

DEMOS

**A ROOM
OF ONE'S
OWN**

A GUIDE TO PRIVATE
SPACES ONLINE

ELLEN JUDSON
JOSH SMITH

OCTOBER 2020

Open Access. Some rights reserved.

Open Access. Some rights reserved. As the publisher of this work, Demos wants to encourage the circulation of our work as widely as possible while retaining the copyright. We therefore have an open access policy which enables anyone to access our content online without charge. Anyone can download, save, perform or distribute this work in any format, including translation, without written permission. This is subject to the terms of the Creative Commons By Share Alike licence. The main conditions are:

- Demos and the author(s) are credited including our web address **www.demos.co.uk**
- If you use our work, you share the results under a similar licence

A full copy of the licence can be found at **<https://creativecommons.org/licenses/by-sa/3.0/legalcode>**

You are welcome to ask for permission to use this work for purposes other than those covered by the licence. Demos gratefully acknowledges the work of Creative Commons in inspiring our approach to copyright. To find out more go to **www.creativecommons.org**



This project was supported by GCHQ



Published by Demos October 2020

© Demos. Some rights reserved.

15 Whitehall, London, SW1A 2DD

T: 020 3878 3955

hello@demos.co.uk

www.demos.co.uk

CONTENTS

ACKNOWLEDGEMENTS	PAGE 4
EXECUTIVE SUMMARY	PAGE 5
INTRODUCTION	PAGE 7
PART 1 TOWARDS A DEFINITION OF PRIVATE SPACE ONLINE	PAGE 8
PART 2 A DEFINITION OF PRIVATE SPACES ONLINE	PAGE 12
PART 3 POLICY AND PRACTICE	PAGE 21
PART 4 RECOMMENDATIONS	PAGE 30
APPENDIX POLLING RESULTS	PAGE 32

ACKNOWLEDGEMENTS

We would like to thank all of those in civil society, academia and government who took time to speak to us about this project, and offer their perspectives on the issues discussed. In particular, those who were kind enough to meet with us, offer comments on the issues and on the draft report, including those who attended a closed roundtable discussion on the report, which was held before publication. Thanks in particular to: Chloé Berthélémy, Dr Elinor Carmi, Fred Langford, Eleonora Nestola, Eliska Pirkova, and Dr Carissa Véliz.

Thanks must of course go to our colleagues at Demos - past and present - who helped us write this report - through all their support, both intellectual and emotional! To Alex Krasodomski-Jones, for his constant guidance and wisdom; Harry Carr for his expert assistance designing the poll and Asli Atay for her superb analysis of the polling results; Bibi Nubir for always keeping the finances in check; Maeve Thompson and Josh Tapper for their amazing work on the production and launch; James Sweetland, for his thorough proofread; Elliot Jones, for helping us kick off this report; and Maria Olanipekun, for helping us see it over the line.

We would also like to thank GCHQ for their support which made this report possible.

As ever, any and all mistakes and omissions are our own.

Ellen Judson
Josh Smith

October 2020

EXECUTIVE SUMMARY

Private spaces, online and offline, are valuable. Privacy allows people to exercise control and grants freedom. A private space may be necessary to develop one's own plans, to forge relationships, and to understand the world. Different political and social contexts will affect people's conceptions of privacy, and the circumstances in which it is most valued. But the key concern remains, that private spaces are necessary for freedom and security.

Which online spaces are considered private by policymakers and platforms has significant ramifications, from defining technical specifications for online spaces to enforcing regulation of platform action on harmful content online. At the heart of this debate is a tension between different security needs: between the need to tackle serious harms that can proliferate in private online spaces, and the need to preserve the ability of individuals to protect themselves and communicate safely in private.

Within current policy and platform discussions, the concepts of public and private spaces are frequently employed, but with admitted uncertainty about their practical application. This lack of clarity on what a private space online is or should be risks a fragmented implementation of different visions of privacy, and the use of different standards and different definitions. This will come at a significant cost to transparency, coherence and predictability of how online spaces operate: affecting internet users, businesses and security.

This paper examines the spectrum of online spaces and our expectations around our private and public lives online, in order to present a definition of a private space online. We draw on philosophical literature, offline analogies to public spaces, as well as legal frameworks and cases. In addition, we build upon the results of an original nationally representative poll, carried out by Demos in May 2020, of 1,035 people in the UK.

KEY RECOMMENDATIONS

We present our working definition of a private space online:

An online space should be considered private insofar as a user can reasonably expect that they control who sees information that they share within that space.

It is not the case that the only spaces which we should think of as private are those in which a user in fact has total control of their information. Rather, if a user reasonably expects to have that control, then the information within that space should be treated as private and that information not accessed or used without their knowledge, except in exceptional circumstances.

We believe that this definition is valuable as, although what is a 'reasonable expectation' is clearly contestable, it centres users' experiences and understanding, and at a minimum confers obligations on companies to be transparent and upfront about who can see information that users share (not simply hide the fact away in terms and conditions or legal jargon). Otherwise users may reasonably expect that their information is private, from platforms as well as from other users.

This definition also acknowledges that there are degrees of privacy. No space is 100% public or 100% private - different social and technical contexts, expectations of users, ownership of and access to the space, all intersect to establish the degree to which a space is or is not private. Definitions suggested by respondents to our polling for what makes a private space online suggests a spectrum along the following lines:

- **Most private** - a personal, secure online space, which can be accessed and controlled only by one individual user.

- **Semi-private** - a space where only a limited number of known participants communicate, where trust and technical safeguards allow information shared to be controlled by users - perhaps with exceptions for legitimate authorities to access or transparent platform oversight.
- **Not at all private** - a space where contents of communications can be viewed by anybody, and used or shared without having to go through any barriers - although social expectations and safety precautions may limit what people share in these spaces.

In practice, this definition leads to various obligations that platforms, policymakers, and other stakeholders should consider when designing, regulating, or accessing private spaces online.

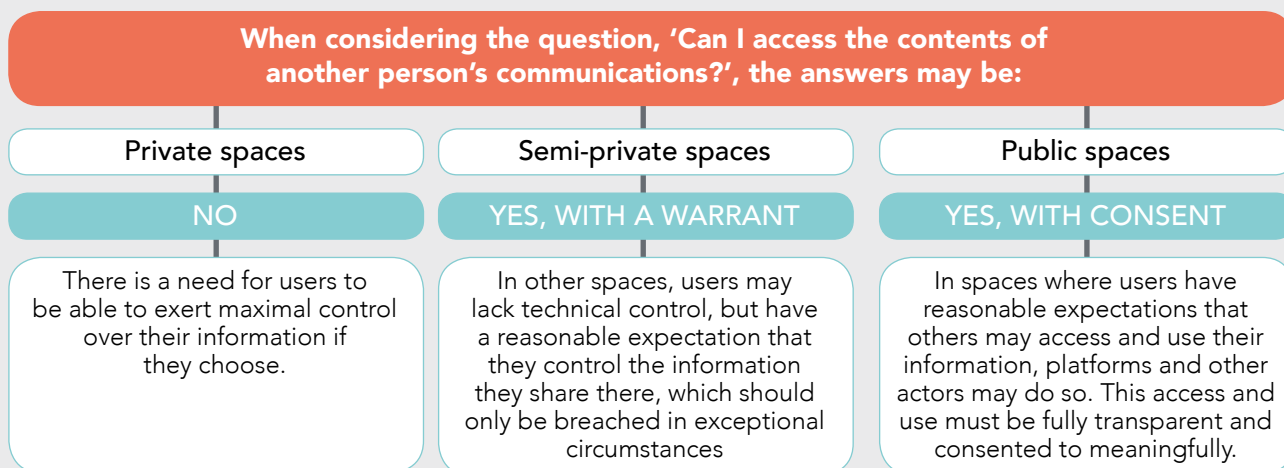
There is a need for users to be able to exert maximal control over their information if they choose. Users should have access to spaces which offer clear privacy - where they are able to understand and control who has access to information which they are sharing, and where data is end-to-end encrypted. This need not be the case for all messaging services, but where it is not the case, this should be clearly communicated to users and alternatives offered. End-to-end encryption as a tool for ensuring privacy should be protected. In our view, current proposals for exceptional access do not provide adequate technical protection for the rights of users against extrajudicial access by state or non-state actors. Therefore, alternative social and technical solutions to the problems of illegal content in end-to-end

encrypted spaces should be invested in and built through collaboration and open discussion between government, tech platforms and civil society.

