scripted

Volume 17, Issue 2, August 2020

Offering 'Home' Protection to Private Digital Storage Spaces

Jaap-Henk Hoepman and Bert-Jaap Koops***

DOI: 10.2966/scrip.170220.359

Abstract

The law classically provides strong protection to whatever is inside a home. That protection is lost now that our photo albums, notes and other documents have become digital and are increasingly stored in the cloud. Even if their owner never intended these documents to be shared, their copies in the cloud may be accessed by law enforcement, under possibly lower conditions than apply to home searches. In this paper, we study this problem from a theoretical perspective, asking whether it is possible to establish home-equivalent legal protection of those private digital storage spaces (smartphones, private cloud storage accounts) that most closely resemble the home as a storage environment for private things. In particular, we study whether it is possible, using technological design, to clearly separate digital storage spaces that are used privately versus storage spaces used to share data with others. We sketch a theoretical architecture for such a 'digital home' that most closely resembles the physical home in terms of the space that is the most personal storage environment for private files. The architecture guarantees the data are indeed only stored for private use, and can never be shared with others unless the device used for storage itself is shared. We subsequently argue

that the law should offer 'home' protection to data stored using this system, as an intermediate stepping-stone towards more comprehensive legal protection of cloud-stored data. Such protection is needed, since nowadays, not the home or the smartphone, but the smartphone/cloud ecosystem holds 'the privacies of life'.

Keywords
Spatial privacy; informational privacy; home; digital devices; cloud; privacy by design

* Associate Professor, Digital Security Group, Radboud University, Nijmegen, The Netherlands. Email: jhh@cs.ru.nl. Postal address: Erasmus building, room 19.08, iHub, Radboud University, PO box 9010, 6500GL Nijmegen, The Netherlands. Associate professor, IT Law group, Faculty of Law, University of Groningen, Groningen, The Netherlands.
** Professor of Regulation and Technology, Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, Tilburg, The Netherlands. Email: e.j.koops@tilburguniversity.edu.

The research for this Article was made possible by a grant from the Netherlands Organisation for Scientific Research (NWO), project number 453-14-004.

1 Introduction

The law classically provides strong protection to whatever is in a home, as opposed to what is outside it. Government intrusion into homes is only allowed under certain conditions, and in most countries the police need a warrant to search a home. Legal protection of the home includes typical information carriers such as photo albums, books, music carriers, diaries, and private administrative documents. Today, many of these items and documents are digitised, and they are increasingly stored on smartphones and in the cloud, rather than (or besides) in the home. Therewith, they lose the legal "home" protection, and may be accessed by law enforcement under lower conditions. The US third-party doctrine, which holds that people do not have a reasonable privacy expectation in data voluntarily shared with others, including cloud service providers,[1] most clearly illustrates how traditional physical spaces and newly developed digital spaces tend to be regulated differently, with differing levels of protection.[2]

However, the mere fact that technology enables (and strongly incentivizes) mobile and remote storage should not by itself lower legal protection. If people store documents in the cloud because they want to share them with others, this might be a reason for giving them less legal protection, since sharing things with others always carries some risk of further access by others. But if people store documents in the cloud purely as a functional equivalent of storing them at home, because this is the twenty-first-century technical reality, they should not have lower legal protection than if they keep documents at home. Similarly, if people store things on a smartphone or laptop in order to have them at hand to show to others, lower protection might be

---

1 On the third-party doctrine, see Orin Kerr, "The Case for the Third-Party Doctrine" (2009) 107 *Michigan Law Review* 561-601.

2 Cf. Bert-Jaap Koops, "Privacy Spaces" (2018) 121 *West Virginia Law Review* 611-665.

warranted, since they are then intentionally carrying the items outside of the traditional home environment; but if people store things on smartphones or laptops simply because that is where nowadays one's photos, music, diaries, or personal administration are kept, without intending to give others access to these files, they arguably should have a home-equivalent legal protection. As the US Supreme Court stated about modern cell-phones, "[w]ith all they contain and all they may reveal, they hold for many Americans 'the privacies of life'…. The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought."[3] The challenge posed by this argument is how to reliably establish the intention, or lack thereof, to share such files with others.

This raises the question whether, and if so, how, it is possible to extend the legal protection of the home to those private digital storage spaces (smartphones, laptops, private cloud storage accounts) that most closely resemble the home as the private storage environment of personal documents and files that are not as such shared with others outside the home. Such protection could be provided purely in legal terms, by a suitable legal definition of which parts of cyberspace would be protected in this sense. However, this is very hard to enforce in practice, since it is technically difficult to recognise whether files in the cloud are the functional equivalent of files stored at home, or rather of documents or folders shared with others through some social media application. Therefore, if the law would try and protect a home-equivalent part of cloud storage space, it will likely be necessary, or at least helpful, to back up such legal protection by technical mechanism(s) that enable delineating this virtual space, similar to walls, doors, and locks offering technical mechanisms to

[3] *Riley v California*, 134 S. Ct. 2473, p. 2495.

delineate a house and therewith help define the boundaries of a home in a legal sense.

In this paper, we aim to make a theoretical argument that a "digital home" can be defined that could claim the same kind of protection for citizens as their physical home, in the sense of the most personal storage environment for their private files. In particular, we aim to show how a system can be devised that enables users to store files on their personal digital devices[4] or in the cloud in a home-equivalent way, as a technical design that may assist law-makers in offering home-equivalent protection to people's "digital homes".

