Shining a Light:

Shadow IT and Data Protection in the Humanitarian Sector

A profile of Skype and Dropbox

By Siobhan Talty

October 2019

Abstract

Focus on new technology products must not outshine a robust analysis of the risks related to embedded, routine technology used in humanitarian workplaces. This paper profiles two common platforms (Skype and Dropbox) against a framework of data protection principles applicable to the humanitarian sector and in the context of their shadow IT – or non-IT authorized – usage. The research finds that while such technology itself may not inherently breach data protection principles, the unmanaged, shadow IT application of technology may. The paper concludes that to meet data protection obligations, the humanitarian sector must begin to proactively manage shadow IT.

Key words: Shadow IT; Humanitarian; Data Protection; Skype; Dropbox; Microsoft; Risk

Contents

Introduction

In 1919, Belgium officially introduced an identity card, with which to register all permanent residents over fifteen years old, recording data such as full name, marital status, nationality, date of birth, occupation and previous residence.[1] For those working in the humanitarian sector, this is a familiar list; humanitarian work also requires people be identified. Similar data fields are processed by humanitarian organisations to create distribution lists, participant lists, or survey sampling frames. The information is necessary for allocating aid, reporting to donors, or monitoring performance. Given this familiarity, it might be uncomfortable for a humanitarian worker to learn the historical uses of these identity cards. Van Brakel and Van Kerckhoven explain Belgium's population registration started in 1792 under French occupation, was regulated following independence to support population registers and censuses, then postal service transactions and evolving into cards introduced by German occupiers in World War One to increase German control over the Belgian population.[2] Cards that in World War Two, had a stamp added to identify cardholders as "*Juif*" (Jew) or "*verplicht weggevoerde*" (requiring deportation). Cards that Belgium then exported to its colonies, including colonial-era Rwanda, where they included a data field for "ethnicity", a categorisation that has been linked to the singling out of Tutsi victims in the 1994 genocide. [3]

[1] Rosamunde Van Brakel and Xavier Van Kerckhoven, "The Emergence of the Identity Card in Belgium and its Colonies," in Kees Boersma, et al. (eds), *Histories of State Surveillance in Europe and Beyond*, Routledge, 2014, p. 3.

[2] *Ibid*, pp. 2-3.

[3] See *Ibid*.; Jim Fussell, "Group Classification on National ID Cards as a Factor in Genocide and Ethnic Cleansing," *Seminar Series of the Yale University Genocide Studies Programme*, New Haven, 2001; Timothy Longman, "Identity Cards, Ethnic Self-Perception, and Genocide in Rwanda," in Jane Caplan and John Torpey (eds), *Documenting Individual Identity*, Princeton University Press, 2001; Zara Rahman, "Dangerous Data: The Role of Data Collection in Genocides," *The Engine Room*, 21 November 2016, available at: https://www.theengineroom.org/dangerous-data-the-role-of-data-collection-in-genocides/ (all internet references were accessed in October 2019).

This is not the only example of the problematic legacies of identification registration systems;[4] many nations have seen government population policies facilitated by group classification on identification cards, including policies of genocide (Nazi Germany, Rwanda), mass expulsion (Ethiopia, Bhutan, Vietnam, France), forced relocation (USSR) and group denationalisation (Cambodia, Myanmar, Syria).[5] Identity cards may not be intended to explicitly sort or control certain groups but their existence opens the door to control and abuse,[6] as could the existence of identity datasets used for humanitarian purposes.

Given the risk to populations this example demonstrates, one would think humanitarian data is subject to strict data protection controls. Unfortunately, this is not quite the case; in fact, instances of high-risk data practices abound. The Australian Red Cross experienced a data breach resulting in 550,000 blood donors' personal details being accessed by an unauthorized person.[7] Concerns were voiced over the limited safeguards in place when collecting the biometric data of persecuted Rohingya populations.[8] The World Food Programme's web-based SCOPE system has been exposed as unreliable and their data handling practices poor.[9] The Red Rose platform for program participant data was breached, resulting in multiple non-

[4] See Gus Hosein and Carly Nyst, *Aiding Surveillance*, Privacy International, 2013; and Z. Rahman, above note 3.

[5] J. Fussell, above note 3, p. 6.

[6] R. Van Brakel and X. Van Kerckhoven, above note 1, p. 12.

[7] Melissa Davey, "Red Cross Blood Service Data Breach: Personal Details of 550,000 Blood Donors Leaked " *The Guardian*, 28 October 2016, available at: https://www.theguardian.com/australia-news/2016/oct/28/personal-details-of-550000-red-cross-blood-donors-leaked-in-data-breach.

[8] Zara Rahman, "Irresponsible data? The Risks of Registering the Rohingya," *The New Humanitarian (formerly IRIN)*, 23 October 2017, available at: https://www.irinnews.org/opinion/2017/10/23/irresponsible-data-risks-registering-rohingya.

[9] Ben Parker, "Audit Exposes UN Food Agency's Poor Data-Handling," *The New Humanitarian (formerly IRIN)*, 18 January 2018, available at: http://www.irinnews.org/news/2018/01/18/exclusive-audit-exposes-un-food-agency-s-poor-data-handling.

government organisations putting programs on hold to review systems[10] and a call for an independent investigatory body.[11] An Ebola patient's name was leaked to the Spanish media, resulting in public vilification and stigmatisation.[12] Questionable ethics and unmanaged risks have been linked to biometrics projects, Ebola data modelling and cargo drones.[13] This all comes in an environment where humanitarian organisations are collecting an increasing array of detailed and intimate data about crisis-affected populations, while operating in parallel with security and control measures.[14] There is no need to imagine what may happen if this data is abused; history has demonstrated the consequences are serious.

[10] Ben Parker, "Security Lapses at Aid Agency Leave Beneficiary Data at Risk," *The New Humanitarian (formerly IRIN)*, 27 November 2017, available at: http://www.irinnews.org/investigations/2017/11/27/security-lapses-aid-agency-leave-beneficiary-data-risk.

[11] Nathaniel A. Raymond, Daniel P. Scarnecchia and Stuart R. Campo, "Humanitarian Data Breaches: The Real Scandal is Our Collective Inaction," *The New Humanitarian (formerly IRIN)*, 8 December 2017, available at: http://www.irinnews.org/opinion/2017/12/08/humanitarian-data-breaches-real-scandal-our-collective-inaction.

[12] Miguel Ángel Royo-Bordonada and Fernando J. García López, "Ethical Considerations Surrounding the Response to Ebola: The Spanish Experience," *BMC Medical Ethics*, vol. 17, n. 1, 2016.

[13] Kristin Bergtora Sandvik, Katja Lindskov Jacobsen and Sean Martin McDonald, "Do No Harm: A Taxonomy of the Challenges of Humanitarian Experimentation," *International Review of the Red Cross*, vol. 99, n. 904, 2017.

[14] Sophia Hoffmann, "Humanitarian Security in Jordan's Azraq Camp," *Security Dialogue*, vol. 48, n. 2, 2017.

Many of these examples relate to the use of technology to process data. Yet, there is limited documented policy, protocol and analysis of the risks related to technologies introduced in humanitarian work. There have been many calls by experts to address this gap, to reduce risk to target populations.[15] There are varying levels of cybersecurity among humanitarian agencies, including a lack of robust guidelines, inadequate policies and insufficient training contributing to risk.[16] Added to this are human resources' deficiencies, such as staff failure to recognize and respect private data[17] and the need for more investment in training for areas including data collection, ethics, security and data protection.[18] Recent publications such as

[15] See Jennifer Chan, Lauren Bateman and Gisli Olafsson, "A People & Purpose Approach to Humanitarian Data Information Security and Privacy," *Procedia Engineering,* vol. 159, 2016; Charles Martin-Shields, "The Technologist's Dilemma Ethical Challenges of Using Crowdsourcing Technology in Conflict and Disaster-Affected Regions," *Georgetown Journal of International Affairs,* vol. 14, n. 2, 2013; Felicity Gerry QC, Julia Muraszkiewicz and Niovi Vavoula, "The Role of Technology in the Fight Against Human Trafficking: Reflections on Privacy and Data Protection Concerns," *Computer Law & Security Review,* vol. 32, n. 2, 2016; Patrick Meier, "New Information Technologies and their Impact on the Humanitarian Sector," *International Review of the Red Cross,* vol. 93, n. 884, 2011; Kristin Bergtora Sandvik, et al., "Humanitarian Technology: A Critical Research Agenda," *International Review of the Red Cross,* vol. 96, n. 893, 2014; and Catherine M. Tansey, et al., "Familiar Ethical Issues Amplified: How Members of Research Ethics Committees Describe Ethical Distinctions Between Disaster and Non-Disaster Research," *BMC Medical Ethics,* vol. 18, n. 1, 2017.