In other spaces (e.g. private messages which are not encrypted) users may have a reasonable expectation that they control the information they share there, which should only be breached in exceptional circumstances. Platforms should provide data to law enforcement only in a targeted way, in response to an authorised request with clear judicial oversight. Platforms should also have a burden of proof to demonstrate, where they are accessing people's messages for commercial use, that their users do not have a reasonable expectation that that information is private from the company. This would include, but not be limited to, clear terms of service. Companies which met independent standards on doing so could be eligible for a 'kitemark' that indicated their appropriate management of private spaces online.

In spaces where users have reasonable expectations that others may access and use their information, platforms and other actors may do so. This expectation must be managed through transparency and access and use should be on the basis of meaningful consent. Platforms should ensure that information about the control and accessibility of spaces is sufficient for users to engage with and meaningfully consent to the terms offered. Researchers, when seeking to access data from private spaces online, should be transparent about their activities and intentions, and give users the option, where possible, to retain or consent to handing over control of their information.

This can be summarised as a tripartite test for engaging with private spaces online.



INTRODUCTION

The ideas of privacy and private spaces online, and the emergence of enormous digital public spaces, represent perhaps the two most important digital policy debates in recent years. Rarely, however, are the two connected. On the one hand are questions around our right to a private life online that tend to flare up around surveillance, security and the microprofiling of each and every internet user by major platforms. Seemingly separate debates take place about the health and freedom of the new, digital communities that so many of us treat as the digital public square.

This paper brings these two debates together, examining the spectrum of online spaces and our expectations around our private and public lives online. In Part 1, we discuss why we need a definition of private spaces online. Which online spaces are considered private, and which ones might not, will shape the future of regulation in this space. In Part 2, we present our working definition of a private space online:

An online space should be considered private insofar as a user can reasonably expect that they control who sees information that they share within that space.

In approaching the question of how to define private spaces online, we present a consideration of offline analogies which we believe are useful in guiding this discussion. In Part 3, we set out some of the ramifications of our proposed definition for policy and practice, from how users can conceive of spaces, to how platforms should design spaces, to how policymakers should regulate them and how law enforcement should approach them.

Continuing our discussion from *What's in a name?*, with its focus on anonymity online, we propose a tripartite test that can be used for examining private spaces online.

Can I access the contents of another person's communications?

- **NO:** There is a need for users to be able to exert maximal control over their information if they choose.
- **YES, WITH A WARRANT:** In other spaces, users may lack technical control but have a reasonable expectation that they control the information they share there, which should only be breached in exceptional circumstances.
- **YES, WITH CONSENT:** In spaces where users have reasonable expectations that others may access and use their information, platforms and other actors may do so. This access and use must be fully transparent and consented to meaningfully.

In Part 4, we present recommendations for policy and practice. Throughout, we draw on philosophical literature, offline analogies to public spaces, legal frameworks and cases, and an original nationally representative poll of 1,035 people in the UK, carried out by Demos in May 2020.

PART 1

TOWARDS A DEFINITION OF PRIVATE SPACE ONLINE

Which online spaces are considered private by policymakers and platforms has significant ramifications, from defining technical specifications for online spaces to enforcing regulation of platform action on harmful content online.

At the heart of this debate is a tension. The recent history of the internet has shown that private online spaces, such as closed groups, chats or other private messaging services, are often those in which terrorist content or CSEA (child sexual exploitation and abuse) imagery is shared, violence is incited, and dangerous misinformation can be spread, without oversight or remedy.^{1,2,3,4} They are also places where journalists can speak to at-risk sources; where members of marginalised groups can come together to support each other and share their experiences safely; where civil society can plan and organise without fear of reprisal or persecution.

Within current policy discussions, the concepts of public and private spaces are frequently employed, but with admitted uncertainty about their practical application. The UK Online Harms White Paper,

A private space may be necessary to develop one's own plans, to forge relationships, to understand the world: a public space is necessary to put that plan into action, to build on and extend those relationships, and to interact with the wider world, not merely observe it.

published by the Department of Culture, Media and Sport in 2019, says that:

'Any requirements to scan or monitor content for tightly defined categories of illegal content will not apply to private channels. We are consulting on definitions of private communications, and what measures should apply to these services.'

Governments are not the only ones making moves here. Platforms are also signalling intentions to change where on the spectrum of public or private spaces they lie. Facebook, in setting out its

1. Paul, K. Facebook's crackdown on dangerous content in groups could backfire, experts say. The Guardian, 2019. Available at <https://www.theguardian.com/technology/2019/aug/14/facebook-private-groups-rules-extremist-fake-news> [accessed 30 July 2020]
2. Porter, T. Unlicensed medical 'cures' are flourishing in closed Facebook groups, where cancer treatments — and even surgery — are sold beyond the reach of the law. Business Insider, 2019. Available at <https://www.businessinsider.com/in-closed-facebook-groups-pushing-unproven-treatments-2019-8?r=US&IR=T> [accessed 30 July 2020]
3. Pietsch, B. Mass shooting rumor in Facebook Group shows private chats are not risk-free. Available at <https://www.reuters.com/article/us-facebook-groups-focus/mass-shooting-rumor-in-facebook-group-shows-private-chats-are-not-risk-free-idUSKBN1WP1CG> [accessed 30 July 2020]
4. Wakefield, J. Facebook encryption threatens public safety, say ministers. BBC, 2019. Available at <https://www.bbc.co.uk/news/technology-49919464> [accessed 30 July 2020]

vision for the future of the platform, has explicitly referenced how it is seeking to move away from being a digital 'town square' to a digital 'living room'. However, what this means beyond metaphor is still being established, and without clarity on what a private space online is or should be, there is a risk of a fragmented implementation of different visions of privacy, and the use of different standards and different definitions. This will come at a significant cost to internet users, businesses and security.

Drawing a distinction between a public and a private space is not easy. The very coherence of the distinction is fiercely debated. The variance across different contexts of conceptions of privacy means that finding a definition that is usable by transnational platforms and international institutions is a challenge. But with these international corporations without democratic accountability on the way to entrenching the standards for our online private and public lives, there is a need to set out the standards that a liberal democracy should expect of platforms, which centre the needs of their citizens.

The traditional 'public/private' distinction contrasts work or political life with home or family life. On this account, what occurs within the home, within the bounds of one's private property, regarding one's closest and intimate relationships, should be private to oneself and not exposed to public scrutiny. In contrast, if you are in the public arena, you are participating in public life, and your actions may be observed and critiqued by others.⁵ It is likely this definition which underpins the majority of debates on the subject.

This distinction has been widely criticised as erasing the public aspects of private life. Those parts of our lives which previously might have been separated by spatial distance (work and home, or family and wider social life) are now more interconnected through the use of online spaces (we can communicate with our closest friends privately while standing in the middle of the street; we can speak to hundreds of people from our living room). As such, this designation of different spaces as 'public' and 'private' captures the realities of life less and less.⁶

Some have argued against the distinction altogether - that putting 'private', family life beyond state intrusion or 'public' concern, has meant that domestic abuse, marital rape, and other forms of abuse or sexual and gender-based violence have historically been overlooked as 'private matters', and so delineating such a distinction victimises particularly women and girls.⁷ However, an elimination of the 'private' altogether, and an invitation of state intrusion into private spaces on the grounds of ending abuse, is itself likely to perpetuate oppressive conditions against members of marginalised groups, and overlook how private spaces hold real value for many people, even if they are hard to precisely define.⁸ Jennifer Nash writes of the value of private spaces for black women and communities of colour in particular:⁹

*'While the private can function as a space of violence, abuse, subordination, and exploitation, it can also operate as a locus of empowerment, safety, community-building, and solidarity, and it can perform contradictory meanings simultaneously.'*¹⁰

What is considered private, or what people desire to be private, also varies according to the political and social context and other norms with which it interacts. In the UK there are frequent concerns raised about surveillance carried out by major social platforms being the antithesis to privacy. Our polling shows that people in the UK often do not consider messages sent on Facebook to be especially private: a majority think that messages sent on Facebook Messenger to a group (54%) or a message posted on a Facebook timeline (62%) are not private (though 53% think that one-to-one messages sent on Facebook Messenger are private).