We construe this argument by analysing how in general the situation differs when data are no longer stored exclusively on a storage device located in someone's home, and then studying under which conditions data stored elsewhere "in the cloud" could be offered the same level of protection as data stored "at home".

In fact, we propose a theoretical architecture for a cloud storage system that guarantees the data stored on it are indeed only used privately, and can never be shared with others. Using hardware-based, so called "tamper-proof" techniques, we can ensure that the data can only be accessed through the device that initially submitted the data for storage in the cloud. As a result, anyone wishing to access that data needs to physically "visit" and hold the device in much the same way as someone wishing to access paper documents or other items in a home needs to physically visit and enter that home. We subsequently argue that data stored using this system should be offered "home" protection.

A simpler solution would be to just offer blanket protection to all data stored on a personal computing device. That approach suffers from various

---

[4] Such a storage medium could be the hard disk in a personal computer, the solid state drive in a laptop, or the permanent storage of a smartphone or laptop.

limitations however,[5] two of which are relevant here. First, protecting smartphones against warrantless searches does not address the protection of data stored in the cloud, resulting in possibly different levels of protection for smartphone-stored data and cloud-stored data. Second, blanket protection of data stored on devices does not distinguish between data stored for purely private purposes and data stored in a way that enables third-party access.

For these reasons, the envisioned solution to secure personal digital data storage may be a more appropriate analogy of traditional home protection afforded to documents and items kept at home. If such a system were in place, law-makers could (at least) stipulate that access to private digital storage spaces is given the same legal protection as accessing objects stored in a home. (They could, and probably should, also provide home-equivalent protection to data stored in other ways, if certain conditions are met. We are not claiming that the proposed architecture is a necessary condition for offering home-equivalent protection to digital storage space; we are rather arguing that it is a sufficient condition to do so.) Thus, we argue that by tying data to one particular physical device without the ability to share it, the device should still enjoy "home" protection when it is brought outside the home; and that consequently, if police arrest the person carrying such a device, they should only be able to investigate it under the same conditions as apply to home searches.

We would like to stress that the proposed architecture has limited use beyond supporting the theoretical argument advanced in this paper. For example, as by definition the data stored in the cloud is only accessible from one particular device, it becomes inaccessible as soon as the device is lost, becomes

---

[5] Cf. Bryce Newell and Bert-Jaap Koops, "From a Ride On Horseback To the Moon and Back: Comparative Limits On Police Searches Of Smartphones After Arrest" (2020) 72 *Hastings Law Journal* (forthcoming).

inaccessible or fails to operate. This makes the proposed architecture a poor solution if people value backups of their files that can be used to restore content on a different device. But the same applies to physical items people carry outside of the home, for example a cherished love letter, or a photo album they want to show to friends: these can also be lost or damaged. If people want backups of their (printed) photos or letters, they must make some effort to achieve this. In that respect, we want to stress that we are making a theoretical argument here that we find important in and by itself: the mere fact that people nowadays store personal items outside of their home, because of the affordances (and nudges) of contemporary technologies, does not imply that they should *therewith necessarily* lose the protection that the home—as a space strongly protected against government access—used to offer to these personal items. In other words, external and portable storage can be conceived in a way that is functionally equivalent to traditional home storage.

The remainder of this paper is organised as follows. We start with discussing the traditional concept of "home", how that is understood and how it is protected in legal terms, and how this protection of the home gets eroded given how digital data are stored in our digital age. In section 3 we then turn to a technical discussion of the different types of cloud storage, and to what extent they allow the files stored on them to be shared or not. Section 4 studies how this sharing of data can be limited, and offers an example of a truly private cloud storage architecture that ties the data stored in that cloud to one particular device. We finish with a discussion, in section 5, of the advantage of our envisioned digital "home" storage method and its accompanying legal "home" protection over existing legal approaches to protect such data.

2 Background

"Home" is, legally speaking, an abstract term designating a certain space in which typically the most personal part of private life is lived. It is a broad term: although it primarily covers modern-age dwelling houses, it can also cover other environments that shelter private life, such as mobile homes, tents, or sleeping parts of cars or boats. The precise scope of "home" differs per country, but almost all jurisdictions mention something like "home" in their constitutions as an especially protection-worthy space.[6] This constitutional protection implies high safeguards for intrusion into these private spaces; typically, law-enforcement officers need a court order or warrant to enter and search homes. In some jurisdictions, such as the US, a search warrant has a narrowly circumscribed scope, limited to certain spaces or objects within the home, while in others, such as the Netherlands and other Continental systems, search warrants can be more general and allow searching the entire home, but subjected to requirements of purpose limitation (looking for evidence of a particular crime), proportionality, and subsidiarity. In both types of jurisdictions, a search warrant of a home can cover physical artefacts such as photo albums, paper notes, books, and records, and it can also include computers and other data carriers within the home. Thus, data stored on digital storage spaces located inside a home benefit from the legal home protection, and can only be investigated if the high standards for home searches are met.[7]

---

[6] Bert-Jaap Koops et al., "A Typology of Privacy" (2017) 38(2) *University of Pennsylvania Journal of International Law* 483-575, pp. 514-516.

