Article 17 of the General Data Protection Regulation (GDPR) is considered by some to be the most difficult obligation to comply with [3, p. 64]. It states that data subjects can, with certain exceptions, have their personal data erased by the responsible data controller. Moreover, it states that personal data should also be erased without undue delay under other circumstances. For example, where the data is no longer required for the purposes it was originally collected, or when the data subject withdraws consent on which the processing was based. The UK's national data protection authority (ICO) states that data which is subject to a valid erasure request must be placed "beyond use, even if it cannot be immediately overwritten" and can, in certain circumstances, pose a significant data protection risk [5].

The terms 'delete' and 'erase' are often used interchangeably. The Merriam Webster thesaurus lists both words as related[4], whilst the Oxford and Cambridge dictionaries list them as synonyms[5]. Yet, in computer science these words have a different meaning, and the distinction between the two has consequences for compliance with data protection legislation.

From a technical perspective these terms describe different concepts. Erase typically describes purposeful overwriting of data with other data – rendering it immediately irretrievable – whilst delete typically refers to data being "forgotten" by the operating system (OS) and being marked as available for overwrite. This allows new data to be stored in its place when required, but is often retrievable until it has been overwritten.

It is perhaps unsurprising that confusion exists between these two terms due to their linguistic similarity and interchangeable use in everyday conversation. Yet, problems can emerge if a data controller is unaware of the technical differences, with significant risks developing that could lead to exposure through non-compliance with data protection legislation. For example, deleting rather than erasing data from a decommissioned storage device could result in a data breach. As most delete and erase operations are executed through a computer's OS, the user interface (UI) of these OS are well positioned to provide users with guidance on the appropriate use of delete and erase operations to limit confusion between these terms.

In this paper we report on an analytical investigation of potential conflicts between UI file removal functions in macOS 10.14 and Windows 10, and legal requirements for data erasure. We use accidental data breaches from decommissioned USB sticks as the context for a streamlined Cognitive Walkthrough to explore the gap between the legal data protection requirements for the erasure of data, and file removal functions in two popular OS. In doing so, we discover linguistic confusion within the UI of these OS, which could lead to increased uncertainty when data controllers undertake their legal obligation to erase data. As a result, our research identifies a need for guidelines and best practice on GDPR compliant erasure. We present a set of implications for practice that could be used to improve consistency between UIs and data protection legislation. Finally, our research evidences the importance of further investigations into the suitability of those tools most commonly used by non-experts to comply with regulatory requirements.

2 Background

In this section we first explore previous research into people's data hygiene, taking a particular focus on the hygiene of decommissioned storage devices. We then explore some of the technical nuances of delete and erase operations using modern day technologies.

[4] https://www.merriam-webster.com/thesaurus/delete
[5] https://en.oxforddictionaries.com/thesaurus/delete
https://dictionary.cambridge.org/dictionary/english/delete

2.1 Personal Data Hygiene

A large number of publications dating back to 2005 provide both longitudinal and intercultural insights into people's data hygiene. Researchers typically buy second-hand storage devices on the open market and forensically analyse them, and report their findings. The first of these studies was conducted on second-hand hard-disk drives (HDD) purchased in the UK back in 2005 [17] and was repeated yearly until 2009 [7]. Similar studies have be conducted on second-hand USB storage devices (e.g., [6]), and mobile phones (e.g., [16]). Studies of this nature are also not limited to the UK market, with similar research being carried out in other parts of the world (e.g., Australia [14] and USA [1]). Consistent across these studies is the presence of sensitive personal data from a large number of decommissioned drives due to failures in the erasure process. Jones *et al.* [7], for example, forensically analysed USB sticks bought in the UK and recovered personal data which included: birth certificates, videos of children at a school, client data, and police staff records (names and date of birth).

In addition, memory chips from decommissioned devices are commonly recycled into new electronics, even though some of their old content may still be available and could be recovered [9,10]. The risk of data breaches from recycled memory chips is likely to increase due to Directive 2012/19/EU on 'waste electrical and electronic equipment'. Article 4 aims at encouraging "cooperation between producers and recyclers" to integrate more recycled material in new equipment and Article 5 gives priority to achieving high recycle rates for small IT devices such as USB sticks.