However, this view of Facebook as not especially private prevails in a context where people appear to trust tech companies with their data less than their government. 73% of people in our poll said they would be upset at tech companies accessing the contents of their communications without explicit permission, as opposed to only 62% if government departments did so. Our respondents

5. DeCew, J. Privacy. The Stanford Encyclopedia of Philosophy, ed. Zalta, 2018. Available at <https://plato.stanford.edu/archives/spr2018/entries/privacy/> [accessed 30 July 2020]

6. Ford, S.M. RECONCEPTUALIZING THE PUBLIC/PRIVATE DISTINCTION IN THE AGE OF INFORMATION TECHNOLOGY. Information, Communication & Society 14:4, 2011. Available at <https://www.tandfonline.com/doi/abs/10.1080/1369118X.2011.562220> [accessed 30 July 2020]

7. MacKinnon, C. in DeCew, J. Privacy. The Stanford Encyclopedia of Philosophy, ed. Zalta, 2018. Available at <https://plato.stanford.edu/archives/spr2018/entries/privacy/> [accessed 30 July 2020] and in Schneider, E.M. The Violence of Privacy. 23 Conn. L. Rev. 973, 1990-1991. Available at <https://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?referer=http://scholar.google.co.uk/&httpsredir=1&article=1363&context=faculty> [accessed 30 July 2020]

8. Allen, A. in DeCew, J. Privacy. The Stanford Encyclopedia of Philosophy, ed. Zalta, 2018. Available at <https://plato.stanford.edu/archives/spr2018/entries/privacy/> [accessed 30 July 2020]

9. Nash, J.C. From Lavender to Purple: Privacy, Black Women, and Feminist Legal Theory. 11 Cardozo Women's L.J. 303, 2004-2005. Available at https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/cardw11§ion=18 [accessed 30 July 2020]

10. Nash, J.C. From Lavender to Purple: Privacy, Black Women, and Feminist Legal Theory. 11 Cardozo Women's L.J. 303, 2004-2005, p.306. Available at https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/cardw11§ion=18 [accessed 30 July 2020]

were all from the UK - in a different social context, where the risks associated with tech companies or government accessing communications are different, these calculations of which spaces are more private may change. Where there is political persecution of activists by the state, people may be happier to use platforms such as Facebook, than more technically secure options. This is because, while Facebook will collect more personal data, it is viewed as less likely to disclose information to other parties, and so may be regarded as 'private' from the state institutions who matter to these users.¹¹

Conceptions of the nature and value of privacy itself vary across contexts. For instance, in China, privacy ('yinsi' '隐私') has historically been associated primarily with protecting one's reputation, and the need to keep secrets - though over time this narrow definition has expanded.¹² The purpose of privacy is often linked to wider social benefits rather than primarily to individual benefits: for example, freedom of thought and autonomy for an individual is linked by Li and Na to greater feelings of safety and so to social stability.^{13,14} Liang Qichao argued that 'the public welfare gong de (公德) was dependent upon a bounded private domain si de (私德) where thought could be cultivated.'¹⁵ But although government surveillance of online spaces is widespread, privacy protection regulation governing what tech companies can do with user data is strengthening, alongside critiques of excesses in surveillance,^{16,17} increasing calls for better data protection, and the persistence of 'reasonable expectations' of privacy.^{18,19}

Thus contextual variance may affect how and why people think that online spaces should be private or not. But the key concern remains, that there is value in private spaces, online and offline, within which you have control and freedom. The value of privacy and data protection specifically online has been affirmed by the AU, BRICS, EU, and UN.^{20,21,22,23} What is missing is consensus on: how far that value is defeasible; the source of that value; how best to protect that value and who from; and what constitutes harm that must be protected against.

Private spaces have an important role to play in facilitating individual autonomy - they are essential to our development of our sense of self, our relationships, and how we understand and connect with the wider world around us. Being able to set the boundaries which determine the form and nature of our interactions with others is a crucial element of realising personal autonomy through using private spaces.^{24,25} This control helps us manage and develop different relationships with different people, in which our behaviour may vary.²⁶ Privacy also helps us to develop our sense of ourselves, separated to some degree from outside view and so influence.²⁷ This was echoed by some of the respondents to our poll, who when asked for their own definition of a 'private space online', defined private spaces as places of freedom:

'Away from trolls and negativity, allowed to express yourself openly'
Female, 18-24²⁸

11. Privacy Camp. "Actually, In Google We Trust"? A 'Deconstructing' Conversation on Russian Internet Activism. 2020. Available at https://privacycamp.eu/?page_id=1949 [accessed 03 August 2020]
12. Pfeifle, S. China's evolving views on privacy. IAPP, 2017. Available at <https://iapp.org/news/a/chinas-evolving-views-on-privacy/> [accessed 03 August 2020]
13. Pfeifle, S. China's evolving views on privacy. IAPP, 2017. Available at <https://iapp.org/news/a/chinas-evolving-views-on-privacy/> [accessed 03 August 2020]
14. Yao-Huai, L. Privacy and data privacy issues in contemporary China. Ethics and Information Technology 7, 2005, pp.7-15. Available at <https://cdn.tc-library.org/Rhizr/Files/4367e301-0301-4e6f-b2d7-f6a54e794a83/042ef109-e363-4179-a284-4e5be354b67f.pdf> [accessed 03 August 2020]
15. Farrall, K.N. Global Privacy in Flux: Illuminating Privacy across Cultures in China and the U.S. International Journal of Communication 2, 2008, 993-1030. Available at <https://ijoc.org/index.php/ijoc/article/viewFile/370/228> [accessed 30 July 2020]. See also Lindsey, N. China's New Encryption Law Highlights Cryptography as a Strategic Priority. CPO Magazine, 2019. Available at <https://www.cpomagazine.com/data-protection/chinas-new-encryption-law-highlights-cryptography-as-a-strategic-priority/> [accessed 03 August 2020]; Verma, A. Internet in China: An Emerging Society. IPCS Series on Inside China, 2012. Available at <https://www.files.ethz.ch/isn/143512/SR120-CRP-InternetinChina.pdf> [accessed 03 August 2020]; Wang Rong. Data Protection Policies. Tencent Research Institute, 2018. Available at <https://www.secrss.com/articles/7496> [accessed 03 August 2020]
16. Yao-Huai, L. Privacy and data privacy issues in contemporary China. Ethics and Information Technology 7, 2005, pp.7-15. Available at <https://cdn.tc-library.org/Rhizr/Files/4367e301-0301-4e6f-b2d7-f6a54e794a83/042ef109-e363-4179-a284-4e5be354b67f.pdf> [accessed 03 August 2020]
17. Farrall, K.N. Global Privacy in Flux: Illuminating Privacy across Cultures in China and the U.S. International Journal of Communication 2, 2008, 993-1030. Available at <https://ijoc.org/index.php/ijoc/article/viewFile/370/228> [accessed 30 July 2020]
18. Sacks, S. and Laskai, L. China's Privacy Conundrum. Slate, 2019. Available at <https://slate.com/technology/2019/02/china-consumer-data-protection-privacy-surveillance.html> [accessed 03 August 2020]
19. Farrall, K.N. Global Privacy in Flux: Illuminating Privacy across Cultures in China and the U.S. International Journal of Communication 2, 2008, 993-1030. Available at <https://ijoc.org/index.php/ijoc/article/viewFile/370/228> [accessed 30 July 2020]
20. Mabika, V. The Internet Society and African Union Commission Launch Personal Data Protections Guidelines for Africa. Internet Society, 2018. Available at <https://www.internetsociety.org/blog/2018/05/the-internet-society-and-african-union-commission-launch-personal-data-protections-guidelines-for-africa/> [accessed 03 August 2020]
21. Belli, L. Data protection frameworks emerging in the BRICS countries. IAPP, 2020. Available at <https://iapp.org/news/a/data-protection-frameworks-emerging-in-the-brics-countries/> [accessed 03 August 2020]
22. OHCHR. The Right to Privacy in the Digital Age. United Nations, 2020. Available at <https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx> [accessed 03 August 2020]
23. General Data Protection Regulation. Intersoft Consulting. Available at <https://gdpr-info.eu/> [accessed 03 August 2020]
24. Farrall, K.N. Global Privacy in Flux: Illuminating Privacy across Cultures in China and the U.S. International Journal of Communication 2, 2008, 993-1030. Available at <https://ijoc.org/index.php/ijoc/article/viewFile/370/228> [accessed 30 July 2020]
25. Kupfer, J. Privacy, Autonomy and Self-Concept. American Philosophical Quarterly 24: 1, 1987. Available at https://www.jstor.org/stable/20014176?read-now=1&refreqid=excelsior%3Af09f486507af243c780703acd873f9f8&seq=2#page_scan_tab_contents [accessed 30 July 2020]
26. Rachels, J. Why Privacy is Important. Philosophy and Public Affairs, 4:4, 1975, pp. 323-333. Available at http://people.brandeis.edu/~teuber/Rachels_on_Privacy.pdf [accessed 30 July 2020]
27. Cohen, J.E. What Privacy Is For. Harvard Law Review 126, 2013. Available at https://cdn.harvardlawreview.org/wp-content/uploads/pdfs/vol126_cohen.pdf [accessed 30 July 2020]
28. NB: Poll responses have been edited throughout for clarity