[7] This applies, at least, to investigations involving physically visiting the premises and physically accessing the computing device located there. Data stored on devices in the home can also be investigated by remotely accessing computing devices over data networks. Although the latter does not require (physically) entering the home with its associated high standards, jurisdictions that allow covert remote access by police often apply similarly high (and often even higher) standards for such access. Ivan Škorvánek et al., "My Computer Is My

The underlying assumption of the law is that the home should be the most strongly protected space because, traditionally, it shelters the most personal part of private life. However, this assumption is becoming obsolete since mobile and networking technologies enable storing a large part of personal life remotely in the cloud, or carrying it around on mobile phones. However, as soon as data leave the home, they also leave the legally protected sphere of home protection. To compensate for this loss of legal protection, jurisdictions are trying to define alternative bases of legal protection. A prominent approach is to consider computers as the new locus of private life – "my computer is my castle".[8] Germany has recognised a right to integrity and confidentiality of computers in the context of remote covert access,[9] while the United States have recognised that searching cell-phones seized after arrest is even more privacy-sensitive than searching homes and therefore requires a warrant.[10]

Useful though such new approaches are, they are not perfect solutions to the challenge of providing adequate legal protection to personal files stored outside the home in situations where the out-of-home storage is functionally equivalent to traditional in-home storage. One problem is that the protection of computers may be limited to certain types of investigation. The German constitutional right applies primarily to methods of covert remote access, but not necessarily also to investigations of devices seized when someone is arrested; and reversely, the US *Riley* warrant requirement applies to cell-phone searches in the context of an arrest, but not necessarily to covert remote access. More importantly, both approaches are focused on data stored on the protected device

---

Castle. New Privacy Frameworks to Regulate Police Hacking" *Brigham Young University Law Review* (forthcoming).

8 *Ibid*.

9 BVerfG, 1 BvR 370/07, Feb. 27, 2008.

10 *Riley*.

itself, disregarding remotely stored data. This is problematic, because many contemporary applications seamlessly move data between devices and the cloud – either to offer an automatic form of backup, or to offload less frequently used data from the device to free up space for new or more frequently used data –, and many users (and possibly police officers too) will not know whether data are actually stored on the device or remotely. If we want to provide home-equivalent protection to data storage (where the storage is functionally equivalent to traditional in-home storage), a more refined approach seems appropriate. Instead of designating particular devices, such as smartphones or computers, as a modern-day equivalent of a "home" for legal-protection purposes, and maintaining different regimes for accessing data on these devices and cloud-stored data, we explore whether it is possible to base legal protection on a clear, technically enforced, distinction between personally stored data and shared data, as modern-day equivalents to in-home and out-of-home data. Our exploration starts with looking at different types of cloud storage.

3 Existing types of cloud storage

When talking about cloud storage,[11] we typically distinguish the following entities:

- users, who have data they want to store remotely,
- the cloud provider, offering storage space to users on its servers, and
- the network interconnecting users' computers with storage servers.

There are, in principle, three forms of cloud storage:

---

[11] Seny Kamara and Kristin Lauter, "Cryptographic cloud storage" in Radu Sion et al. (eds.), *Financial Cryptography and Data Security. FC 2010. Lecture Notes in Computer Science, vol 6054* (Berlin, Heidelberg: Springer, 2010).

- *unencrypted* storage,
- *encrypted* storage, using a key chosen by the cloud provider, and
- *end-to-end* encrypted storage (also called zero-knowledge cloud storage), using a key chosen by the user storing the data.

3.1 Unencrypted storage

In the case of unencrypted storage, a user wishing to store data on the storage server sends these data to the server, which stores it unencrypted. Thus, the cloud provider has access to these data. External access to the storage server may be restricted using access control mechanisms enforced by the cloud provider or user. But users are free to share their access credentials (i.e. username and password) to other users at any point in time, thus allowing these others access to their data, at any time and from any location they please.

Setting up access credentials for others and distributing them can be done well in advance of any actual data sharing taking place. In fact, it can be done before any data to be shared exist. Consequently, it is difficult in this case to distinguish between personally-stored data and shared data by merely looking at how the data are stored, since it is not known how many people have access to the account and the stored data.[12]

3.2 Encrypted storage

The case of encrypted storage, using a key chosen by the cloud provider, works as follows. A user wishing to store data on the storage server sends these data to

[12] Depending on the way access credentials are shared, and depending on how users access the data they have been given access to, the service provider may be able to tell, by observing data accesses over time, which data items have been shared with others, and which data items have never been accessed by others and thus could be considered unshared, personally stored data. The point here, however, is that the service provider cannot tell this a priori.

the server. Typically, a secured, i.e. encrypted, communication link is used for this purpose. Vendors call this "encryption in transit". But whatever means of transport is used, the original, unencrypted, data are received by the cloud provider. These original, unencrypted, data are then encrypted against another cryptographic key chosen by the cloud provider. Vendors call this "encryption at rest". To later access these data, the user signs in to her account using her credentials, after which the cloud provider decrypts the data using the key it generated earlier, before sending the original data back to the user (again possibly using a secure communication link). Specific files or sections of the cloud storage can be shared with other user accounts on the cloud service.