[16] Kristin Bergtora Sandvik, "The Humanitarian Cyberspace: Shrinking Space or an Expanding Frontier?," *Third World Quarterly,* vol. 37, n. 1, 2016.

[17] L. Butt, "Can You Keep a Secret? Pretences of Confidentiality in HIV/AIDS Counseling and Treatment in Eastern Indonesia," *Medical Anthropology: Cross Cultural Studies in Health and Illness,* vol. 30, n. 3, 2011.

[18] See F. Gerry QC, J. Muraszkiewicz and N. Vavoula, above note 15; C. Martin-Shields, above note 15; P. Meier, above note 15; and C. Tansey et al., above note 15.

the *Signal Code*,[19] or the *Handbook on Data Protection in Humanitarian Action*,[20] attempt to fill this gap and are part of a growing body of literature that draws attention to these risks.[21]

This paper aims to contribute to this literature, by analysing and documenting an area of technology usage called shadow IT, in the context of its potential consequences for the humanitarian sector's data protection efforts. Presently, literature on risks focus primarily on humanitarian innovation and experimentation; this paper will take a step back to look at the more routine or ordinary instances of technology in humanitarian workplaces. It presents four sections. The first section introduces the concept of shadow IT and establishes its linkage to humanitarian workplaces. The second section establishes a framework for analysis, outlining the data protection standards applicable to the humanitarian sector. The third section

[19] Farine Greenwood, et al., *The Signal Code: A Human Rights Approach to Information During Crisis*, Harvard Humanitarian Initiative and Signal Program, Cambridge, 2016.

[20] Christopher Kuner and Massimo Marelli (eds), *Handbook on Data Protection in Humanitarian Action* Brussels Privacy Hub and the International Committee of the Red Cross, Geneva, 2017.

[21] See Mark Duffield, "The Resilience of the Ruins: Towards a Critique of Digital Humanitarianism," *Resilience,* vol. 4, n. 3, 2016; Ben Hayes, "Migration and Data Protection: Doing No Harm in an Age of Mass Displacement, Mass Surveillance and "Big Data"," *International Review of the Red Cross,* vol. 99, n. 904, 2017; G. Hosein and C. Nyst, above note 4; Katja Lindskov Jacobsen, "Making Design Safe for Citizens: A Hidden History of Humanitarian Experimentation," *Citizenship Studies,* vol. 14, n. 1, 2010; Katja Lindskov Jacobsen, "Humanitarian Technology," *The Politics of Humanitarian Technology: Good Intentions, Unintended Consequences and Insecurity,* Routledge, 2015; Katja Lindskov Jacobsen, "Experimentation in Humanitarian Locations: UNHCR and Biometric Registration of Afghan Refugees," *Security Dialogue,* vol. 46, n. 2, 2015; Anja Kaspersen and Charlotte Lindsey-Curtet, "The Digital Transformation of the Humanitarian Sector," *International Committee of the Red Cross,* 5 December 2016, available at: http://blogs.icrc.org/law-and-policy/2016/12/05/digital-transformation-humanitarian-sector/; C. Martin-Shields, above note 15; Sean Martin McDonald, *Ebola: A Big Data Disaster - Privacy, Property, and the Law of Disaster Experimentation,* Centre for Internet and Society, Bengaluru and Delhi, India, 2016; K.B Sandvik, K.L Jacobsen and S.M McDonald, above note 13; K.B Sandvik, et al., above note 15.

examines the features and functionality of two common workplace software products, Skype and Dropbox, in the context of their shadow IT usage. The fourth section brings these three elements together, assessing the shadow IT use of Skype and Dropbox against the data protection principles applicable to humanitarian work. The paper concludes with recommendations to address the risk of shadow IT in the humanitarian sector, to pave a way towards better data protection practices.

What is shadow IT?

Shadow IT is the implementation of user-driven IT solutions without the formal approval of workplace IT administrators.[22] Shadow IT is often introduced with the best of intentions, or with a genuine absence of knowledge of the associated risks;[23] risks that increase the more embedded the technology becomes into work practices.[24]

While there is no quantifiable data on the prevalence of shadow IT in the humanitarian sector, consider the ease at which non-IT humanitarian workers can adopt shadow IT solutions, with its simplicity, low cost and availability. Consider how a group messaging app can easily convey information between coordinating cluster partners. Do staff know if the chosen app is encrypted and protects the information shared from being accessed by malicious actors – perhaps a party to a conflict wanting to know personnel locations? Consider personal email addresses used by new or short-term staff. Are the data protection policies of the third-party email provider understood; could the provider be duplicating the emailed content, which may list the addresses and asset values of a cyclone-affected community? Consider a humanitarian agency’s office space destroyed in an earthquake and staff using personal computers until new assets can be procured. Do the personal computers have IT-supported software installed,

[22] For a deeper understanding, see Andreas Antonius Béla Györy, et al., "Exploring The Shadows: IT Governance Approaches To User-Driven Innovation", *20th European Conference on Information Systems (ECIS) 2012*, Paper, Association for Information Systems, Barcelona, Spain 2012; and Mario Silic and Andrea Back, "Shadow IT – A View from Behind the Curtain," *Computers & Security*, vol. 45, 2014.

[23] See Max Metzger, "The Inside Man: Decoding the Threat from Within," *SC Magazine: For IT Security Professionals (UK Edition)*, 2016; and M. Silic and A. Back, above note 22.

[24] Daniel Fürstenau and Hannes Rothe, "Shadow IT Systems: Discerning the Good and the Evil," *Twenty Second European Conference on Information Systems*, Tel Aviv, Israel, 2014.

regular backups, or an antivirus program to protect data records? The opportunity for shadow IT clearly exists in the humanitarian working environment.

Skype and Dropbox offer free account options and are simple to operate, which makes them ripe for shadow IT installation. Therefore, Skype and Dropbox have been chosen as subjects for this analysis, to examine how shadow IT may impact humanitarian organisations' data protection considerations.

Framework for analysis

The data protection standards used as this paper's framework for analysis are from the *Handbook on Data Protection in Humanitarian Action* (henceforth "the Handbook"), published by the Brussels Privacy Hub and the International Committee of the Red Cross, in June 2017. The Handbook's purpose is to raise awareness of data protection standards and guide humanitarian organisations to interpret data protection principles in the context of humanitarian action. [25] The Handbook draws on international instruments and existing guidelines, thus provides a robust framework with which to examine the implications of the shadow IT use of Skype and Dropbox in the humanitarian sector.

Basic concepts in data protection

A few basic terms will be defined to understand exactly what data and what elements of data management require special consideration when using technology in humanitarian work. The Handbook defines personal data as ". . . any information relating to an identified or identifiable natural person."[26] This might include names, personal identification numbers (for example, identity papers), addresses, telephone numbers, personal characteristics, information identifying assets or property, and more.[27] In humanitarian work, such data fields are present in core documents such as distribution registration lists, community surveys, or activity participation lists. The Handbook makes an additional point regarding humanitarian contexts, stating ". . . data can cause severe harm even when the data cannot be considered

[25] C. Kuner and M. Marelli (eds), above note 20, p. 15.

[26] *Ibid*. p. 20

[27] US Department of Commerce, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, by Erika McCallister, Timothy Grance and Karen A Scarfone, National Institute of Standards and Technology, 2010, p. 2-2.