Private spaces online also have clear instrumental value in protecting people from certain harms. They allow people to communicate safely - especially important for, for instance, journalists or activists in countries where they face government persecution, or for people discussing things which could lead to discrimination or persecution against them, such as their religion or sexual orientation. As such, private spaces online enable rights to be protected which we value in a liberal democracy - a free press, non-discrimination, safety and security and liberty of the person.

Private must also be defined in contrast to public. There are parts of the web that must be public: or at least, there is a spectrum, and some parts of the web - Twitter's timeline, for instance - are more public than others. Public spaces have always served a crucial purpose in the context of a liberal democracy, and now public spaces online continue this tradition:

*‘These websites can provide perhaps the most powerful mechanisms available to a private citizen to make his or her voice heard. They allow a person with an Internet connection to “become a town crier with a voice that resonates farther than it could from any soapbox.”’*²⁹

A private space may be necessary to develop one's own plans, to forge relationships, to understand the world: a public space is necessary to put that plan into action, to build on and extend those relationships, and to interact with the wider world, not merely observe it.

It is worth noting that access to private spaces online is not coextensive with having personal data privacy online: personal data privacy is a necessary, but not a sufficient, condition for a space online being private. An online platform could have 'gold standard' protections for personal data, but the spaces in which you operate on that platform may still be 'public' in the sense that anyone could see what you post. Similarly, if you went offline completely, and erased your online presence, your privacy in the personal data sense would be very well protected - but your access to private spaces online would be completely cut off - indeed, several respondents to our poll said that they did not use social media because they did not constitute private spaces. Alternately, a space where the contents of your communications is private, but all of your personal data and metadata of your communications are collected and shared, is less private than one where this data is not collected.³⁰ Hence protecting privacy online, which primarily concerns an individual, and protecting private spaces online, which concerns spaces where communication between individuals can occur, require different interventions.

29. Supreme Court of the United States. *Packingham vs North Carolina*. No. 15-1194, 2017. Available at https://www.supremecourt.gov/opinions/16pdf/15-1194_0811.pdf [accessed 30 July 2020]

30. With thanks to participants at our roundtable discussion for clarifying the necessity of this point, July 2020

PART 2

A DEFINITION OF PRIVATE SPACES ONLINE

In this section, we present our working definition of a private space online. We then discuss how each part of the definition is consistent with our understanding of offline private spaces, legal frameworks around private online spaces, and with public attitudes towards private spaces.

Based on our understanding of how concepts of private spaces are used and understood, online and offline, socially, conceptually and legally, we offer the following maxim:

An online space should be considered private insofar as a user can reasonably expect that they control who sees information that they share within that space.

This reasonable expectation should be able to be based both on social and technical elements of a space, in particular accessibility: how social relationships as well as design affect who can access a space, and for what purposes.

In approaching the question of how to define private spaces online, we consider four offline analogies, in which our beliefs about and expectations of privacy may be more developed. This approach of comparing online and offline is prompted by public debate: discussions of online spaces are full of references to 'public squares', 'town halls' and 'shopping malls'.³¹ The persistence

Visitors to these places find their behaviour is monitored, their information collected and controlled, for private gain and monetisation by the owners of the platform.

of these metaphors in popular vernacular, tech advertising, and policy debates shows that spatial metaphors are shaping how we think about these issues - and so we need to interrogate them appropriately.³²

We present four metaphors for online space below. These spaces all vary in their technical aspects: how they are designed, how they are built; how many entrances they have; whether the walls are glass or brick. They also vary in their social aspects - who uses the space, and what for, and the norms which govern interpersonal behaviour within that space.³³





Based on these analogies, we can see that privacy online has several constituent parts:

First, privacy as a matter of degrees. Second, privacy as attributable to individuals who use a space. Third, the role of reasonable expectation in determining how spaces are treated, and finally, the relation of information control within a space to privacy. Each part is discussed in more detail below.

31. Zuckerberg, M. A Privacy-Focused Vision for Social Networking. Facebook, 2019. Available at <https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/> [accessed 30 July 2020]

32. Hammett, E. Facebook launches UK privacy campaign. Marketing Week, 2019. Available at <https://www.marketingweek.com/facebook-launches-uk-privacy-campaign/> [accessed 30 July 2020]

33. Karaçor, E.K. Public vs. Private: The Evaluation of Different Space Types in Terms of Publicness Dimension. European Journal of Sustainable Development 5: 3, 2016, 51-58. Available at <https://ojs.ecsdev.org/index.php/ejsd/article/download/331/328> [accessed 30 July 2020]