Diesburg *et al.* [1] compared people's data hygiene practices with their intentions when decommissioning USB sticks, and found people regularly confusing delete and erase functions. The authors recovered data from 83.3% of USB sticks where previous owners anticipated it being "very hard" to recover.

In summary, people often fail to appropriately erase sensitive data when decommissioning USB sticks, and these devices can cause data breaches when sold as second-hand devices or recycled into new electronics.

2.2 Delete and Erase Functions

When files are written to a storage device, the device must be running some type of file system (e.g., FAT, NTFS). The job of a file systems is to keep a record of the existence and location of all files and folders written to the storage device. When a file is deleted, the record of the file is deleted, but the file's content remains and can usually be recovered. Over time, when additional files are written to the device, the deleted files may become overwritten, at which point they are no longer recoverable [4].

To improve the security around file deletion, *DoD 5220 Block Erase* requires that a file is overwritten (erased) a minimum of three times and then verified. An even higher level of security is obtained by erasing an entire storage device, ideally using the device's internal secure erase function. These functions can either execute a slow secure wipe operation, or in more modern drives can quickly

delete cryptographic keys that were used to encrypt each file on the device, making the data permanently unintelligible [4].

3 Methodology

We investigate and compare the UI for removing files in both macOS 10.14 and Windows 10. We focus on these two OS as they account for more than 97% of the desktop/laptop OS market share [12]. We perform an exploratory data collection using a streamlined Cognitive Walkthrough (CW) method to gain insights into how users may perceive the functionality of file removal operations in macOS 10.14 and Windows 10.

CW is a commonly used method for evaluating how well a system supports users towards achieving their goals. It places a particular focus on the users cognitive activities, e.g. their goals and knowledge [8]. This method is characterised by having an evaluator work through a series of tasks from the user's perspective, and to evaluate the systems ability to provide users with cues and prompts to guide them towards task completion.

We oriented ourselves on the process described by Rieman *et al.* [13] and Spencer [15] to prepare our CW. The context is defined by the UI's of macOS 10.14 and Windows 10. The user has basic familiarity with both systems and understands that the terms 'erase' and 'delete' denote similar concepts. The two goals were to (1) erase a single file on a USB memory stick and (2) erase all files on a USB memory stick. The necessary sequence of actions consist of locating the target for erasure, the appropriate UI elements to erase the file, and lastly erasing the file.

We installed both OS on separate devices and ensured that they were fully patched. We followed the streamlined CW approach by Spencer [15], conducting a step-by-step analysis of how the UI could guide the user attempting to execute the necessary sequence of correct actions. At each step of this process, we assess the visual cues available for the next action and the feedback given to the user after each action.

3.1 Forensic analysis

Prior to each CW we restored the test USB stick back to its "factory state" and analysed it with FTK Imager Lite 3.4.3.3[6] to confirm that no residual data was residing on the device. We then created a text file containing *lorem ipsum* placeholder text, and saved this file inside a folder on the USB stick. At the end of each CW, we forensically analysed the USB stick with FTK Imager Lite to determine whether the CW had resulted in a delete or erase operation.

The CW were conducted by the first author and evidenced with screenshots and note taking. The second author sighted the screenshots and notes and verified that they fulfilled the necessary sequence of actions, and were consistent with a typical user being guided by UI cues and prompts.

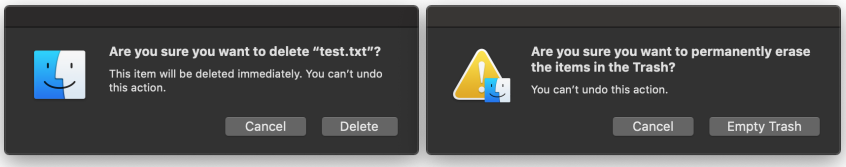
[6] https://forensicswiki.org/wiki/FTK_Imager

4 Results

In this section we report on the results from our CW following the process described in section 3. Although we maintained a detailed record of step-by-step user actions during each CW, we limit our reporting to UI screens presented to users that are relevant to either delete or erase functions. We present findings from a total of nine goal-oriented CW using two different OS. We then report the results from our forensic analyses which determine the effectiveness of these functions. In doing so, we can identify any inconsistencies between the UI's reported functionality and the underlying technical operation.