Personal Data."[28] The Handbook cites an example of aerial imagery showing populations fleeing violence that could be used by armed groups for reprisals. Thus, organisations must also consider protecting aggregated population or location data, where people may not be individually identifiable, but identifiable as a community or group. This has implications for the management of documents such as situation reports, donor reports, maps, photographs, or even funding proposals.

"Processing" is what organisations do with data and processing must be limited to protect data subjects' rights. The Handbook defines processing as:

> [A]ny operation or set of operations which is performed upon Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination, or erasure.[29]

Organisations may also process data for purposes other than those initially specified ("further processing"), but this further processing must be compatible with the initial purposes.[30] Linked to these concepts are two key roles[31] in data management: the Data Controller is "the person or organisation who alone or jointly with others determines the purposes and means of the Processing of Personal Data"[32] and the Data Processor is ". . . the person or organisation who processes Personal Data on behalf of the Data Controller."[33] Thus, if a software such as Skype or Dropbox is used for data processing by a humanitarian organisation, the software company plays a role in data management and becomes part of the data protection considerations.

[28] C. Kuner and M. Marelli (eds), above note 20, p. 23.

[29] *Ibid* p. 22.

[30] *Ibid*. p. 29.

[31] Correctly identifying the roles of Controller and Processor are important and can have legal implications, particularly in European Union jurisdictions. This paper, like the Handbook, will not delve into the specifics of applying data protection laws in specific jurisdictions.

[32] C. Kuner and M. Marelli (eds), above note 20, p. 23.

[33] *Ibid*. p. 23.

Principles of data protection

The principle of fairness and lawfulness of processing requires that personal data must be processed fairly – that is, in a manner transparent to the data subject – and lawfully, under a valid legal basis.[34] Fairness requires that data subjects receive transparent information about the purpose of the processing of their personal information and, when using the legal basis of consent,[35] data subjects must receive information on the risks and benefits of this processing.[36] Thus, providing this information accurately requires advance knowledge of what software and processing actions will be applied to the data.

The principle of purpose limitation requires that the purposes for data processing are explicit and legitimate, including any further processing that might take place beyond the initial purpose.[37] For example, the initial purpose of collecting patient data may be to provide medical assistance and further processing may calculate morbidity prevalence or incidence. Processing beyond these articulated purposes would breach the principle of purpose limitation.

The principle of proportionality "requires consideration of whether a particular action or measure relating to the Processing of Personal Data is appropriate to its pursued aim".[38] Points to consider are that the data are "adequate, relevant and not excessive", that the data are "necessary to achieve the purpose" (and that this purpose is determined in advance); and that the period the data are stored before being deleted or anonymized is minimized.[39]

The principle of data minimization seeks to limit the processing of personal data to the minimum amount and extent necessary.[40] This includes deleting data when it is no longer necessary according to the purpose of the initial data collection, when data is no longer compatible for further processing, when data subjects have withdrawn their consent and when data subjects justifiably object to the data processing. Circumstances must be considered

[34] *Ibid*. p. 25.

[35] *Ibid*. Refer to Chapter Three of the Handbook for more information on legal bases.

[36] *Ibid*. p. 36.

[37] *Ibid*. p. 26.

[38] *Ibid*. p. 26.

[39] *Ibid*. p. 26.

[40] *Ibid*. p. 27.

however, in which data may need to be kept for legitimate historical, statistical or scientific purposes.

The principle of data quality requires organisations ensure data is as accurate and up to date as possible, including deleting or correcting inaccurate data without undue delay.[41] As with the principles of proportionality and minimization, this requires diligence in data retention and deletion, including version control.

In addition to these principles, the Handbook makes note of several other general considerations, two of which will be considered in this paper. Data retention requires data is retained only for a predefined period.[42] Data security and processing security refers to technical and organisational protections, such as physical equipment security, IT security, or staff access policies.[43]

Thus, the Handbook provides a framework which humanitarians can utilize when adopting technology; the features and functionality of the technology can be investigated and considered against the Handbook's principles to determine whether using the technology complies with data protection standards.

Summary of technology features and functionality

The following section will summarize the features and functionality of Skype and Dropbox, based on the software versions, terms of service and privacy policies available in October 2019. Future readings of this paper should take into account potential changes made by Skype and Dropbox beyond this date.

[41] *Ibid*. p. 28.

[42] *Ibid*. p. 31.

[43] *Ibid*. pp. 31-35.

Skype

Features and data processing

The Microsoft-owned Skype service facilitates internet-based communication using voice, video and instant message (IM) for group or one-on-one communications, with features including file transfer, translation and location sharing.[44] Humanitarian workers often coordinate with colleagues in multiple geographic areas, therefore the free[45] Skype-to-Skype voice and video calls may be useful for anything from interviewing job candidates to holding team meetings. While the quality of Skype calls at times may be variable, including issues such as dropped calls, delays, or poor-quality video or audio, particularly in areas of poor network connection,[46] its low cost and ease of installation make it a likely shadow IT installation in a humanitarian workplace.

Shadow IT use of personal Skype accounts in the workplace does not breach the *Microsoft Services Agreement*, which explains Skype is for personal and non-commercial use, and permits the ". . . use [of] Skype at work for your own business communications."[47] Microsoft does not guarantee services will be "uninterrupted, timely, secure, or error-free or that content loss won't occur".[48]

Skype facilitates IM conversations, both user-to-user or in a group chat. IM text syncs across all of a user's devices and is stored on Microsoft servers, with storage dating back to April

[44] Microsoft purchased Skype in 2011 and the privacy policy and terms of service applicable to Skype apply to the suite of Microsoft products as a whole. Thus, any references to policy in this paper will use the term "Microsoft" and references to the product itself will use the term "Skype".

[45] Skype does offer paid business solutions, however it is the free, basic account type that will be considered in this paper, because this is the account type an individual humanitarian worker is most likely to install without IT support.

[46] "Troubleshooting Issues with Skype Call Quality," *Microsoft*, n.d, available at: https://support.skype.com/en/faq/FA12097/troubleshooting-issues-with-skype-call-quality?q=skype+call+quality.

[47] "Microsoft Services Agreement," *Microsoft*, 1 July 2019, available at: https://www.microsoft.com/en-us/servicesagreement.

[48] *Ibid.*

2017, or until the user chooses to delete the IM.[49] The IM can only be deleted by the sender of the IM.[50] Files and IM chat history can be exported by submitting a request to Skype.[51] Historically, Microsoft has changed its IM storage policy and IM storage location with changing versions of Skype software, for example, a previous version of Skype stored IM text locally on users' hard drives, with users specifying the retention period.[52] If users choose to export their history to the current version of Skype, this places a local copy on their device.[53] Skype also offers the option of a private IM (and private calls), user-to-user only. A private conversation is end-to-end encrypted, which means third parties including Microsoft cannot see the content being shared.[54] IMs sent outside of a private conversation are not end-to-end encrypted,[55] which means content can be seen by Microsoft.

[49] See "Can I Sync My Skype Instant Messages Across Devices?," *Microsoft*, n.d, available at: https://support.skype.com/en/faq/FA12368/can-i-sync-my-skype-instant-messages-across-devices?q=offline+access+to+messages; and "How Long are Files and Data Available in Skype?," *Microsoft*, n.d, available at: https://support.skype.com/en/faq/FA34893/how-long-are-files-and-data-available-in-skype.

[50] "How Do I Remove an Instant Message or Delete a Chat in Skype?," *Microsoft*, n.d, available at: https://support.skype.com/en/faq/FA34636/how-do-i-remove-an-instant-message-or-delete-a-chat-in-skype.

[51] "How do I Export my Skype Files and Chat History?," *Microsoft*, n.d, available at: https://support.skype.com/en/faq/FA34894/how-do-i-export-my-skype-files-and-chat-history.

[52] Martin Brinkmann, "Clear the Skype Instant Messaging History," *ghacks.net*, 21 November 2012, available at: https://www.ghacks.net/2012/11/21/clear-the-skype-instant-messaging-history/.

[53] "Getting to Know Version 8 and Above Skype for Desktop," *Microsoft*, n.d, available at: https://support.skype.com/en/faq/FA34850/getting-to-know-version-8-and-above-skype-for-desktop?q=how+long+is+data+stored.