Place	Accessibility	Permitted behaviour	Control of information	Online equivalents
 <p>Public park</p>	<p>Free access - open to all to enter the space, act within the space, or observe the space from outside ³⁴</p>	<p>Law enforcement may intervene in illegal activity</p> <p>Some legal activities may be banned, or others encouraged, by park rules and facilities (set by democratic authority)</p> <p>Social norms also govern behaviour - you don't go sit next to someone you don't know even though you can ³⁵</p>	<p>What people are doing is visible to all - no 'membership' restrictions</p> <p>But they can reasonably expect e.g. their conversations will not be recorded by others</p> <p>CCTV may be used</p>	<p>Democratic oversight of platforms is minimal; social conventions influence how information is shared ³⁶</p> <p>Closest equivalents:</p> <ul style="list-style-type: none"> • Subreddit • Public Twitter account • Public forum page (e.g. on Mumsnet)
 <p>Private garden</p>	<p>The owner can choose who to let into the garden, when, and has the right to ask them to leave for any reason</p> <p>Law enforcement may enter but the threshold of evidence/process needed to enter is high (e.g. a warrant)</p>	<p>Any legal behaviour permitted. Social norms will affect what is considered appropriate but the owner of the garden is likely to set the boundaries of acceptable behaviour rather than the group at large</p>	<p>What is happening may be observed outside of the space e.g. overheard by neighbours and vice versa, may be intruded upon by noise from outside the garden ³⁷</p> <p>Law enforcement may observe from outside without special permissions ³⁸</p>	<p>A space, observable by outside parties (such as platforms), within which the terms of engagement and admission are primarily determined by the owner/administrator</p> <p>Closest equivalent:</p> <ul style="list-style-type: none"> • Closed Facebook group ³⁹ • Email accounts which are monitored by provider (e.g. Gmail)
 <p>Open-air shopping centre</p>	<p>No visible demarcation or barriers to entry between outside the centre and inside the centre</p> <p>Individual shops may control entry to their shops though they appear free to enter at will</p> <p>Legal precedents in the US have established that though free to access, the public are 'invited' for the purpose of doing business, limiting their rights to free action or expression ⁴⁰</p>	<p>Dictated by the law and social norms, but also by rules of private owners of the centre</p> <p>Rules can be enforced by private security (e.g. against loitering, gathering, playing games) and often disproportionately affect marginalised groups (e.g. homeless people being told to move) ⁴¹</p> <p>First Amendment (free speech) rights do not generally apply in the US as centres are not public spaces</p>	<p>Surveillance of people's movements within shopping centres is commonplace</p> <p>Shopping centres can employ facial detection technologies to gather demographic information as well as attempt to record people's moods or reactions in response to certain advertisements</p> <p>If you connect to WiFi in a shopping centre or make a purchase, you are handing personal information over about your movements, location, and possibly dispositions</p> <p>There are limits on what kinds of surveillance or seen as socially acceptable - e.g. facial recognition uses can generate outcry ⁴²</p>	<p>Privately owned space which is generally accessible but which controls activities and collects information according to private interests</p> <p>Closest equivalents:</p> <ul style="list-style-type: none"> • Public Facebook page
 <p>Car</p>	<p>Accessible only to individuals with the key and selected companions</p> <p>Cars may be surveilled but only bugged in certain circumstances with appropriate authorisation. ⁴³</p> <p>This is regarded as 'intrusive' surveillance in the UK. ⁴⁴</p>	<p>Legal activities only permitted</p> <p>Within a car, certain design features must be configured in order to protect occupants and others (e.g. seatbelts installed).</p>	<p>A car does not exist in a private vacuum - generally, they are pockets of privacy which exist in and travel through public spaces</p> <p>You can have visibility of what people are doing in a car, and in some circumstances may be able to hear (if they have the windows open)</p> <p>However, generally, we would presume that conversations within a car are between the few occupants of that car, and not for other people to engage with, overhear or act on</p>	<p>A space within which accessing conversations requires a key; conversations are held to be private, though metadata can be collected</p> <p>Closest equivalent:</p> <ul style="list-style-type: none"> • End-to-end encrypted one-to-one chat (e.g. WhatsApp)

34. Planning and Housing Committee. Public life in private hands. London Assembly, 2011. Available at https://www.london.gov.uk/sites/default/files/gla_migrate_files_destination/Public%20space%20June%202021%20Webme.pdf [accessed 30 July 2020]

35. Hement, D. and others. Digital Public Space. FutureEverything, 2013. Available at <https://discovery.dundee.ac.uk/ws/portalfiles/portal/20381952/DPS.pdf> [accessed 30 July 2020]

36. Online, people operate with different social norms than in a physical space - a conversation between two people, posted for all to see on Twitter, is regularly picked up and used, commented upon, and so forth - someone's comment can instantly be broadcast to a whole new audience with the click of a button. This affects what expectations users can have, and so reduces the privacy those conversations can be said to have. However, there is still a desire for privacy: for instance, on Twitter there is a common critique that if one person criticises someone powerful without mentioning them by name, that others should not then mention that person as that risks fall-out for the original speaker. The original user does not expect their conversation to be completely private, but they do expect that a measure of the control they exerted over whose attention is drawn to a conversation or not should be respected.

37. Carmi, E. Media Distortions: Understanding the Power Behind Spam, Noise, and Other Deviant Media. Digital Formations. Available at <https://doi.org/10.3726/b15334> [accessed 30 July 2020]

38. US Supreme Court. Florida v. Riley. 488 U.S. 445, 1989. Available at <https://supreme.justia.com/cases/federal/us/488/445/> [accessed 03 August 2020]

39. Frankel, M. The promises and pitfalls of reporting within chat apps and other semi-open platforms: A journalist's guide. Nieman Lab, 2018. Available at <https://www.niemanlab.org/2018/07/a-journalists-guide-to-the-promises-and-pitfalls-of-reporting-within-open-and-closed-and-semi-open-platforms/> [accessed 30 July 2020]

40. Foster, J.C. Lloyd Corporation, Ltd. v. Tanner (1972). The First Amendment Encyclopedia. Available at <https://www.mtsu.edu/first-amendment/article/582/lloyd-corporation-ltd-v-tanner> [accessed 03 August 2020]

41. Shenker, J. Revealed: the insidious creep of pseudo-public space in London. The Guardian, 2017. Available at <https://www.theguardian.com/cities/2017/jul/24/revealed-pseudo-public-space-pops-london-investigation-map> [accessed 03 August 2020]

42. Sabbagh, D. Facial recognition technology scrapped at King's Cross site. The Guardian, 2019. Available at <https://www.theguardian.com/technology/2019/sep/02/facial-recognition-technology-scrapped-at-kings-cross-development> [accessed 03 August 2020]

43. The Newsroom. How police bug and hack crime barons. The Scotsman, 2009. Available at <https://www.scotsman.com/news/how-police-bug-and-hack-crime-barons-2444297> [accessed 03 August 2020]

44. Home Office. Covert Surveillance and Property Interference Revised Code of Practice. 2018. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf [accessed 03 August 2020]

PRIVACY AS A MATTER OF DEGREES

As discussed, drawing a clear line between a private and a public space is likely to be difficult and error-prone, if not impossible. No space is entirely 100% public or entirely 100% private - different social and technical contexts, expectations of users, ownership of and access to the space, all intersect to establish the degree to which a space is or is not private.

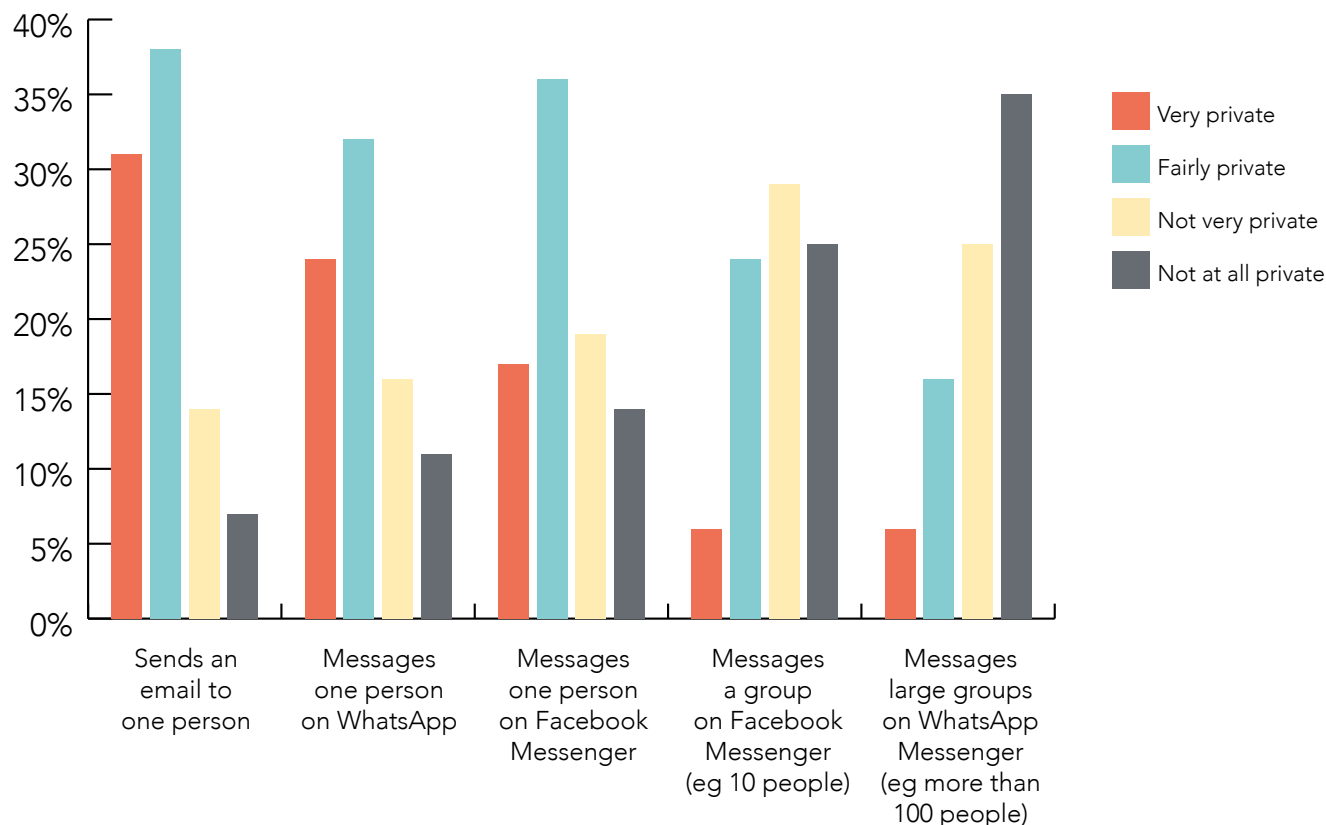
The offline spaces discussed demonstrate how different features may increase the privacy or public nature of a space - that controlled access may increase, but does not guarantee privacy, that there may be oversight even with an individual's privately owned space, and that behaviour may be permitted, facilitated or recorded within different spaces to different degrees. An approach which recognises that privacy of a space is a spectrum, rather than an either/or attribute is more likely to be practically applicable to different spaces and in different contexts. Moreover, privacy admitting of degrees is more likely to be conducive to protecting users online than a strict definition.