4.1 macOS 10.14

Goal: Erase a single file. To remove a file from a USB stick, the user can locate the USB stick in the *Finder* application and move the file to *Trash*. As the file is still visible in the *Trash*, the user can attempt to further remove it using either of two methods. (1) The user can right mouse button click on the file to open the context menu, and select *"Delete Immediately..."*. This opens a new dialogue window, which will inform the user that this action will immediately delete the file (see fig. 1a) and cannot be undone. The CW concludes when the user confirms the operation by selecting the *"Delete"* button. (2) The user can right mouse button click on the *Trash* symbol in the *Dock* to open the context menu, and select *"Empty Trash"*. This opens a new dialogue window, which informs the user that this action will permanently erase all files in the *Trash* and cannot be undone (see fig. 1b). The CW concludes when the user confirms the operation by selecting the *"Empty Trash"* button. Under both conditions our forensic analysis was able to recover the test file.



(a) Dialogue when deleting a single file from the *Trash*.

(b) Dialogue when deleting all files from the *Trash*.

Fig. 1: macOS 10.14 dialogues when deleting the test file from the *Trash*.

Goal: Erase all files on a USB stick. To remove all files on the USB stick, the user has two options. (1) They can remove all files similar to the removal of a single file (see above). Using this method entails that the files are deleted and

likely to be recoverable under a forensic examination. Alternatively, (2) the user can launch the *Disk Utility* application, and select the *"Erase"* option on the top feature bar. This opens a new dialogue window, which informs the user that this action will delete all data stored on the USB stick and cannot be undone. (see fig. 2). The CW concludes when the user confirms the operation by selecting the *"Erase"* button. Our subsequent forensic analysis was able to recover the test file.

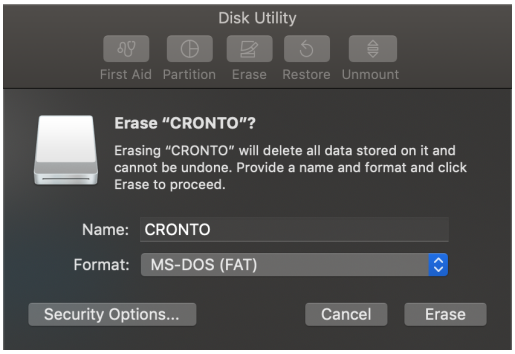


Fig. 2: macOS 10.14 dialogue when erasing the USB stick with *Disk Utility*.

In a variation to the above procedure, the user can select the *"Security Options"* prior to selecting the *"Erase"* button. This opens a new dialogue window (see fig. 3) where the user can select a range of security options. On the default option, the dialogue window informs the user that this will not securely erase the files and disk recovery applications may recover them. For the other three options, the dialogue window informs the user that the function will erase the data. The CW concludes when the user makes a selection and confirms the operation when selecting the *"OK"* button followed by the *"Erase"* button (see fig. 2). Our forensic analysis was able to recovery the test file when using the default security option, but unable to recover the file when using any of the other three secure erase options.

4.2 Windows 10

Goal: Erase a single file. To remove the test file from the USB stick, the user can locate the USB stick in the *Explorer* application and physically press the keyboard delete button whilst the file is selected. This opens a new dialogue window[7], which informs the user that this action will permanently delete the file (see fig. 4). The CW concludes when the user confirms this operation by

[7] Windows 10 treated our USB stick as 'removable media', which is why files were not placed in the *Recycle Bin* first. This might differ under other circumstances but is unlikely to affect the overall result of this CW.

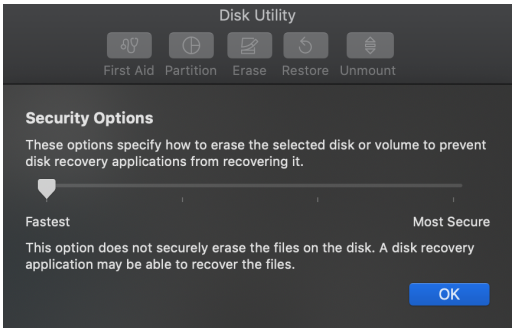


Fig. 3: macOS 10.14 dialogue to select *Security Options* when erasing the USB stick with *Disk Utility*. The lower description changes as different options are selected on the horizontal slider.

selecting the "*Yes*" button. Our subsequent forensic analysis was able to recover the test file.