Such encrypted cloud storage is essentially no different from unencrypted cloud storage: whoever knows the credentials of the user, has access to her data. Clearly, the cloud provider himself has access to these data as well. Most cloud providers (like Google Drive, Microsoft One Drive, Apple iCloud, or Dropbox) are of this type. Any cloud provider that somehow allows users to recover access to their data, even if they lost their password and/or lost all of their personal computers linked to the cloud account, are of this type.[13]

3.3 End-to-end encrypted storage

In an end-to-end encrypted cloud storage system the *user herself* generates and stores the cryptographic keys, which are subsequently used to encrypt the data on the user computer before the data are transmitted to the cloud provider and stored on its storage server. Unlike the previous case, the cloud provider does not perform any decryption or (re)encryption. And therefore, only the original

[13] This is called the Mud Puddle Test, available at https://blog.cryptographyengineering.com/2012/04/05/icloud-who-holds-key/ (accessed 22 July 2020).

user has access to the data, using the computer on which the necessary encryption keys are stored; others, including the cloud provider, have no access to the data (except if they have access to the user's computer and know the credentials to access the encryption keys stored therein, e.g. through the software used to access the cloud storage). This is very similar to the concept of *end-to-end encryption* used for secure messaging to ensure that even messaging service providers have no access to the messages exchanged over their platform. Only a limited number of cloud providers provide this service: Sync, TeamDrive, and SpiderOak are notable examples.

Typically, in the third type of encrypted storage, a so-called *hierarchy* of keys is used to encrypt the data. An illustrative setup works as follows. When a user creates an account with the cloud provider, she installs a piece of software that allows her to store and access data on the storage server, and that also manages the necessary cryptographic keys (and deals with data encryption and decryption). In particular, user master key k_M is generated. This key allows the user to access all her data. It is therefore highly important for the user to securely store it, in order to ensure that nobody else gets a copy (and hence access to all the data), but at the same time make sure that she has a backup of this key somewhere in case her device crashes, gets stolen or lost.

This master key is never used to encrypt data directly. Instead it is used to encrypt other keys that are then used to encrypt (and decrypt) data. For example, if a user wishes to store a folder with documents[14] in the cloud, the software first creates a folder key k_f and then creates document keys k_{d_i} for each document in the folder. Each document is then encrypted with its own key, and later updates to this document are also encrypted using this key; in other words, once a

[14] To distinguish the abbreviations of folder keys and file keys, we use 'document' here as a synonym for a (digital) file, which may have textual, visual, or audio content.

document is created, its key is typically never changed (unless the key is compromised). After that, each document key is encrypted using the folder key k_f, and the folder key is then encrypted with the user master key k_M. The encrypted documents and the encrypted document keys and folder keys are then sent to the cloud provider and stored on the server.

To access a document stored in the cloud, the user first needs to obtain the encrypted folder key and decrypt it with her master key k_M to obtain the folder key k_f. She then obtains the encrypted document key and uses the folder key to obtain the document key k_{d_i}. Finally, she obtains the encrypted document and uses the document key to decrypt the document and get access to its contents.

This rather complicated and lengthy discussion was necessary to expose that even cloud storage using end-to-end encryption allows users to share access to documents with others at any point in time: all that is required is to give other users the corresponding document key k_{d_i} as soon as the document is created; this allows others to access the contents of this document from that point onward. If someone wants to share all current *and future* documents in a folder with someone else, she can give them the corresponding folder key k_f. In fact, all well-known cloud providers offer this type of document or folder sharing.

Again we see that the keys needed to offer others access to some data can be created and distributed well in advance of any actual data sharing taking place, even when some or all of the data to be shared later do not yet exist. So also in this case, it is difficult to distinguish between privately stored data and shared data.

4 Limiting the possibilities for sharing data stored in the cloud

Can the type of end-to-end encrypted document or folder sharing discussed in

the previous section somehow be distinguished from remote storage purely for personal use? This is possible, if we hypothesise that personal-use storage is done through a device strongly linked to the user, such as a smartphone or laptop. The question then becomes: can we design a cloud storage system that guarantees that a document is *only* accessed using the same computer with which it was created?

Before discussing this further, it is worth stressing that this is not something users would like to do from a usability perspective: it implies, by definition, that if someone loses her computer, or if the computer stops working, she also irrevocably loses access to all documents stored in the cloud. This risk can be mitigated by creating a backup copy of all data stored in the cloud on another personal physical storage device (similar to making a copy of physical letters or photos – which you can leave safely at home – if you want to carry them with you outside). The advantage would be, however, that the data are strongly protected against third-party access: neither the service provider nor hackers or government officials can access the data by accessing the cloud server, except if they have access to the user's physical device itself. The system also extends the storage space available to the device with the (usually much larger) storage capacity offered by the cloud. This space can be used to offload less frequently used data, and can also be used to create automatic backups of data that allows these data to be recovered if they are accidently deleted on the device. And law-makers could attribute home-equivalent protection to documents stored in this way, by establishing similar conditions for law enforcement to access the user's device and the encryption keys stored therein as they do for entering and searching homes.

4.1 Example: disk encryption and copy protection

In a sense, the situation is quite similar to both disk encryption (with any type of

external storage, like a hard drive or a solid state drive)[15] and copy protection of digital content, like books, movies or music. In the first case, data on an encrypted disk should not be accessible from any other computer than the one in which the disk was originally installed, and even then only if that computer is powered-on and unlocked using the computer user's account. In the second case, a copy of some digital content that someone bought to access on one computer should not be playable or readable on another computer. Typically, such copy-protected digital content is also encrypted (against a device-specific key, usually hidden within the software used to access the content). In both cases, access to the data or the content is restricted to one particular computer.