Since very few spaces can be called 100% private from all other parties, a degrees-based definition allows us to require that information shared in certain spaces be treated as private even if it could technically be accessed or compromised.⁴⁵ It also allows for distinctions to be made where a space may be private from some parties and not private from others, without designating such a space as simply not private due to limited access.⁴⁶

*'The element of control over one's personal life is never all-or-nothing, but a matter of an infinite number of degrees and decisions.'*⁴⁷

That different spaces may be private in some aspects and not private in others was reflected in our polling results. For instance, 38% of people said an email sent to one person was 'fairly private' and 31% said it was 'very private'; 36% said a message sent to one person on Facebook Messenger was 'fairly private' and 17% said it was 'very private'. Respondents did not view spaces as either 'very private' or 'not at all private', but affirmed that there were spaces in-between that had elements of both.

In general, how private do you think the content shared is when someone does the following?



45,46. Thanks to roundtable participants for these clarifying comments, July 2020

47. Lord Justice Leveson. AN INQUIRY INTO THE CULTURE, PRACTICES AND ETHICS OF THE PRESS: REPORT. The Leveson Inquiry, 2012.

Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/270939/0780_i.pdf [accessed 30 July 2020]

Definitions suggested in our polling for what makes a private space online suggests a spectrum along the following lines:

- Most private - a personal, secure online space, which can be accessed and controlled only by one individual user.
- Semi-private - a space where only a limited number of known participants communicate, where trust and technical safeguards allow information shared to be controlled - perhaps with exceptions for legitimate authorities to access or transparent platform oversight.⁴⁸
- Not at all private - a space where contents of communications can be viewed by anybody, and used or shared without having to go through any barriers - though social expectations and safety precautions may limit what people share in these spaces.

In short, we should not think of spaces as 'private' or 'public' completely. Rather, the existence of a spectrum of privacy, and a wider variety of types of spaces, need to be recognised in policy debates on these spaces.

PRIVACY AS ATTRIBUTABLE TO INDIVIDUALS WHO USE A SPACE

The analogy of the private garden specifically shows that one space may hold different levels of privacy for different people. The person who owns the garden can ensure anyone they do not trust, or feel comfortable speaking freely around (highlighted in our polling as key elements of a private space online) is excluded. However, the other guests in a space lack this privilege - they have been invited in and must put up with other people if the owner (or the admin) does not see fit to remove them. This shows that the privacy of a space can best be understood on an individual level, related to whom an individual has privacy from, rather than designating a space in all cases as 'private' or 'public'.

Privacy is also a human right which is owed at the individual level (respecting the privacy of a group at the expense of the privacy of some of its members would not be consistent with the framework). Article 12 of the UN Declaration on Human Rights states that: 'No one shall be subjected to arbitrary interference with his privacy,

family, home or correspondence, nor to attacks upon his honour and reputation.'⁴⁹ Article 8 of the European Convention on Human Rights states that 'Everyone has the right to respect for his private and family life, his home and his correspondence'.⁵⁰ The General Data Protection Regulation also affords protection for data privacy on an individual level, with personal data defined as information that relates to an identified or identifiable individual.⁵¹

Our polling highlighted the importance of privacy as relating to an individual. When asked to define a private space online, many respondents focused on the individuality of a private space - that it was specifically a space for them alone to use that was 'mine', particularly to store 'personal' information, that were your own 'business', such as photos, videos, documents, and personal one-to-one emails to family and friends. The sense of a space being 'one's own' was important in defining a private space online - being alone in a room or being in one's home were metaphors used to describe these spaces:

'Me and me only' Female, 60+

'My own world' Female, 25-39

'Encrypted and never available to be viewed by another human being ever' Male, 40-59

In short, though an online space may have many different members, the privacy of that space as it pertains to different individuals should be taken into consideration when designating a space as private or public.

THE RELATION OF INFORMATION CONTROL WITHIN A SPACE TO PRIVACY

An online space should be considered private insofar as a user can reasonably expect that *they control who sees information that they share within that space.*

Control of information is crucial to privacy offline: when we think about the ways our privacy can be invaded in the spaces discussed, people or companies gathering information about our presence in the space, our activities or information we share with others through conversations. We can also be said to share information through our actions - about who we are and what we are doing.⁵²

48. Demos. The Online Harms White Paper: A Consultation Response From Demos. 2019

49. OHCHR. Universal Declaration of Human Rights. 1948, Article 12. Available at https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf [accessed 30 July 2020]

50. ECHR. European Convention on Human Rights. 2010, Article 8, p.11. Available at https://www.echr.coe.int/Documents/Convention_ENG.pdf [accessed 30 July 2020]

51. ICO. What is personal data? Available at <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/> [accessed 31 July 2020]

52. Thanks to roundtable participants for these clarifying comments, July 2020

In the shopping centre, which is the closest offline analogy to commonly-used social media sites such as Facebook, apparent freedom is somewhat illusory. Visitors to these places find their behaviour is monitored, their information collected and controlled, for private gain and monetisation by the owners of the platform. This commercial oversight means that in such spaces you cannot be entirely in control of who has access to information about you and what you do in that space.⁵³

The legal discussion of what accountability people should hold for sentiments expressed in personal messages often centres around whether employers can fire or discipline staff on the basis of the contents of such messages. Legal analysis of cases in France surrounding employees' use of Facebook suggests that where personal messages are visible to the sender and recipient, they count as private (and so cannot be the basis for employer disciplinary action). However, if the visibility of these messages is made broader (e.g. by leaving the message on a screen others can read) the protections for private messages no longer apply.⁵⁴ Similarly, with posts on a Facebook profile, where that profile is public or even where it is not fully private (i.e. friends of friends can view it), the contents are viewed as public as they are widely accessible - the user has ceded control over who precisely can access their communications. Accordingly, a private profile is often viewed as private - though with some contention that the purpose of Facebook is the wide sharing of content, and it is not technically confidential as it is posted on an unsecured space on the Internet.^{55,56} Thus ceding control of information in a space is frequently seen as reducing the privacy of that space.

Our polling also highlighted that control of information and control of who accesses a space were crucial in people's conception of private spaces online. A high majority of participants (87%) said having control of who can see the information they share online is important to them.

When asked to define a private space online, there were several themes which emerged from the responses, which highlighted that control of information shared within a space was central. Control itself was central to many of the

respondents' definitions of a private space online. The word 'control' was frequently used, but other words, such as 'decision' or 'choice', reinforced the central role that a user being able to determine for themselves what happens in a private space plays. Often this control was about who gets to make decisions about who has access to spaces, using terms like 'permission', 'consent', 'authorisation' and 'invitation'. It was also about control of information shared within spaces - including information about your identity (anonymity), messages or data posted within a space.