[54] *Skype Private Conversation: Technical White Paper*, Microsoft, 2018, p. 2.

[55] "Does Skype Use Encryption?," *Microsoft*, n.d, available at: https://support.skype.com/en/faq/FA31/does-skype-use-encryption?q=encryption.

Skype transmits any type of file, up to 300 MB, between users; files are synced across all devices and storage time depends on the type of file.[56] Files, recordings, voicemails and videos over 100MB are stored by Skype for up to thirty days and videos under 100MB and pictures will be stored by Skype until they are deleted by the user or dating back to April 2017.[57] Once a voicemail is listened to, it is stored unencrypted on the user's local machine.[58] Sent files can be automatically or manually downloaded to a chosen folder on a user's hard drive, depending on the user's preferences.[59] This feature also works in private conversations; the files are sent using end-to-end encryption and can be automatically or manually downloaded for unencrypted storage on the user's local machine.

Information on retention periods and data storage is all sourced from Skype's online support articles; the *Microsoft Privacy Statement* does not articulate these specifics. This document explains Microsoft stores personal data "as long as necessary", with actual retention periods that may "vary significantly" depending on the context of the users' interactions with the products.[60] Forensic analysis of user devices show personal data from Skype can be recovered. In 2015, researchers uncovered potentially identifying plain text Skype artefacts on user devices[61] and, in 2013, forensic investigation of Skype on Android devices revealed

[56] "Skype File Sharing: File Types, Size, and Time Limits," *Microsoft*, n.d, available at: https://support.skype.com/en/faq/FA34644/skype-file-sharing-file-types-size-and-time-limits?.

[57] "How Long are Files and Data Available in Skype?," above note 51.

[58] "Does Skype Use Encryption?," above note 57.

[59] "How Do I Automatically Download Incoming Photos or Files in Skype on Desktop?," *Microsoft*, n.d, available at: https://support.skype.com/en/faq/FA34883/how-do-i-automatically-download-incoming-photos-or-files-in-skype-on-desktop?q=file+automatic+download.

[60] "Microsoft Privacy Statement," September 2019, available at: https://privacy.microsoft.com/en-us/privacystatement.

[61] Asma Majeed, et al., "Forensic Analysis of Three Social Media Apps in Windows 10," *High-Capacity Optical Networks and Enabling/Emerging Technologies (HONET), 2015 12th International Conference on*, Islamabad, Pakistan, IEEE, 2015.

call and IM evidence in the device, even after deleting histories and signing out of the Skype account.[62]

Some versions of Skype have the ability to record audio and video. Using this feature will store the recording in the conversation history with the person or group, with the onus for gaining consent for recording call participants placed on the initiating user.[63] The recording will have a visual output (MP4 file), even in audio calls, so if a user shares their screen to display a file during an audio call, this image and therefore the file content will be captured in the recording. The recording will be stored in the Skype app for thirty days,[64] to save it users must download the file; all participants in the chat will have access to the file for download.

Some Skype apps offer a free translation service. The Skype section of the *Microsoft Privacy Statement* notes, "When you use translation features, your voice and text data are used to provide and improve Microsoft speech recognition and translation services."[65] In the section of the *Microsoft Privacy Statement* explaining the usage of personal data, Microsoft notes ". . . we manually review short snippets of a small sampling of voice data we have taken steps to de-identify to improve our speech services, such as recognition and translation."[66] This also links to the captioning feature offered by Skype, which may use data to ". . . improve Microsoft speech recognition and related services."[67] This means that Microsoft employees or vendors are listening to samples of the voice data submitted through these Skype's features, which can include private or confidential conversations.[68]

[62] Mohammed I Al-Saleh and Yahya A Forihat, "Skype Forensics in Android Devices," *International Journal of Computer Applications*, vol. 78, n. 7, 2013.

[63] "Microsoft Privacy Statement,"above note 60.

[64] "Skype File Sharing: File Types, Size, and Time Limits," above note 58.

[65] "Microsoft Privacy Statement," above note 60.

[66] *Ibid*.; also see "Skype Translator Privacy FAQ," *Microsoft*, n.d, available at: https://support.skype.com/en/faq/FA34583/skype-translator-privacy-faq.

[67] "Microsoft Privacy Statement," above note 60.

[68] Joseph Cox, "Microsoft Admits Humans Listen to Skype and Cortana in Privacy Policy Update," *Vice*, 14 August 2019, available at: https://www.vice.com/en_us/article/qvgpkv/microsoft-updates-privacy-policy-admits-humans-listen-to-cortana-skype.

Data sharing

Microsoft collects a complex web of users' personal data. Microsoft's personal data collection includes a user's identifying information (name, contacts details, age, sex, country, language); credentials; payment information; account details (such as history, contracts, licences); interactions with Microsoft products (such as browsing history, bots, frequency of use, devices); interests and favourites; product consumption (such as media viewing, books, games); input data (such as voice, text, inking, typing); social interactions; feedback; or location data.[69] This data may be supplemented by data collected by third parties and shared with Microsoft.[70] Microsoft partners with third party advertising companies, whom ". . . may place cookies on your computer and collect data about your online activities across websites or online services."[71] Opting out of advertising does not stop the data from being collected.

Data is also collected in the form of content generated or shared by the user, such as voice messages, video files or IM text. Microsoft collects content to provide services, such as collecting the content of a file shared by one Skype user in order to display it to another Skype user.[72] Error reports sent to Microsoft may include content of files or other data about software on the user's device.[73] Microsoft does not claim any ownership of content and does not use content to target advertising, but does claim a "worldwide and royalty-free intellectual property license to use Your Content, for example, to make copies of, retain, transmit, reformat, display, and distribute via communication tools",[74] confirming processing of content to "the extent necessary to provide the Services".[75]

Microsoft may also share personal data with third parties, confirming further processing of data, including content data, will occur when complying with valid legal processes, protecting customers, operating and maintaining the security of products or protecting the rights or property of Microsoft.[76] If users access Skype through a Microsoft partner company,

[69] "Microsoft Privacy Statement," above note 60.

[70] *Ibid*.

[71] *Ibid*.

[72] *Ibid*.

[73] *Ibid*.

[74] Microsoft Services Agreement," above note 47.

[75] *Ibid*.

[76] "Microsoft Privacy Statement," above note 60.

that company's privacy policy governs how it handles the data; Microsoft may help partner companies comply with laws or legal requests by accessing, transferring, disclosing or preserving data, including private Skype content.[77]

Microsoft-controlled affiliates, subsidiaries, vendors and agents may receive personal data to carry out functions on Microsoft's behalf.[78] Push notifications on many devices are provided by other companies; Microsoft shares data with these companies (such as the first few words of a Skype IM or the name of a caller), who then use this information in accordance with their own terms and privacy policies. Skype bots, offered by Microsoft or third parties, "may have access to your display name, Skype ID, country, region, language, and any messages, audio, video, or content," depending on the bot's capabilities.[79]

Breaches and risks

The security of voice over internet protocol (VoIP) systems like Skype are often assumed, creating a false sense of privacy;[80] both research and actual security breaches confirm this hypothesis. Following increased scrutiny of the company after eBay's 2005 purchase of Skype, some experts advised reconsidering the use Skype in the workplace.[81] Many security risks were linked to Skype around this time period, especially pertaining to its former peer-to-peer architecture and still-current ease of installation.[82] Following Skype's transition to a

[77] *Ibid.*

[78] *Ibid.*

[79] *Ibid.*

[80] Benoit Dupasquier, et al., "Analysis of Information Leakage from Encrypted Skype Conversations," *International Journal of Information Security*, n. 9, 2010, p. 313.

[81] Andy Reinhardt, Robert D. Hof and Ben Elgin, "Getting Skittish About Skype," *Bloomberg, L.P.*, 15 January 2018, available at: https://www.bloomberg.com/news/articles/2005-11-27/getting-skittish-about-skype.