The security of both disk encryption and copy protection dramatically increases when using an additional piece of tamperproof hardware that contains some essential piece of the puzzle (typically a cryptographic key) that is required to decrypt the contents of the disk or to unlock the piece of software. In the case of disk encryption this could be a *smart card* or some other tamper-proof device embedded in the computer (laptop, smartphone) that contains the disk. In the case of copy protection this could be a USB *dongle*. For digital broadcasting and satellite TV, set-top boxes with smart cards are also used. The reason for the improved security is that essential cryptographic operations are done within the smart card or dongle, which particularly guarantees that the cryptographic key never leaves the tamper-proof hardware component.[16]

4.2 Tamper-proof hardware

In situations where an additional layer of protection is deemed necessary, so-

---

[15] Cameron Laird, "Taking a Hard-Line Approach to Encryption" (2007) 40(3) *Computer* 13-15.

[16] As we will see below, smart cards and dongles cannot actually decrypt content on the fly. Instead, they contain and protect some master keys that are used to derive and release less sensitive and valuable temporary keys that are then used to actually decrypt the content itself.

called tamper-proof or tamper-resistant devices can be used to perform the most security-critical operations.[17] Such devices are independent pieces of hardware that contain

- some data to be protected (for example cryptographic keys),
- some execution logic (a program, some software) that allows the device to perform operations on or using that data, and
- an interface that allows authorised external agents to instruct the device to perform a certain operation (for example asking it to decrypt a document).

The device itself verifies whether an external agent is authorised to send such an instruction, typically using the secret data stored on it.

Tamper-proof devices are the digital equivalent of a safe. They make it practically impossible for attackers to obtain the secret data stored in the device, even if the attacker has physical access to the device, and even if the attacker has sophisticated equipment at his disposal. Examples of tamper-proof devices are smart cards, secure USB tokens, and hardware security modules (HSM). A SIM card used in mobile phones is a tamper-proof device, which securely stores the identity information and corresponding authentication keys used to set up a secure connection with the mobile network. Public-transport smart cards securely store the remaining credit on the card (and thus prevent the owners of the card to surreptitiously increase this balance for their own benefit). This latter example illustrates the general security principle implemented by tamper-proof devices: they enforce an external security policy (defined by the issuer of the

[17] Ross Anderson and Markus Kuhn, "Tamper Resistance: A Cautionary Note" (The Second USENIX Workshop on Electronic Commerce Proceedings, Oakland, California, November 18-21, 1996).

device) on the environment in which the device is subsequently used. In other words, they are useful when the environment is not trusted, and thus protect the data stored in the device against the environment in which the device is used. This "environment" can either be the owner or carrier of the device (in the case of a public-transport card) or some other device with which it cooperates or in which it is embedded (in the case of a SIM card inserted into a mobile phone).

4.3 An example of disk encryption

Now, let us look at disk encryption in a little more detail. Many modern computing devices (smartphones, laptops, PCs) already contain some form of tamper-proof hardware that provides a trusted execution environment that can be used to offer secure disk encryption (like Intel Trusted Execution technology and ARM TrustZone). In these cases, a separate smart card or dongle is not necessary. As a particular case, let us study how Apple's FileVault (its software-based disk encryption system) works on modern Macbooks that have the T2 Security Chip installed.[18]

FileVault encrypts the data on the disk using a form of symmetric encryption[19]. The T2 Security Chip contains a so-called Secure Enclave Processor and a cryptographic engine, which, given a symmetric key, encrypts or decrypts these data on the fly. This ensures that the key never leaves the security chip. The key used to encrypt the data on the disk is actually derived from two keys securely stored in the secure enclave:

---

[18] Apple, "Apple T2 Security Chip. Security Overview" (Apple.com, October 2018), available at https://www.apple.com/mac/docs/Apple_T2_Security_Chip_Overview.pdf (accessed 19 August 2019).

[19] Advanced Encryption Standard (AES) in XTS mode, to be precise.

- the Mac unique ID (UID), a 256-bit key fused into the secure enclave during manufacturing, and
- the Class Key, which in turn is derived from this UID and the user password.

The UID is unique and presumably securely and randomly assigned without any connection to some device serial number. The class key is presumably erased when a user logs out or when the device is powered off or put to sleep. Both keys never leave the secure enclave. Therefore, this way of deriving the actual decryption key from these two "master" keys ensures two things. First, the contents of the disk can never be decrypted on any other device, as this other device does not have access to the UID necessary to derive the decryption key. Second, the contents of the disk can never be decrypted without knowledge of the password, as this password is necessary to derive the Class Key.

4.4 Cloud storage approach

A similar approach could be used to ensure that data stored remotely in the cloud can only be encrypted and decrypted using one particular computer. That computer should either contain some tamper-proof hardware that provides a trusted execution environment, or require a smart card or USB dongle to be inserted before the data can be accessed. The tamper-proof hardware inside the computer, or the smart card or USB dongle inserted in the computer, must all guarantee that the master keys stored inside them never leave the hardware.