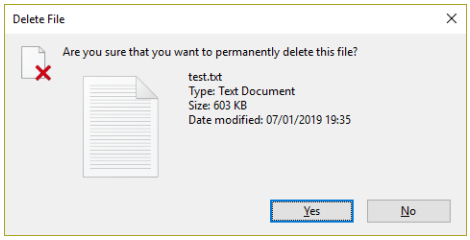


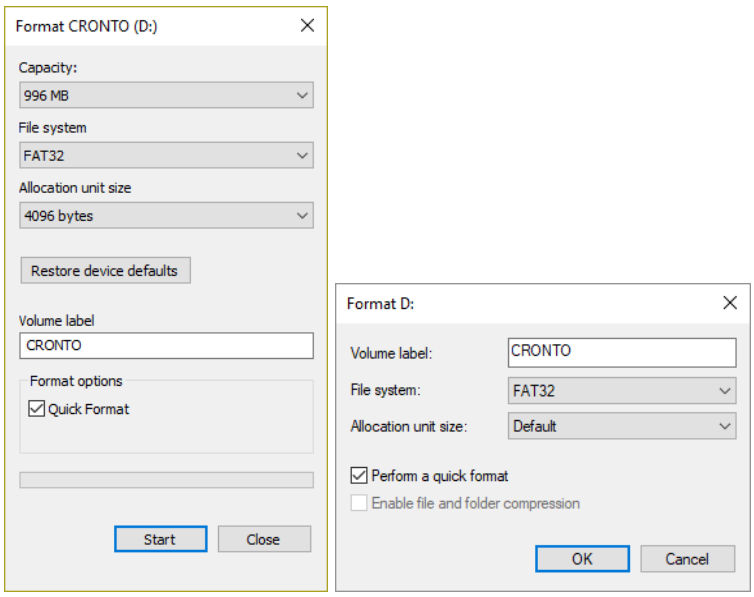
Fig. 4: Windows 10 dialogue when deleting the test file from the USB stick.

Goal: Erase all files on a USB stick. To remove all files on the USB stick, the user has three options: they can (1) proceed similarly to the removal of a single file[8] (see above), (2) access the "*Format*" dialogue from the *Explorer*, or (3) access the application "*Disk Management*".

If the user chooses to access the *Format* dialogue in *Explorer*, a new dialogue window opens (see fig. 5a), where the user can confirm the operation by selecting "*Start*". A second dialogue window informs the user that this will erase all data (see fig. 6a). The CW concludes when the user confirms this operation by selecting "*OK*". After performing this quick format operation, our forensic analysis was able to recover the test file. In a variation to the above, the user deselects "*Quick Format*" (which is selected by default) before selecting "*Start*". Our forensic analysis was unable to recover the test file after this operation.

[8] This option would entail that the files are deleted and likely to be recoverable under a forensic examination.

If the user chooses to access the *Disk Management* application, they can select "*Format...*" from the context menu of the USB stick. This opens a new dialogue window (see fig. 5b), where the user can confirm the operation by selecting the "*OK*" button. A second dialogue window informs the user that this will erase all data and suggests making a backup before formatting the USB stick (see fig. 6b). The CW concludes when the user confirms the operation by selecting "*OK*". After performing this quick format, our forensic analysis was able to recover the test file. In a variation of the above, the user can deselect "*Perform a quick format*" (which is selected by default) before selecting "*OK*". Consistent with previous results our forensic analysis was unable to recover the test file.

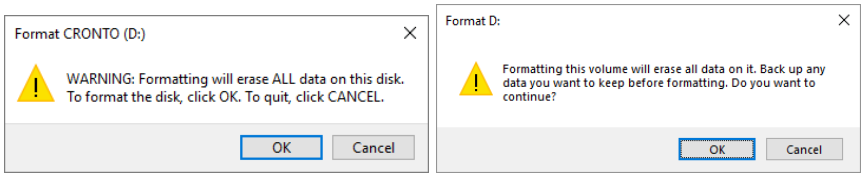


(a) Format dialogue accessed via *Explorer*.