[82] See authors including Ray-Guang Cheng, et al., "Design and Implementation of a Skype Protocol Analyzer," *IEEE Conference on Communications and Network Security 2013,* National Harbor, MD, USA, IEEE, 2013; Jane Dudman and Gaynor Backhouse, "Voice Over IP: What It Is, Why People Want It, and Where It Is Going," *JISC Technology and Standards Watch*, 2006; B. Dupasquier, et al., above note 80; Tim Greene, "Study: Skype Dangers May Be Acceptable to Businesses," *Network World,* 2006, *InfoTrac Computer Database*, accessed

cloud infrastructure in recent years, breaches and privacy concerns have continued to be identified.

In 2012, a serious security flaw allowed Russian hackers to take over accounts just by knowing the associated email address.[83] In 2014, the Syrian Electronic Army posted to Skype's official blog and social media pages, using a phishing attack and enabled by Skype's failure to activate two-factor authentication.[84] In 2015, an Italian hacking company was itself breached; it was discovered the company was selling software to Morocco and the United Arab Emirates that allowed the countries to monitor applications like Skype.[85] A 2015 analysis of Skype's use in the health care system, identified various security risks and concluded Skype is unsuitable for communicating private health information.[86] In 2016,

22 January 2018; Marcus Sachs, Paul Piccard and Brian Baskin, "Skype," *Securing IM and P2P Applications for the Enterprise*, Kidlington, Elsevier Science, 2005; Mudhakar Srivatsa, et al., "Privacy in VoIP Networks: Flow Analysis Attacks and Defense," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, n. 4, 2011; Joanne Taaffe, "Into The Breach," *Total Telecom Magazine*, 2006; James Watson, "Voice Over IP Not Without Risks, Warn Experts," *Computing*, 2005, p. 16, *ACI*, accessed 15 January 2018; Valerie JM Watzlaf, Sohrab Moeini and Patti Firouzan, "VoIP for Telerehabilitation: A Risk Analysis for Privacy, Security, and HIPAA Compliance," *International Journal of Telerehabilitation*, vol. 2, n. 2, 2010; Ye Zhu and Huirong Fu, "Traffic Analysis attacks on Skype VoIP Calls," *Computer Communications*, vol. 34, n. 10, 2011.

[83] Charles Arthur, "Skype Disables Password Reset to Block Account Hijack by Email," available at: https://www.theguardian.com/technology/2012/nov/14/skype-password-account-hack-reset.

[84] See Sean Michael Kerner, "Syrian Electronic Army Goes After Skype," *eWeek*, 2014, p. 1, *EBSCOhost*, accessed 15 January 2018; and Chester Wisniewski, "Shame on SnapChat, Skype for Security Breach," *CNN Wire*, 2014, *EBSCOhost*, accessed 15 January 2018.

[85] "'Professional Hacking' Company Suffers Data Breach," *Al Jazeera*, 2015, *Newspaper Source Plus*, accessed 15 January 2018.

[86] In the context of the United States' Health Insurance Portability and Accountability Act, see Sweta Gurung and Yoohwan Kim, "Healthcare Privacy: How Secure Are the VOIP/Video-Conferencing Tools for PHI Data?," *2015 12th International Conference on Information Technology-New Generations*, IEEE, 2015.

Microsoft patched a backdoor in Skype code for Apple operating systems, that appeared to have existed since 2005 and which would have allowed attackers to control many aspects of the software.[87] Also in 2016, Skype accounts were used to send spam links, a result of challenges relating to the process of integrating Skype and Microsoft accounts.[88]

VoIP communications such as Skype can be intercepted lawfully, through a warrant issued by a law enforcement agency, or unlawfully, by malicious actors.[89] The lawful interception of Skype data fell into the spotlight in 2013. United States intelligence documents were leaked to the media by contractor Edward Snowden, revealing that Microsoft and Skype had cooperated with intelligence agencies to circumvent encryption and provide access to data – including collecting Skype audio, video, chat and file transfers as part of the PRISM monitoring program.[90] Included on surveillance lists were aid agencies such as UNICEF and Médecins du Monde.[91] It was reported that Skype's integration with PRISM began in November 2010, in spite of the legal order not being received until February 2011, with interceptions increasing even further within nine months of Microsoft's acquisition of Skype in May 2011.[92] Shortly after the PRISM disclosure, it was reported that Skype had its own

[87] Robert Lemos, "Skype for Mac Backdoor Allowed Access to Calls, Messages for Years," *eWeek*, 2016, *MasterFILE Premier*, accessed 15 January 2018.

[88] Tom Warren, "Why Are Skype Accounts Getting Hacked So Easily?," *Vox Media*, 17 January 2018, available at: https://www.theverge.com/2016/11/8/13561024/microsoft-skype-baidu-linkedin-hack.

[89] Abdullah Azfar, Kim-Kwang Raymond Choo and Lin Liu, "A Study of Ten Popular Android Mobile VoIP Applications: Are the Communications Encrypted?," *2014 47th Hawaii International Conference on System Science*, Waikoloa, HI, IEEE, 2014, p. 4858.

[90] National Security Agency, *User's Guide for PRISM Skype Collection*, by National Security Agency, Canadian Journalists for Free Expression, 2012.

[91] Laura Poitras, Marcel Rosenbach and Holger Stark, "Friendly Fire: How GCHQ Monitors Germany, Israel and the EU," *Der Spiegel*, 20 December 2013, available at: https://www.spiegel.de/international/world/snowden-documents-show-gchq-targeted-european-and-german-politicians-a-940135.html.

[92] Glenn Greenwald, et al., "Microsoft Handed the NSA Access to Encrypted Messages," *The Guardian*, 11 July 2013, available at: https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data.

internal secret program called Project Chess, which explored ways to make Skype calls more readily available to intelligence and law enforcement agencies.[93]

Technology companies have insisted data sharing processes were driven by legal demands,[94] with Microsoft issuing a statement saying:

> We provide customer data only when we receive a legally binding order or subpoena to do so, and never on a voluntary basis. In addition we only ever comply with orders for requests about specific accounts or identifiers. If the government has a broader voluntary national security program to gather customer data we don’t participate in it.[95]

Similar controversy arose in 2006 and 2008, when Skype was first revealed to be censoring keywords in TOM-Skype IMs, the version of the software used in China.[96] Skype was then found to be transmitting and insecurely storing the censored messages instead of discarding them.[97] The Electronic Frontier Foundation’s *Who Has Your Back* series rates companies on privacy and transparency; Skype last appeared independently of Microsoft in 2012, where it was awarded zero stars for its privacy and transparency commitments.[98]

In a 2016 report, Amnesty International asserts end-to-end encryption is essential for the protection of human rights because it ensures companies cannot access the content of

[93] James Risen and Nick Wingfield, "Web's Reach Binds NSA and Silicon Valley Leaders," *The New York Times*, 19 June 2013, available at: http://www.nytimes.com/2013/06/20/technology/silicon-valley-and-spy-agency-bound-by-strengthening-web.html?_r=1.

[94] G. Greenwald et al., above note 92.

[95] "Statement of Microsoft Corporation on Customer Privacy," *Microsoft*, 7 June 2013, available at: https://news.microsoft.com/2013/06/07/statement-of-microsoft-corporation-on-customer-privacy/.

[96] Ben Charny, "Chinese Partner Censors Skype Text Messages," *Ziff Davis*, 20 April 2006, available at: https://www.pcmag.com/g00/article2/0,2817,1951625,00.asp?i10c.encReferrer=&i10c.ua=1.

[97] Nart Villeneuve, *Breaching Trust: An Analysis of Surveillance and Security Practices on China's TOM-Skype Platform*, Information Warfare Monitor/ONI Asia, 2008.

[98] Marcia Hofmann, Rainey Reitman and Cindy Cohn, *2012: When the Government Comes Knocking, Who Has Your Back?*, Electronic Frontier Foundation, 2012.

communications under pressure from law enforcement, nor can malicious actors or surveillance operatives access the content via a breach to the company systems, concluding, ". . . [Microsoft] is not using an adequate level of encryption on [Skype]."[99] The report gives Microsoft's Skype a rank of forty out of 100 for messaging privacy. As at 2019, Skype offers end-to-end encryption within the abovementioned limits of the private conversation feature, but not by default.