In the end, the data stored in the cloud are encrypted with some key derived from these master keys. This could be done in a similar fashion using a key hierarchy as described above for end-to-end encrypted cloud storage. As mentioned already there, this encryption/decryption key is static, i.e. it should not change, as any change of key requires all documents encrypted using the old

key to be re-encrypted using the new key to ensure that they can later be decrypted using this new key. This implies that this encryption/decryption key is highly valuable and offers long-term access to the data stored in the cloud.

To prevent the possibility of sharing this key with others (and thus to ensure that only personally stored data benefit from "home" protection), this key should preferably not leave the hardware, smart card or dongle. Otherwise, there is a risk that some specially designed software could intercept this key. Therefore, encryption and decryption should also take place within the hardware itself. This is certainly possible with hardware embedded within the computer itself, as Apple's disk encryption setup proves, but this is a lot harder using external hardware like smart cards or USB dongles. Especially smart cards have poor data transfer rates and are slow data processors. Moreover, using removable smart cards or USB dongles increases the options for the user to still share the data with others, by sending them the smart card or USB dongle (note, however, that this *also* makes the data immediately inaccessible to the user herself). In other words, a trusted execution environment physically embedded in the device (laptop, smartphone) is the preferred embodiment.

As noted before, this approach does prevent users to recover their data as soon as the device used to store the data crashes, malfunctions, or is lost or stolen. Moreover, the construction discussed above expressly prevents a user to sync her data with any other personal device. This makes it impossible to automatically share, for example, a digital photo album with one's smartphone and one's tablet (which, it may be noted, also applies to physical photo albums: one cannot easily "sync" the photo collection stored in the bedroom and that stored in the living room)[20].

[20] This situation could perhaps be mitigated if an additional access control step based on biometrics is implemented. Modern devices can be unlocked using a fingerprint or facial scan.

As an alternative approach to embedded hardware encryption/decryption, one could use strategies deployed in the context of copy protection that allow some specially designed software to decrypt the data using the decryption key while still shielding this key from obvious ways of interception. Such software-only-based obfuscation approaches (also known as whitebox cryptography)[21] are known to be weak, however: copy protection is typically circumvented by sufficiently skilled and determined attackers. On the other hand, the average person will lack the skills or the specific tools to easily obtain these decryption keys.

5 Discussion

We have shown that there are various theoretical possibilities to perform data storage in the cloud in a way that the remote storage is by and large a functional equivalent to personal data storage that traditionally took place inside the home, strongly protected against third-party access. The most robust possibility is a hardware-based solution that uses on-device encryption/decryption with a key stored in tamper-proof hardware embedded in the device. Here, access to data stored on the device itself and data stored with that device in the cloud is limited to the person having physical access to the device and knowledge of the credentials to access the keys.

If the biometrical template used to unlock a device can somehow be inextricably bound to the encryption and decryption keys to store and access the data, this would still ensure that the data can only be accessed if the same user that stored the data earlier (possibly on another device) now unlocks the device to access it. Binding encryption keys to biometrical data can be done in a secure fashion using so-called secure sketches and fuzzy extractors. Yevgeniy Dodis et al., "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data" (2008) 38(1) *SIAM Journal on Computing* 97-139.

[21] Bercht Wyseur, "White-Box Cryptography" in HCA van Tilborg and S Jajodia (eds.), *Encyclopedia of Cryptography and Security* (Boston, Springer 2011).

Such a system ensures that, similarly to documents stored in a traditional home environment, data stored in the digital "home" environment can be accessed by others, but only if they have physical access to the environment itself. Thus, the data can be shared by others if the user voluntarily hands over the device to another and opens up the key, similarly to opening the door to one's house to allow someone inside, so that they can have a look around and see the resident's music or photo collection. The data can also be accessed by law enforcement if they have access to the device and to the user's credentials, roughly similarly to police entering a home in order to search documents inside. (There is, however, a significant difference between accessing users' digital credentials and accessing door keys, which we discuss below.)

One difference with traditional home storage is that digital "home" storage is mobile: instead of leaving one's personal documents behind when leaving the protected environment of the home, users can and will normally carry the protected environment around with them, in the form of their personal computing device (smartphone, laptop). However, this need not affect the character of the secured digital storage space as a "home" environment. After all, traditional legal home protection also usually covers mobile homes. Moreover, one important characteristic of the home is that is shelters personal belongings, including souvenirs and mementos that are important for people's sense of self; the home traditionally is an especially safe environment for keeping objects associated with important life moments, such as photos and mementos.[22] Now that digitisation and networked technologies have facilitated mobile and remote storage of personal belongings, it makes sense to extend home protection to mobile storage devices that nowadays serve as the shelters of information objects

[22] Russel Belk, "Attachment to Possessions" in I Altman and SM Low (eds.), *Place Attachment* (New York/London: Plenum Press 1992).

central to one's personal life. As observed in the above-quoted *Riley* case, it is mobile phones that nowadays contain "the privacies of life".

The main advantage of our envisioned digital "home" storage method over existing legal approaches to computer protection, including the US *Riley* judgement that strongly protects data stored in smartphones, is that protection is afforded to data stored *with* the personal device regardless of whether they are stored *on* the device or stored remotely in the cloud. A blanket protection of all data stored on a personal computing device, which does not extend to data stored remotely through that device, is a poor proxy for home protection for two reasons.