(b) Format dialogue accessed via *Disk Management*.

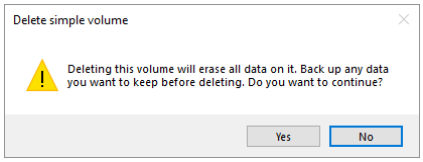
Fig. 5: Windows 10 dialogues when erasing the USB stick.

Alternatively, within the *Disk Management* application, the user can select "*Delete Volume...*" from the context menu of the USB stick. This opens a new dialogue window, which informs the user that the action will erase all data and suggests making a backup before deleting the USB stick (see fig. 6c). The CW concludes when the user confirms the action by selecting the "*OK*" button. After performing this delete volume operation, our forensic analysis was able to recover the test file.



(a) Dialogue when selecting to start *Formatting* a USB stick in fig. 5a (*Explorer*).

(b) Dialogue when confirming the *Formatting* of a USB stick in fig. 5b (*Disk Management*).



(c) Dialogue when confirming to *Delete Volume* of USB stick. (*Disk Management*)

Fig. 6: Windows 10 confirmation dialogues for formatting and deleting a volume.

4.3 Results of forensic analysis

Our CW identified three methods for removing a file from a test USB stick when using macOS 10.14, and six methods when using Windows 10. However, after completing a forensic examination of our test USB stick after performing each method, the test file was fully recoverable after two of the file removal methods in macOS, and after four of the file removal methods in Windows 10. (see table 1).

5 Discussion

Modern OS for computers commonly provide accessible data delete functionality to users. Yet, data erasure functions for entire drives are typically located at deeper levels of administrative tools, whilst functionality to erasure individual files is not provided without expert knowledge or the use of third-party software.

Restricting these functions can protect users from accidental data loss. However, omitting information, guidance, and functionality can place lay users – especially those in the role of data controller – at risk of causing accidental data breaches. This could result in data subjects having their data exposed, and organisations being non-compliant with data protection legislation.

In the following section we discuss the results from our investigation of delete and erase functions in macOS and Windows, and suggest alternative UI design approaches. We focus on default options and the terminology used to label and describe these functions in the UI; and then discuss the relevance of sufficient guidance for users. Entwined into these discussions, we argue for OS-dependent changes to the UI and highlight OS-independent implications of our findings.

Table 1: Summary of our forensic analysis for various methods to remove data from USB sticks. Data removed with a delete function was successfully recovered, data removed with an erase function was not recoverable.

System	Function	Forensic evaluation	
		Deletion	Erasure
macOS 10.14	**Goal** Erase single file		
	➤ Finder	✓	
	Goal Erase all files		
	➤ Disk Utility (default options)	✓	
	➤ Disk Utility (changed options)		✓
Windows 10	**Goal** Erase single file		
	➤ Explorer	✓	
	Goal Erase all files		
	➤ Explorer Format (default options)	✓	
	➤ Explorer Format (changed options)		✓
	➤ Disk Management Delete Volume	✓	
	➤ Disk Management Format (default options)	✓	
	➤ Disk Management Format (changed options)		✓

5.1 Default options

macOS 10.14 and Windows 10 provide functionality to securely erase all data from a USB stick. Yet, both OS use default options that reduce the effectiveness of these functions. We suspect that these default options are designed to increase the speed in which these operations are executed, with delete operations being much faster then erase operations to execute. Under macOS 10.14, the *Disk Utility* application contains security options (see fig. 3) to "specify how to erase the selected disk". Its default option contains a description that the files may be recoverable using certain data recovery applications. Figure 5 shows two UI screens for formatting a drive in Windows 10, with options "Quick Format" and "Perform a quick format" preselected. These options do not provide the user with any form of description. In both OS we were able to recover the test file when these default options were set.