Dropbox

Features and data processing

Dropbox is a cloud-based file hosting service, ". . . to store your files, documents, photos, comments, messages . . . collaborate with others, and work across multiple devices and services."[100] This free[101] service is popular with humanitarian workers because it allows co-workers to establish a share drive with only an internet connection, a useful feature to facilitate the easy sharing and syncing of documents in a geographically dispersed workplace.

Dropbox users can create shared workspaces by inviting other users to edit or view shared folders or files, by sharing links to folders or files, or by sending a file request to receive a file.[102] A link can be accessed with or without a Dropbox account and all link recipients will be able to download any documents to which they receive access. [103] [104] The link may be

[99] Amnesty International, *For Your Eyes Only*, London, 2016, p. 38.

[100] "Dropbox Privacy Policy," *Dropbox*, 25 July 2019, available at: https://www.dropbox.com/privacy.

[101] Paid business solutions exist, but this paper will consider the free version employees are likely to install independently of their IT departments.

[102] "Share a File or Folder," *Dropbox*, n.d, available at: https://help.dropbox.com/files-folders/share/share-file-or-folder.

[103] "How Do I Share With People Outside Dropbox?," *Dropbox*, n.d, available at: https://help.dropbox.com/files-folders/share/share-outside-dropbox.

[104] Paid Dropbox services allow higher control over link sharing, such as passwords, download controls, or expiration dates.

further shared or accessed if it is bookmarked, stored in browsing logs or history, or sent to a shortening service provider.[105]

Dropbox can be synced across multiple devices. This means that if a user has Dropbox on their phone, computer and tablet, files will be available on all these devices.[106] Syncing reduces the use of USBs or emailed copies but does allow for files to be accessible on multiple devices – regardless of the device security or ownership – and also limits the ability of copies to be recovered if the file is already synced or downloaded, for example, after an employee has left the organisation.[107]

Dropbox allows users to collaborate on shared files. Features include syncing edits across all files; the creation of clearly labelled "conflicted copies", which are multiple copies to manage and preserve conflicting edits (as may occur when users edit files offline, simultaneously edit, or edit and leave the file open[108]); a version control function that stores previous versions for thirty days;[109] and notifications of edits made by other users to a shared Dropbox.[110]

Dropbox retains the information stored on the service as long as the account exists, or as long as Dropbox requires it to provide the service. When a user deletes information, Dropbox will "initiate deletion" after thirty days.[111] In circumstances where users delete information, Dropbox notes:

[105] Cheng-Kang Chu, et al., "Security Concerns in Popular Cloud Storage Services," *IEEE Pervasive Computing,* vol. 12, n. 4, 2013, pp. 55-56.

[106] "Syncing: An Overview," *Dropbox*, n.d, available at: https://help.dropbox.com/installs-integrations/sync-uploads/sync-overview.

[107] See David Gibson, "Dodging the Effects of the Big Bang: Collaborating Securely in the Cloud," *Computer Fraud & Security,* vol. 2013, n. 2, 2013; and Dan Sorensen, "Left to Your Own Devices," *Utah Business,* vol. 27, n. 5, 2013.

[108] "What's a Conflicted Copy?," *Dropbox,* n.d, available at: https://help.dropbox.com/files-folders/share/conflicted-copy.

[109] "File Version History Overview," *Dropbox,* n.d, available at: https://help.dropbox.com/files-folders/restore-delete/version-history-overview.

[110] "How To Turn On Dropbox Notifications," *Dropbox*, n.d, available at: https://help.dropbox.com/accounts-billing/settings-sign-in/notified-changes.

[111] "Dropbox Privacy Policy," above note 100.

> (1) there might be some latency in deleting this information from our servers and back-up storage; and (2) we may retain this information if necessary to comply with our legal obligations, resolve disputes, or enforce our agreements.[112]

An incident in January 2017 saw files that had been deleted up to eight years ago restored to user accounts.[113] In a Dropbox forum, an employee explains this was the result of a bug and confirms files are typically removed within sixty days (the removal period at the time of the incident).[114]

Dropbox takes no responsibility for loss of data and its consequences, although in certain countries may be liable for foreseeable loss.[115] Dropbox will delete any free account that has not been accessed for twelve consecutive months.[116]

Data sharing

In order to "provide, improve, protect, and promote" services, Dropbox collects and uses user data, including account information (contact details, payment data); "Your Stuff" (user content hosted by the service such as documents or pictures); your contacts (such as the email of people you collaborate with); usage information (what you do with and on the service); device information (such as IP address, location, device type, browsing history); cookies and other technologies (for service functionality and advertising); and marketing information (such as sending promotional emails).[117]

[112] *Ibid*.

[113] Robert Hackett, "Dropbox Didn't Actally Delete Your 'Deleted' Files," *Fortune*, 25 January 2017, available at: http://fortune.com/2017/01/25/dropbox-bug-delete-files-restore/.

[114] Ross S, "Deleted Folder Reappeared After a Couple of Years," *Dropbox*, 19 January 2017, available at: https://www.dropboxforum.com/t5/Missing-files-and-folders/deleted-folder-re-appeared-after-a-couple-of-years/m-p/203016/highlight/true#M8819.

[115] "Dropbox Terms of Service," *Dropbox*, 25 July 2019, available at: https://www.dropbox.com/privacy#terms.

[116] *Ibid*.

[117] "Dropbox Privacy Policy," above note 100.

Dropbox users retain ownership of the content data uploaded to the service; Dropbox clearly states, “Your Stuff is yours. These Terms don’t give us any rights to Your Stuff except for the limited rights that enable us to offer the Services.”[118]

The permission users grant when accepting the terms of service include Dropbox hosting, backing up and sharing content when the user requires;[119] to provide certain features, Dropbox also “. . . accesses, stores, and scans Your Stuff. You give us permission to do those things, and this permission extends to our affiliates and trusted third parties we work with.”[120]

Dropbox states it will not sell information to advertisers, or other third parties; when trusted third parties are used to “provide, improve, protect, and promote” Dropbox services, they will be bound by the same privacy policy, with Dropbox taking responsibility for their handling of information as per Dropbox instructions.[121] At the time of writing, these trusted third parties included Amazon, Google and Oracle, among others.[122] Disclosure of data to third parties will also occur to comply with applicable laws, regulations, legal processes, or government requests; protect any person from death or injury; prevent fraud or abuse; protect Dropbox’s rights, property, safety or interests; or perform a task carried out in the public interest.[123] Presently, Dropbox opposes governments’ installation of backdoors into online services;[124] which has been interpreted by industry experts as policy that prohibits Dropbox from sharing data for surveillance.[125] If the user chooses to give access to third parties, for example via Dropbox APIs, then the user enables Dropbox and the third party to exchange information and the third parties’ privacy policies and terms will apply.[126]

[118] "Dropbox Terms of Service," above note 115.

[119] *Ibid*.

[120] *Ibid*.

[121] "Dropbox Privacy Policy," above note 100.

[122] "The Dropbox Privacy Policy: Frequently Asked Questions," *Dropbox*, n.d, available at: https://help.dropbox.com/accounts-billing/security/privacy-policy-faq.

[123] "Dropbox Privacy Policy," above note 100.

[124] "Transparency Overview," *Dropbox*, n.d, available at: https://www.dropbox.com/transparency.

[125] Nate Cardozo, et al., *Who Has Your Back?*, Electronic Frontier Foundation, 2017, p. 35.

[126] "Dropbox Privacy Policy," above note 100.

Dropbox’s ability to disclose information to third parties is facilitated by Dropbox’s control of encryption keys on users’ behalf, reportedly for simplicity, advanced features and stronger cryptographic control.[127] This means Dropbox does not use end-to-end encryption.[128] In 2014, Edward Snowden criticized this setup, calling Dropbox “hostile to privacy” because controlling the encryption keys enables the company to give user data to the government.[129] The Snowden leaks included a document indicating the United States’ National Security Agency planned to add Dropbox as a PRISM provider.[130] Dropbox has a clear policy on handling government requests, only acting on legal, valid and specific requests.[131] In the 2017 *Who Has Your Back* report, the Electronic Frontier Foundation gave Dropbox a full five stars in recognition of the company’s approach to transparency and user privacy.[132] Overall, this indicates that while the mechanism for data sharing is there, the company’s public-facing stance prioritizes the protection of user data.