First, it does not reflect the contemporary digital reality of seamless data flows between user devices and cloud storage. For users, it does not matter much (and it is also often not clear) whether, for instance, a smartphone-made photo is stored on the device itself or directly in the cloud, if they want to store it privately: they can access the photo in both cases in real-time. Consequently, legal protection should not differ substantially between the two forms of storage.

Second, blanket protection of data stored on devices does not distinguish between data stored for purely private purposes (as a contemporary equivalent of storing data in the home) and data stored in a way that enables third-party access (as a contemporary equivalent of bringing a photo album along when visiting a friend). As mentioned in the introduction, data shared with others arguably may have somewhat lower legal protection because the sharing of data involves some risk of (further) dissemination of the data. But storing data only with a service provider for purely personal purposes should not count as "sharing" with others in this sense: remote storage is a contemporary functional equivalent of home storage, enabled by the computer/cloud ecosystem, as long as the user does not give others access to these data.

For these reasons, the envisioned solution to secure personal digital storage spaces is a more appropriate analogy of traditional home protection afforded to documents kept at home. If such a system were in place, law-makers could stipulate that (at least[23]) access to private digital storage spaces is given the same legal protection as accessing objects stored in a home. Similarly to physical homes and documents stored therein, law enforcement would have no other way to access the data than through having physical access to the personal device. To be sure, this considerably limits law enforcement access to data – but that is actually the point of our argument. It limits law enforcement's options to access data stored in the cloud, but only to the extent that these data are stored remotely for purely personal purposes. Users can store data safely in the cloud, knowing that law enforcement (or other third parties) only can access them if they have physical access to their device; but they cannot do this with data they want to share with others, such as friends to see their photo collection. Hence, the restriction of law enforcement access to cloud-stored data only applies to the extent that the cloud is used as a contemporary equivalent of a safe storage place for one's personal documents, which traditionally was one of the typical functions of a home. This ensures that, if the cloud is used for sharing data with others, this does not as such block law enforcement's capacity to access those data without physical proximity to the personal computing device, similarly to the police potentially seizing a photo album that someone carries along on the street, outside the safety of home protection.

We think that the above-sketched system is an interesting way to recalibrate legal protection in an age with a radically different geography of data

[23] As observed above, we argue that using the proposed architecture would be a sufficient condition to merit 'home' protection, but not a necessary condition: also other forms of data storage could be attributed 'home' protection.

storage than the previous centuries in which home protection was the key pillar of privacy protection. We should, however, note four limitations.

First, we hypothesised that personal-use storage is done through a device closely linked to the user, such as a smartphone or laptop. This implies that if users have multiple personal devices (say, a smartphone, laptop, and tablet), they may have multiple digital "homes". This is not problematic: people can also have several physical homes (say, a dwelling house, a mobile home, and a countryside cottage). It also implies that if people temporarily lend their personal device to another, which may happen with laptops, these others temporarily occupy the digital home environment of the device owner. That is also not fundamentally different: people also often temporarily lend their home to others, e.g., through AirBNB rental.

Second, there is some difference between in-home document storage and private digital storage linked to personal devices. Physical homes, after all, are not only personal shelters but also family shelters, and family members in the same home may mutually access the objects stored therein. Only if things are locked away with a key not shared with household members, are objects stored in the home environment for purely personal purposes; this may be an exception rather than the rule. With the digital storage system sketched above, the exception becomes the rule, since household members will normally not have access to each other's personal computing devices (except if they share the credentials with them). To some extent, this affects the analogy we have drawn. With physical homes, jurisdictions may allow law enforcement to access a home and objects stored therein without a warrant, if they have a household member's consent. Such a situation would be more exceptional with legal protection connected to personal devices. But since it already is an exceptional situation – the default being that search warrants are needed to search a home – we think that this is not a fundamental objection to the analogy.

Third, one might wonder why anyone would choose to use the proposed private cloud storage architecture instead of any of the available end-to-end encrypted cloud storage solutions discussed in section 3.3. After all, the latter form of cloud storage prevents any unauthorised third party (including the cloud provider and any law enforcement agency) from obtaining direct access to the data stored in the cloud, while still allowing users to securely share documents and to recover data from the cloud for backup purposes. In other words: such an end-to-end encrypted cloud storage appears to have the same benefits, without any of the drawbacks of the architecture proposed. The answer is largely one of legislative argumentation. Our proposed architecture more closely resembles the way in which documents and items used to be stored in the home than end-to-end encrypted cloud storage, which does not have a clear equivalent in traditional, analogue data storage. For this reason, law-makers may hesitate to award "home" protection to cloud-stored data, if they argue that cloud storage – whether or not based on end-to-end encryption – merits lower privacy protection because the data might actually be shared with others, and because there is no easy way to distinguish between data stored in the cloud purely as a functional equivalent of in-home storage, and data stored in the cloud (also) to share with others. Lack of such "home" protection will often not make much difference, since the data are encrypted and therefore inaccessible anyway; but there is a significant difference in cases where law enforcement have access to the user credentials (for instance, when they found them written down on a note in a seized wallet, or when they seize a smartphone when it is open and cloud-connected). Our argument basically refutes a law-maker's argument that cloud-stored data are less protection-worthy because they are, or might be, shared data; it therewith provides a stronger incentive for law-makers to treat cloud-stored data as equally protection-worthy as home-stored data. To be sure, there are good reasons for law-makers to provide a high level of protection to cloud-stored

data in any case, and we are not arguing that cloud storage should only be strongly protected by law if people use the architecture sketched here. What we are arguing is that, with this architecture, law-makers can no longer withhold strong, home-equivalent protection from cloud-stored data based on an argument that storing data out-of-home lowers the reasonable expectation of privacy.