Defaulting an option is commonly understood by users as a recommendation, reducing the likelihood of other options being selected by the user [11]. In the context of this research, default options discourage users from securely erasing files. Yet, those users might have significant interests in a secure erasure. We recommend an active selection process which encourages users to make an informed decision. In Windows 10, for example, the single confirmation button in fig. 5 could be replaced with two confirmation buttons to actively select between "Quick Format" and "Full Format".

5.2 Incorrect terminology

Inconsistent and incorrect terminology was used for delete and erase functions across both OS. For example deleting a file (or multiple files) from the *Trash* in macOS is labelled as both *delete* and *erase*, depending on whether a single file or all files are deleted (see fig. 1). However, our forensic analysis found that both of these functions perform a delete operation, as in both cases the test file was fully recoverable.

Incorrect use of the terms delete and erase in OS UI might reinforce colloquial use and foster the misunderstanding that they denote the same technical function. This interferes with users' ability to make informed decisions. We argue the terms erase and delete should be used exclusively in relation to their technical meaning. In some cases the outcome of an operation (i.e. whether the OS will execute an erase or delete function) depends on future input from the user, e.g. in fig. 2 the outcome of pressing the *Erase* button depends on possible changes to the default security option. Under such circumstances we recommend labelling the confirmation button with a neutral term, e.g. *'Proceed'*, and customising the description text depending on the selected security options.

5.3 Insufficient guidance and cues

During our CW we encountered multiple dialogue screens with insufficient or inadequate descriptions of underlying technical operation. For instance, the descriptive text in fig. 1 provides macOS users with a warning that they "can't undo this action". Whilst it may not be possible for users to undo this action using native functions within the OS, forensic software is able to fully recover these files. This can therefore create a false sense of security that these files are no longer recoverable. In Windows 10, when a file is deleted from the system, the final description of the function (see fig. 4) informs users that the file will be "permanently deleted" but lacks detail on what 'permanent' means and whether the file could, under certain conditions, still be recovered.

Informative and accessible descriptions are required for informed decision making. Information related to a user task should not be exclusively accessible through optional UI screens. On each screen, where a user can make a selection, the relevant consequences of this decision should be explained. We suggest adding informative text to describe the difference between delete and erase functions where it is contextually relevant within an OS UI. Furthermore, a note about the existence of file recovery applications should be added to all delete function confirmation screens.

5.4 OS-independent implications

Designers of UIs rely on metaphors to make complex and abstract functions more intuitive and comprehensible for users [2]. For instance, placing an unwanted *file* into the *recycle bin* uses multiple metaphors from an office environment, allowing users to relate these complex computing artifacts and processes to everyday

physical items and actions. Yet, the 'delete' and 'erase' metaphors are problematic, as they denote different meaning in the UI, whilst relating back to the same constructs in the physical world. Designers should therefore consider integrating new metaphors that better distinguish between these two functions to reduce the risk of confusion for users.

As well as being well positioned to provide users with guidance on the appropriate use of delete and erase functions, OS can also provide appropriate cues and prompts towards more secure outcomes. In section 2.1 we discussed past research showing how people intend to erase data from decommissioned drives but fail to do so securely, with researchers being able to recover data using digital forensic techniques. We propose OS should detect when a user deletes all (visible) files from a memory storage device, e.g. USB stick. Upon detection of this event, the OS could remind the user about the difference between delete and erase functions, nudging the user to take an informed decision before potentially decommissioning said device.

Lastly, we suggest official guidelines and best practice be developed on GDPR compliant erasure of data. This would be informative to users and provide OS a single source for developing consistent UI functionality across platforms. The European Data Protection Board[9] may be best positioned to develop these as they are already tasked with issuing guidelines, recommendations, and best practice on other GDPR-related topics (Article 70 GDPR), and consist of representatives from each national data protection authority (including EEA countries). In addition, national data protection authorities could make recommendations to carry out a data protection impact assessment (DPIA) for the process of decommissioning data storage devices, since this activity can be "likely to result in a high risk to the rights and freedoms of natural persons" (Article 35 GDPR).