'One which I could monitor, and had control over who was able to access it, and only open to the people I chose it to be open to.'
Female, 40-59

Features which made spaces online more technically secure, a means by which to control information, were frequently cited as defining a private space online, as well as general terms used like 'safe' and 'secure'. Encryption, including end-to-end encryption, password protection, use of VPNs, security against hacking or leaks, verification, use of security questions and PIN numbers, were all mentioned by respondents. Social elements of a space which made information control more likely were also mentioned in definitions: from access to a space being limited only to known people, to trusting everyone else in the space, to communicating primarily with friends and family in private spaces.

Many also thought that private spaces online were impossible because of a lack of control of information. This lack of control was linked to 'government and intelligence spyware', the possibility of other people in a space sharing information more widely, and people determined to access information (potentially referring to hackers). Those who said it was non-existent often expressed negative attitudes towards its non-existence - showing a desire for privacy, but a frustration with the lack of control that online services currently provide to their users, which puts some people off engaging online altogether.

'No such thing, as once information is online it can be made available by anyone who has access.' Male, 60+

53. Carmi, E. Media Distortions: Understanding the Power Behind Spam, Noise, and Other Deviant Media. Digital Formations. Available at <https://doi.org/10.3726/b15334> [accessed 30 July 2020]

54. Guardelli, L. and Fonseca L. Can employees be disciplined for their Facebook comments? International Law Office, 2018. Available at <https://www.internationallawoffice.com/Newsletters/Employment-Immigration/France/Coblence-Associis/Can-employees-be-disciplined-for-their-Facebook-comments> [accessed 30 July 2020]

55. Guardelli, L. and Fonseca L. Can employees be disciplined for their Facebook comments? International Law Office, 2018. Available at <https://www.internationallawoffice.com/Newsletters/Employment-Immigration/France/Coblence-Associis/Can-employees-be-disciplined-for-their-Facebook-comments> [accessed 30 July 2020]

56. The Association for the Defense of Human Rights in Romania – the Helsinki Committee. Personal Facebook Pages Are Public Space in Romania. Liberties, 2014. Available at <https://www.liberties.eu/en/news/romania-facebook-profiles-are-public-space/2494> [accessed 30 July 2020]

As identified in the polling, once any information is shared in an online space we cede some level of control over who sees it. A friend could tell someone else; a family member can take a screenshot and post it on Twitter; information could be obtained by hackers. Hence we take 'control' here to be control of the first-order; that is, does a user control who immediately has access to the information? And does a user not only have the potential to control this, but actually do so? For instance: a Facebook wall is set to 'public'. The user cannot control, under these settings, whether or not I look at their Facebook wall. They can change the settings to private, to keep me out; or block me specifically - but to do so would be to change the privacy of the online space. A public Facebook wall is not private just because it could be made private - it is private only if control is actually exerted.

In short, user control of the information they share must be central to any definition of a private space online. People may vary in how they wish that control to be exerted - whether via technical security, access restrictions, or social factors such as trust - but the need for private spaces online to grant users control over their information is clear.

THE ROLE OF REASONABLE EXPECTATION IN DETERMINING HOW SPACES ARE TREATED

An online space should be considered private insofar as a user *can reasonably expect* that they control who sees information that they share within that space.

How far online spaces are private is affected not only by whether users in fact have total control over their information (these will be few and far between)

PRIVACY BY DESIGN – A NOTE ON ENCRYPTION

As well as granting us new places in which to speak, online communication grants us new ways of speaking. Online, we can safeguard many of our most private actions from intrusion by speaking in code, using encryption. Put simply, encryption is the ability to encode data - a message, for example, or a password - in such a way that only the intended recipient can decrypt and view it.

Encryption comes in different forms, which can affect who is able to read encrypted messages. Let's suppose that a user's phone sends a message to the phone of a recipient, by sending it through a server run by a messaging application.

- 'Transport-layer' encryption protects messages in transit. In our example, this type of encryption protects the message as it was sent from the sender's phone to the messaging server (which may be e.g. run by Google), where it is decrypted. It is then encrypted again before being sent from the server to the recipient's phone. This protects the message from anyone able to intercept it in transit, but does not prevent the company controlling the server from reading the message.^{57,58}
- End-to-end encryption, by contrast, means that the message is encrypted on the sender's device, and decrypted on the recipient's device.⁵⁹

Due to how the message is encrypted, it can only be decrypted by the intended recipient, and not by the company providing the communications service, law enforcement or other third parties.

The success of either of these methods depends upon the strength of the encryption. No encryption is perfect, and anyone who is able to intercept a message and work out exactly how it was encoded will be able to convert it back into the original text (or image, video, voice call etc.) The aim of encryption is to make the task of finding the 'key' used to turn the data from a message into code so nearly impossible that the data remains secure.

The ability to seamlessly encrypt messages has a powerful effect on the privacy of those messages from eavesdroppers. This power flows not from the design of the platforms on which a message is sent, or from the rules and regulations governing those platforms, but from the form of the communications themselves. A subject sending a strongly encrypted message on the internet doesn't need to trust the cables, routers and other machines which will transmit this message to its recipient not to intercept it, nor trust assurances given by platforms that they will not access message contents, since only the recipient themselves can decode and understand it. The privacy of the message is built into the message itself.

57. EFF. What Should I Know About Encryption? Surveillance Self-Defense, 2018. Available at <https://ssd.eff.org/en/module/what-should-i-know-about-encryption> [accessed 30 July 2020]

58. Newsbeat. Encryption on Facebook Messenger and other chat apps. BBC, 2018. Available at <https://www.bbc.co.uk/news/newsbeat-43485511> [accessed 30 July 2020]

59. EFF. A Deep Dive on End-to-End Encryption: How Do Public Key Encryption Systems Work? Surveillance Self-Defense, 2018. Available at <https://ssd.eff.org/en/module/deep-dive-end-end-encryption-how-do-public-key-encryption-systems-work> [accessed 30 July 2020]

but also by whether users have a reasonable expectation of control.

In offline spaces, how people's information is treated is governed not only by legal or commercial oversight, but also by social norms. This is linked to how people expect that they will be treated and think that others expect to be treated: nothing prevents someone from sitting next to someone and listening to their private conversation in a park, other than the general social expectation that it should not be done.

Reasonable expectation is also a concept often cited in legal and regulatory cases around privacy, both online and offline.

The Press

When conversations are held in a space where other members of the public are present, (e.g. in a cafe, a park, a bar), how private information communicated in such a setting should be used has been held to depend not only upon the expectation of the speaker, but the reasonableness of that expectation. When Paul Mason claimed he had a 'reasonable expectation of privacy' in a restaurant discussing Jeremy Corbyn, a conversation which was reported by the Sun, IPSO did not find that their code of conduct had been breached and rejected his claim due to 'the complainant's professional role, the nature of his conversation, its timing and its location, in the environment of the party conference'.⁶⁰ Jonathan Peters has suggested that in these 'quasi-private' environments, who has control of and access to the space and whether those in the space have signalled they expect privacy are relevant factors in establishing whether a space is private or not. These need not be explicit requests for privacy, but could be, for instance, behavioural signals, such as a user anonymising themselves.^{61,62}

Employers

In the case of *Bărbulescu v. Romania*, Mr Bărbulescu had been dismissed by his employer after he was found to have used a company email account

to send personal emails, which was established by the company accessing these emails.⁶³ The European Court of Human Rights found that 'Bărbulescu's right to respect for his private life and correspondence under Article 8 was not adequately protected by the national authorities'.⁶⁴ This was not on the basis that the employer should not have accessed the personal emails at all - but rather that legitimate access required certain steps be taken, including ensuring employees had accurate expectations of the privacy of their work emails, such as being notified in advance that the contents of their emails might be monitored.⁶⁵

Platforms

Platforms' use has also been criticised on the grounds that personal messages should not be accessed by platforms where users are led to expect they are private. A class action lawsuit was brought against Facebook in the USA on the grounds that Facebook read and used which URLs were shared in private Facebook messages to target ads at individuals. (The case was settled on condition that Facebook updated its data policy and shared information in its Help Centre).⁶⁶ This case implies that whether a space online should be counted as private from platforms accessing them depends on user expectation and knowledge of whether or not a space will be accessed, rather than the nature of the communications or the public accessibility of the contents.