Fourth, the envisioned system requires not only physical access to the personal device through which data are stored; it also requires access to the credentials needed to use the relevant decryption keys, in particular the user's master key k_M to unlock the encrypted folder (and subsequently document) keys. This master key will be protected by the user with a password or biometrics. In case of biometric protection, law enforcement may – if they have physical access to both device and user – perhaps be able to access the key, for instance by putting the user's finger on a sensor, without violating the privilege against self-incrimination;[24] it may depend on jurisdictions whether they allow such breaking of biometric protection. But with password protection, obtaining the user credentials without the voluntary co-operation of the device user will often be impossible. In contrast to physical locks on doors and desks, which can if necessary be broken by brute force, digital locks may be impenetrable to brute force attacks; and forcing suspects to give passwords is highly contested in view of the privilege against self-incrimination. This implies that, if law enforcement have physical access to a user device and have a warrant to search the data stored with that device, they are dependent on voluntary collaboration (which is unlikely if it concerns suspects) or on alternative means to acquire the user's

[24] Cf. Ingvild Bruce, "Forced biometric authentication – on a recent amendment in the Norwegian Code of Criminal Procedure" (2017) 14 *Digital Evidence and Electronic Signature Law Review* 26-30.

credentials. For the latter, powers to covertly hack into computers may perhaps be useful, but this requires time and effort and will not be possible at the scale on which house searches, or searches of devices seized incident to arrest, typically occur.

In this sense, protection of data in private storage spaces seems higher than protection of data traditionally stored in the home. This is not as much a consequence of the above-sketched system, but rather a consequence of digital devices themselves. The same, after all, applies to smartphone and computer searches in general. However, one consequence of the envisioned system is that, for those data that are stored remotely for purely personal purposes, these would no longer be accessible through alternative means, such as a production order to cloud providers. But if cloud storage happens with end-to-end (user) encryption, as is increasingly common, the alternative means to access cloud-stored data are limited anyway. More importantly, even if the above-sketched system would limit law enforcement access to data stored through personal devices to some extent, this is arguably warranted by the heightened privacy risk associated with personal computing devices that store "the privacies of life". As the US Supreme Court recognised in *Riley*, "a cell phone search would typically expose to the government far more than the most exhaustive search of a house".[25] From this perspective, strong protection of digital files stored for purely personal purposes on and with one's personal device is warranted, to update legal protection in an age where the place of storage no longer really matters.

To conclude, let us reiterate that in this paper, we aimed to make a theoretical argument that it is possible to design a "digital home" for storing digital data in a way that most closely resembles how physically stored

[25] *Riley*.

information (such as photos and diaries) used to be stored in the physical home. We do not think that users are craving for such an architecture; nor are we making a normative claim that such an architecture should be implemented. Rather, we have tried to demonstrate that, with some changes to the increasingly common end-to-end encrypted cloud storage architecture, the out-of-home storage of data in today's smartphone/cloud ecosystem can be designed to closely resemble traditional in-home storage of personal belongings. Therewith, so we have argued, there is no valid reason to treat such out-of-home-stored data differently from data stored in-home, in terms of legal protection.

There are good reasons nowadays to offer home-equivalent protection to cloud-stored data in the first place, regardless of the precise storage architecture. After all, it is not so much, as the *Riley* court held, that *smartphones* hold the privacies of life; rather, it is the *smartphone/cloud amalgam* that holds the privacies of life. However, most jurisdictions are not noticeably doing much to pass laws that strongly protect cloud-stored data. One reason for this may be that the smartphone/cloud amalgam is too different from what law-makers know, so that the analogy between homes and digital storage spaces may not be sufficiently compelling when conceiving of legal protection. Possibly, the step from home protection to home-equivalent cloud storage protection is too large, for law-makers who may think of the cloud as a space for sharing rather than for safely storing one's personal belongings. In that case, the architecture we outlined in this paper may serve as an intermediate stepping-stone towards more comprehensive protection of cloud-stored data, as this architecture offers a digital storage space that more clearly functions as the most personal storage environment for private files and that can therefore claim the same kind of protection for citizens as their physical home environment.

We realise the limitations of the sketched architecture, including challenges to practical implementation and usability. We certainly welcome

alternative suggestions that could provide equally strong arguments for offering home-equivalent protection to data stored in the cloud and that may be more realistic to implement. Absent such alternatives, we offer the sketched architecture as a suboptimal solution, to salvage at least something of the quickly eroding level of protection that the law actually achieves in protecting photos, diaries, and other personal belongings that used to be stored in the safety and sanctity of the home, but that nowadays are stored in other spaces. Something, at least, needs to be done. Because, in our opinion, the twenty-first century equivalent of "my home is my castle" may not so much be "my computer is my castle" or "my smartphone is my castle", but rather "my castle is wherever my privately stored data are".