6 Limitations

Cognitive walkthroughs are limited in that they do not involve (non-expert) users, the results are solely based on skills and expertise of the evaluators, and the frequency of identified problems cannot be estimated. This means that cognitive walkthroughs commonly only identify a subset of usability issues of the evaluation system. However, we do not believe this limitation reduced the validity of the issues identified in our analysis. The file system of the USB stick used in our study was set to FAT32 as it is the most commonly used file system for this type of device. We do not anticipate different file systems would have affected our findings but further work would be needed to confirm this.

7 Conclusion

We investigated possible causes for confusion around delete and erase functions, which was identified as a privacy and security threat in context of decommissioned USB sticks. In two of the most commonly used OS in today's market, we

[9] See https://edpb.europa.eu.

identified inconsistencies in the UI, insecure default options, and confusing and occasionally incorrect guidance. Finally, we propose design changes that could alleviate these issues and motivate a "call for action" for official guidelines and best practice on GDPR compliant erasure to be developed.

Acknowledgements

This work has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 675730, within the Marie Skłodowska-Curie Innovative Training Networks (ITN-ETN) framework.

References

1. Diesburg, S., Feldhaus, C., Fardan, M.A., Schlicht, J., Ploof, N.: Is your data gone?: measuring user perceptions of deletion. In: Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust. pp. 47–59. ACM (2016)
2. Donath, J.: The social machine: designs for living online. MIT Press (2014)
3. EY: IAPP-EY Annual Privacy Governance Report 2018. Tech. rep., International Association of Privacy Professionals (2018), https://iapp.org/media/pdf/resource_center/IAPP-EY-Gov_Report_2018-FINAL.pdf (Accessed: 21 December 2018)
4. Hughes, G.: Tutorial on disk drive data sanitization (2006)
5. ICO: Guide to the General Data Protection Regulation (GDPR) (2018), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/ (Accessed: 21 December 2018)
6. Jones, A., Dardick, G.S., Davies, G., Sutherland, I., Valli, C.: The 2008 Analysis of Information Remaining on Disks Offered for Sale on the Second Hand Market. Journal of International Commercial Law and Technology **4**(3) (2009)
7. Jones, A., Valli, C., Dabibi, G.: The 2009 analysis of information remaining on USB storage devices offered for sale on the second hand market. In: Australian Digital Forensics Conference. p. 61 (2009)
8. Mahatody, T., Sagar, M., Kolski, C.: State of the art on the cognitive walkthrough method, its variants and evolutions. Intl. Journal of Human–Computer Interaction **26**(8), 741–785 (2010)
9. Martin Westman: eMMC Chip Off – Benefits and Risks Workshop (2017), https://www.dfrws.org/conferences/dfrws-eu-2017/sessions/emmc-chip--benefits-and-risks-workshop (Accessed: 21 December 2018)
10. Martin Westman: Where Did That Incriminating Evidence Come From? (2018), https://www.dfrws.org/conferences/dfrws-eu-2018/sessions/where-did-incriminating-evidence-come (Accessed: 21 December 2018)
11. McKenzie, C.R., Liersch, M.J., Finkelstein, S.R.: Recommendations implicit in policy defaults. Psychological Science **17**(5), 414–420 (2006)
12. NetApplications.com: Operating System Market Share, https://www.netmarketshare.com/operating-system-market-share.aspx (Accessed: 21 December 2018)

13. Rieman, J., Franzke, M., Redmiles, D.: Usability evaluation with the cognitive walkthrough. In: Conference companion on Human factors in computing systems. pp. 387–388. ACM (1995)
14. Robins, N., Williams, P.A., Sansurooah, K.: An investigation into remnant data on USB storage devices sold in Australia creating alarming concerns. International Journal of Computers and Applications **39**(2), 79–90 (2017)
15. Spencer, R.: The streamlined cognitive walkthrough method, working around social constraints encountered in a software development company. In: Proceedings of the SIGCHI conference on Human Factors in Computing Systems. pp. 353–359. ACM (2000)
16. Storer, T., Glisson, W.B., Grispos, G.: Investigating information recovered from re-sold mobile devices. In: Privacy and Usability Methods Pow-wow (PUMP) Workshop. ACM, University of Abertay, Dundee. p. 2 (2010)
17. Valli, C., Jones, A.: A UK and Australian Study of Hard Disk Disposal (2005)