[127] *Dropbox Business Security: A Dropbox Whitepaper*, Dropbox, 2019, p. 29.

[128] "How Dropbox Keeps Your Files Secure," available at: https://help.dropbox.com/accounts-billing/security/how-security-works.

[129] Jemima Kiss, "Snowden: Dropbox Is Hostile to Privacy, Unlike 'Zero Knowledge' Spideroak," *The Guardian*, 17 July 2014, available at: https://www.theguardian.com/technology/2014/jul/17/edward-snowden-dropbox-privacy-spideroak.

[130] National Security Agency, "PRISM/US-984XN Overview," *The Courage Foundation*, April 2013, available at: https://edwardsnowden.com/2013/06/07/prism-overview-slides/.

[131] "Transparency Overview," above note 124.

[132] N. Cardozo, et al., above note 125, p. 34.

Breaches and risks

Dropbox has experienced data breaches. In June 2011, a software glitch allowed accounts of twenty five million users to be accessed without an accurate password,[133] leaving users sensitive content exposed for a four hour period until it was discovered and fixed by the company.[134] In 2012, usernames and passwords stolen from other websites were used to gain unauthorized access to a Dropbox staff member's account, resulting in the launch of a spam campaign using customers' email addresses.[135] In August 2016, personal data from sixty eight million Dropbox user accounts were published online, data likely obtained during the 2012 breach;[136] Dropbox stated they did not believe any accounts were improperly accessed due to their threat monitoring systems and password security measures.[137] In January 2019, this data was still circulating the dark web.[138]

Overall, it is evident the unmanaged, shadow IT use of Skype or Dropbox may put a humanitarian organisation at odds with its responsibilities to meet data protection standards. The next section will provide an analysis of each data protection principle that incorporates an assessment of compatibility with the relevant features and functions of each service.

[133] Christian Cachin and Matthias Schunter, "A Cloud You Can Trust," *IEEE Spectrum*, vol. 48, n. 12, 2011.

[134] Arash Ferdowsi, "Yesterday's Authentication Bug," *Dropbox*, 20 June 2011, available at: https://blogs.dropbox.com/dropbox/2011/06/yesterdays-authentication-bug/.

[135] See Kevin Beaver, "Breach in the Cloud," *Security Technology Executive*, vol. 22, n. 7, 2012; and "Dropbox Employee Password Theft Leads to Spam Campaign," *CIO Insight*, 2012, *Health Business Elite*, accessed 24 January 2018.

[136] Michael Kan, "The Dropbox Data Breach Is a Warning to Update Passwords," *CIO (13284045)*, 2016, *Business Source Complete*, accessed 24 January 2018.

[137] Patrick Heim, "Resetting Passwords to Keep Your Files Safe," *Dropbox*, 25 August 2016, available at: https://blogs.dropbox.com/dropbox/2016/08/resetting-passwords-to-keep-your-files-safe/.

[138] Scott Ikeda, "The Data Dump of 2.2 Billion Breached Accounts: What You Need to Know," *CPO Magazine*, 9 February 2019, available at: https://www.cpomagazine.com/cyber-security/the-data-dump-of-2-2-billion-breached-accounts-what-you-need-to-know/.

Applying the Framework to the services

The principle of fairness and lawfulness requires data collectors explain to data subjects a minimum amount of information concerning the data processing.[139] Skype and Dropbox functionality meets the Handbook’s definition for data processing – in particular: recording, organisation, structuring, retrieval, use, disclosure by transmission, dissemination, erasure – thus if Skype and Dropbox are utilized, they will need to be considered in transparency statements to data subjects. This raises two issues: first, if the products are being used and installed in an ad hoc manner by humanitarian staff without formal IT support, this complicates the formulation of any statements to data subjects regarding the processing. In other words, how can the role of Skype and Dropbox in processing be accurately explained to needs assessment survey respondents, if the technology is not part of formal data management policy or procedure? Meeting this principle will require advance knowledge of processing actions, something that not just Skype or Dropbox challenge, but any instance of shadow IT.

The second issue is demonstrated by the summary of Skype and Dropbox features: using these products may expose data to complex processing actions that go beyond simply sharing or storing a file. For example, once a distribution registration list is stored in Dropbox, it is exposed to users’ link sharing and downloading options. Focus group transcripts sent between users on Skype can result in a copy saved to the recipient’s hard drive. Any data processed by either Skype or Dropbox exposes the data to content collection and processing policies, potentially including sharing data with third parties. Determining the “minimum amount” of information to convey under the principle of fairness, as well as identifying and explaining the associated risks and benefits to data subjects, may be a lengthy and challenging process, particularly in a fast-paced emergency setting; managing this requires organisations have a planned, established and controlled data processing approach.

Humanitarians using Skype and Dropbox could breach the principle of purpose limitation, by exposing personal data to further processing at the discretion of the technology company within the scope of enabling third party applications, advertising and improving the functionality of the product. For example, Microsoft may use content to “improve” Microsoft products, an example given is to “make copies” of content.[140] Thus, Skype users must

[139] C. Kuner and M. Marelli (eds), above note 20, p. 32.

[140] “Microsoft Services Agreement," above note 47.

consider if improving Microsoft services is an additional purpose for that content and what exactly improving entails.

Likewise, Microsoft and Dropbox may undertake further processing in circumstances including law enforcement requests, protecting customers or the product, protecting against fraud, abuse or attacks on the product, or protecting the rights and property of the companies.[141] While none of these actions are unreasonable in theory, the extent and method of further processing will lie in the hands of the software companies; humanitarians must consider if this expands the purpose of the data collected and if this expansion is appropriate for the data in question. For example, given the current climate of hostility towards refugees and migrants by many receiving governments, transferring the interpretation and decision making on government requests for documents that might contain program participants' medical, protection, location or other sensitive information to Skype and Dropbox – companies that were, respectively, enthusiastic and shortlisted PRISM participants – should give humanitarian actors pause. This means that humanitarian organisations need to develop robust operating protocols: determining what data can be processed with what technology. This requires knowledge of the technology actually being used by staff, thus circling back to the need to manage shadow IT.

Additionally, the nature of humanitarian response in itself challenges purpose limitation, so technology that simplifies the informal communication of information may exacerbate this tendency. Humanitarian programming often changes rapidly from day-to-day, thus it is quite likely that data collected for one purpose may become useful for another at a later point in time. For example, data initially collected by program staff for the purposes of a distribution and stored in a widely accessible Dropbox folder, could be accessed by other staff to aggregate and use in donor reports, funding proposals or media releases. While the technology itself is not the cause, it certainly enables the process, thus underscoring the need for robust policy on the use of such tools, including managing access permissions and ensuring staff can recognize which documents must be protected.

[141] "Microsoft Privacy Statement," above note 60; "Dropbox Privacy Policy," above note 100; and Dropbox includes an additional broad circumstance, for a task "carried out in the public interest".

Skype and Dropbox's automatic collection of metadata – such as location, frequency of use, language preferences, device type – has implications for the principles of proportionality and minimization, potentially affecting the safety of crisis-affected populations and humanitarian staff. The Handbook observes that metadata accessed and analysed by third parties can be detrimental to vulnerable individuals and advises that the collection of metadata should be as limited as possible, to minimize the risk of it being turned over to government or sold for commercial interests.[142] To illustrate this risk, consider a humanitarian operation in a politically sensitive location, with tenuous humanitarian access. Skype's metadata may reflect a great increase in communications in the area, due to a surge of staff; increased communications and information sharing about the crisis may not be viewed positively by belligerents. If this metadata is breached and becomes known to belligerents, it may affect humanitarian access, which could result in crisis-affected populations losing access to life-saving services, or it could allow humanitarian workers to be targeted for kidnapping, violence or other negative actions to discourage their presence. The collection of metadata by Skype and Dropbox enable this risk, so the metadata these services generate must be considered in relation to proportionality and minimization (is this excessive data collection and handling?), as well as the general risk of harm. In fact, this consideration applies not only to Skype and Dropbox, but to any use of a technology: all create metadata. Organisations must weigh the benefits of using such tools versus the risk, likely in a context-specific assessment; which, of course, requires organisations to know and control what tools staff are using.

The principles of proportionality, minimization and quality, as well as the implementation of any policies regarding data retention, are affected by the usage of Skype and Dropbox. Consider this scenario:

A monitoring and evaluation (M&E) officer is responsible for a spreadsheet containing distribution registration data, keeping the master copy saved locally. Using Skype IM, a program manager requests a copy of the data from the M&E officer; the M&E officer replies by transmitting the spreadsheet via Skype. When the program manager receives the file, a copy is automatically downloaded to the computer's hard drive. The program manager opens the spreadsheet and manually saves a copy to a Dropbox folder, where it will now be accessible to the whole program team. Program staff access the spreadsheet using their

[142] C. Kuner and M. Marelli (eds), above note 20, p. 142.

personal Dropbox credentials to log in and view the file. Most have the Dropbox application sync to their personal phones and work laptops; they do not always work in locations with internet access, so sometimes view or edit the data offline, which creates conflicted copies of the spreadsheet in the Dropbox folder. The program manager also emails the Dropbox link to an external consultant. The consultant does not have a Dropbox account, so downloads a copy of the data and saves it to the consulting firm's cloud storage drive instead. This syncs with colleagues' local folders.

If the organisation's data protection policy requires the data be deleted after twelve months to ensure a proportional storage period, how will it be ensured that the multiple people using multiple programs across multiple devices all delete their copy of the data? Likewise, has the creation and sharing of multiple copies breached the criterion for minimization of processing? And if an error is detected in the data, will the erroneous copies continue to be used and interfere with maintaining data quality? Can this affect distribution planning or cause erroneous donor reporting? This is an issue that could be controlled by strict information management policies, however if Skype and Dropbox are utilized without information management policy in place – as would occur in the shadow IT usage of the services – it is easy to see how the control of documents can be lost.

Unregulated shadow IT will exacerbate the challenges of ensuring data security and processing security in humanitarian workplaces. It is clear the sector is making increasing use of technology, but developing the internal policies, procedures and general level of staff knowledge and ability to use technology responsibly is less apparent.[143] While historically Skype and Dropbox have both experienced data breaches, companies whose core business is managing and protecting user information may be better equipped to manage and detect threats[144] than the average humanitarian organisation. Skype and Dropbox are both at risk of lawful or unlawful intercept of data, but – while making no guarantees about data loss or security, nor employing end-to-end encryption and with Skype historically lacking transparency on data sharing and facilitating surveillance – the companies do work to minimize the risk of breaches. It is the shadow IT use that elevates risk of data breach,

[143] See L. Butt, above note 17; F. Gerry QC, J. Muraszkiewicz and N. Vavoula, above note 15; P. Meier, above note 15; K.B. Sandvik, above note 16; C. Tansey et al., above note 15.

[144] Tina Irgang, "Cloud On Your Horizon? What Managers Should Ask About Data Storage," *New Orleans CityBusiness (LA)*, 2017, *Newspaper Source Plus*, accessed 24 January 2018.

including employees linking accounts to unsecure devices, personal accounts, or weak and infrequently changed passwords. Users can be the weakest link when it comes to data security because humans make mistakes.[145] The shadow IT use of Skype and Dropbox put data security and processing security at risk because it bypasses the creation of IT security policy, information management procedure and appropriate staff training.

Conclusion

Looking back to the historical examples of identity card systems that were abused to harm the populations the cards purportedly helped manage, it can certainly be hypothesized that humanitarian organisations' data could be abused too. In fact, there are already concerns about humanitarian organisations' initiatives inadvertently aiding surveillance of target populations, about interest from the military and surveillance industries and about publicly available humanitarian data supporting non-humanitarian purposes. [146] Examples include the possibility that military commanders used information from crisis maps during the Libyan Civil War,[147] or the United Kingdom's Home Office using a charity data map intended to protect rough sleepers, to target people for deportation.[148] There is demand for this data, therefore humanitarian organisations must protect it.

The features of Skype and Dropbox can facilitate the breach of data protection principles. However, it is their shadow IT application creating the problem; Skype and Dropbox are not inherently in breach of data protection principles. This indicates that not only does the use of Skype and Dropbox in humanitarian work require scrutiny, but so does other shadow IT

[145] See B. Hayes, above note 21; Fran Howarth, "The Role of Human Error in Successful Security Attacks," 2 September 2014, available at: https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/; C. Martin-Shields, above note 15.

[146] See B. Hayes, above note 21; G. Hosein and C. Nyst, above note 4; and K.B. Sandvik, et al., above note 15.

[147] Steve Stottlemyre and Sonia Stottlemyre, "Crisis Mapping Intelligence Information During the Libyan Civil War: An Exploratory Case Study," *Policy & Internet*, vol. 4, n. 3-4, 2012.

[148] Mark Townsend, "Home Office Used Charity Data Map to Deport Rough Sleepers," 19 August 2017, available at: https://www.theguardian.com/uk-news/2017/aug/19/home-office-secret-emails-data-homeless-eu-nationals.

trends in the humanitarian sector, such as online collaboration (Google Docs, Google Drive), electronic data collection tools (KoBo Toolbox, Open Data Kit), messaging apps (WhatsApp, Viber), social media (Facebook, Twitter), virtual assistants (Siri, Alexa), the use of personal email addresses by new staff or consultants (Gmail, Yahoo, Outlook), café or hotel Wi-Fi networks, personal USBs, personal hard drives, personal phones. . . the list is extensive.

Humanitarian actors can take action. This starts with increasing awareness of the issue. At sector-level, this means developing and disseminating software-specific profiles – like this one for Skype and Dropbox – through the lens of applicable data protection guidance. And conducting research, to determine the prevalence of shadow IT and galvanize action. At organisation-level, this means internal awareness raising around the risks related to shadow IT and failure to maintain data protection standards. Staff must be taught to identify what data is considered personal data, what documents may contain this data, what technologies pose risk, how to manage this risk and when to turn to IT specialists for support. This could even extend to program activities, supporting community members to understand what happens to their data, the risks it poses and their data rights. At individual-level, staff members can adopt a culture of assessing before implementing technology, seeking information about data protection standards and thinking critically about data collection in the first place, in terms of the risk level associated with collected data fields. Managers can lobby for their teams to have access to data protection information and training relevant to their technical area.

Awareness must be supported by policies and procedures that guide better data management practices. Organisations must develop robust information management and IT security policies, then effectively socialize these. Organisations must find out what tools staff use and assess these tools against data protection frameworks and the organisation's risk acceptance levels. If freely available software is found to be lacking, organisations must invest in more robust systems, including the expertise needed to establish and run systems. This includes considering interoperability, capacity building and resourcing for partners. Bringing organisations into compliance with data protection standards requires investment in developing IT systems that are appropriate to the increasingly data-driven sector and the current needs of staff, providing the right software and hardware. To better ensure systems are both compliant and realistic for field use, organisations will need to work to foster better inter-departmental collaboration and mutual understanding between IT, M&E and program teams, while ensuring policy is developed with a clear understanding of day-to-day field work. What not to do is develop an aspirational, high level document with no means to operationalise it – the very nature of shadow IT is that staff are using it due to an absence of systems appropriate to their needs, data protection must be a full package. This requires a genuine shift in organisational thinking and commitment to view data management as a collective responsibility to protect and respect program participants.

These steps will require support and investment from donors, along with donor acknowledgement that to responsibly meet reporting requirements, data must be managed appropriately – to do so requires ongoing financial investment in suitable tools, technology and in-house expertise. This may also require donors and humanitarian organisations to better communicate how data is being collected, so mutual decisions can be made on the necessity of the data used in reporting versus its risk and management costs. Ultimately, humanitarians are here to assist and protect crisis-affected populations; this extends to protecting their personal data. This means going beyond the simple acceptance of the quickest or cheapest technology available, to a method of working that brings the day-to-day technological tools used in humanitarian work out from the shadows.