Law Enforcement

In the US, legal discussions around when communications online should be private from law enforcement without a warrant arises from where those communications have been given to a third party (not the sender or recipient). The 'third-party doctrine' holds that 'the Fourth Amendment does not prohibit government authorities from requesting and obtaining information entrusted to a third party' - such as a phone company to whom you have conveyed the phone number which you are calling.⁶⁷ However, Hodge argues that a demonstrated expectation of privacy can

60. IPSO. Decision of the Complaints Committee 13165-16 Mason v thesun.co.uk. 2017. Available at <https://www.ipso.co.uk/rulings-and-resolution-statements/ruling/?id=13165-16> [accessed 03 August 2020] via Porter, D. Brexit whispers: when eavesdropping on private conversations by a journalist is ethically justified. *The Conversation*, 2019. Available at [accessed 03 August 2020] <https://theconversation.com/brexit-whispers-when-eavesdropping-on-private-conversations-by-a-journalist-is-ethically-justified-111799>

61. Peters, J. Can I do that? A legal primer for journalists. *Columbia Journalism Review*, 2015. Available at https://www.cjr.org/united_states_project/can_i_do_that_a_legal_primer_for_journalists.php [accessed 03 August 2020]

62. IPSO. Decision of the Complaints Committee 13165-16 Mason v thesun.co.uk. 2017. Available at <https://www.ipso.co.uk/rulings-and-resolution-statements/ruling/?id=13165-16> [accessed 03 August 2020]

63. Columbia University. Case of Bărbulescu v. Romania. *Columbia Global Freedom of Expression*, 2020. Available at <https://globalfreedomofexpression.columbia.edu/cases/case-barbulescu-v-romania> [accessed 03 August 2020]

64. ECHR. Q & A: Grand Chamber judgment in the case of Bărbulescu v. Romania. 2017. Available at https://www.echr.coe.int/Documents/Press_Q_A_Barbulescu_ENG.PDF [accessed 03 August 2020]

65. ECHR. Q & A: Grand Chamber judgment in the case of Bărbulescu v. Romania. 2017. Available at https://www.echr.coe.int/Documents/Press_Q_A_Barbulescu_ENG.PDF [accessed 03 August 2020]

66. Bharatkumar, A. Campbell v. Facebook: California District Judge Approves Final Class Action Settlement Over Facebook's Use of URL Data. *Jolt*, 2018. Available at <https://jolt.law.harvard.edu/digest/campbell-v-facebook-california-district-judge-approves-final-class-action-settlement-over-facebooks-use-of-url-data> [accessed 03 August 2020]

67. Dixon, H. B. Telephone Technology versus the Fourth Amendment. *American Bar Association*, 2016. Available at https://www.americanbar.org/groups/judicial/publications/judges_journal/2016/spring/telephone_technology_versus_the_fourth_amendment/ [accessed 03 August 2020]

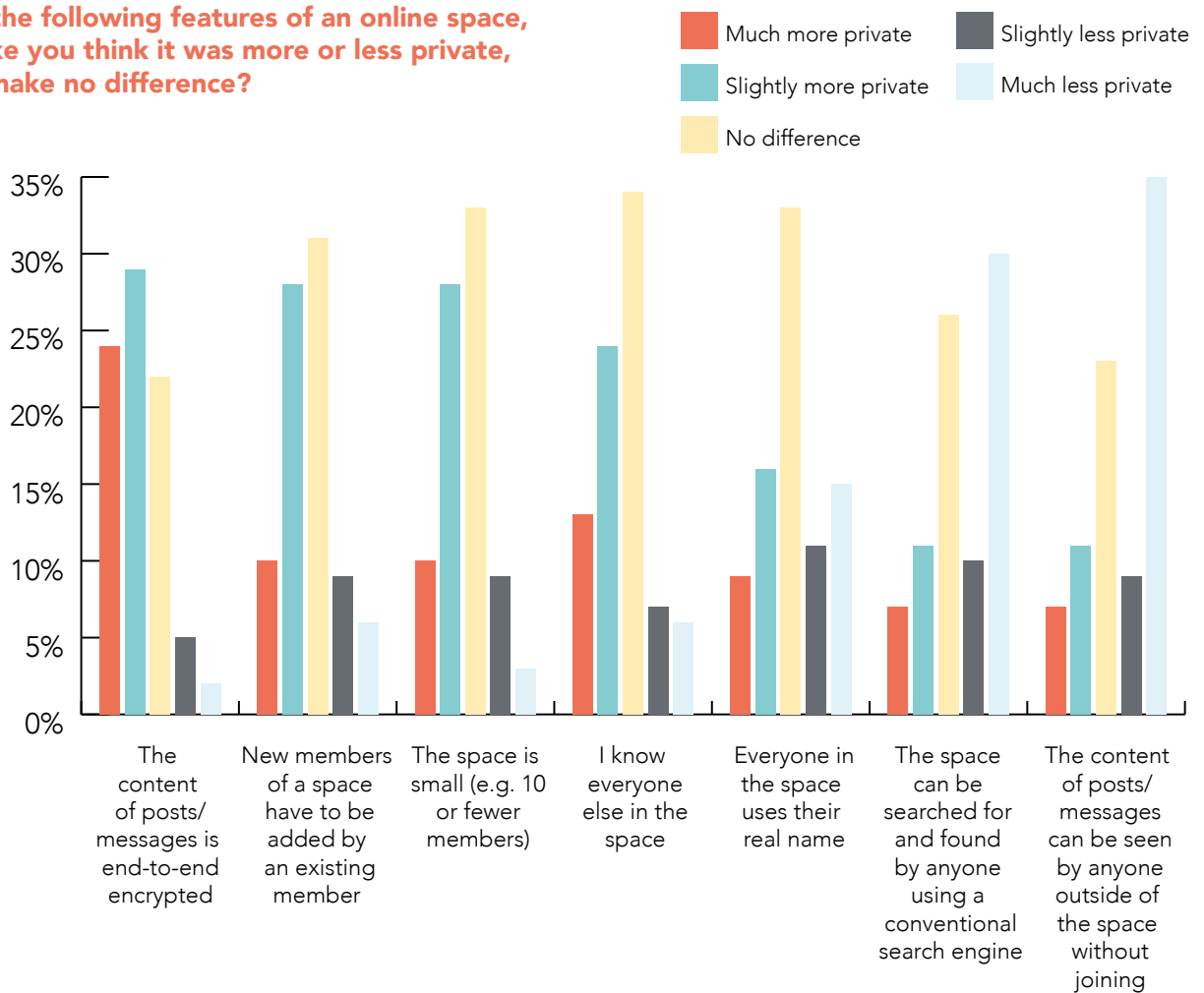
override the third-party doctrine and come under the Fourth Amendment when a user expected the third party to keep their information private.⁶⁸ The third party doctrine has been contested in relation to online services, in particular, given that users may not expect platforms to have access to or access their communications - hence emphasising that expectation of control is more pertinent to determining privacy than actual control.⁶⁹

In practice, defining a 'reasonable' expectation will be contested: reasonable according to whom, by whose standards?⁷⁰ It is true that adherence to this concept runs the risk that it is subject to amorphous change, as both society and technology develop.⁷¹ However, what it does do at a minimum is confer obligations on companies to be transparent and upfront about who can see information that users share (rather than simply hiding the fact away in

terms and conditions or legal jargon) - otherwise users may always reasonably expect that their information is private.

Does this not risk giving platforms free rein to simply make it very clear that users have no privacy on their services, and so claim no-one can reasonably expect - and thus cannot demand - privacy?⁷² We think not: 'reasonable expectation' should not be defined purely in relation to (though should certainly take into account) how transparent a platform's terms of use are about how they control access to, collect and use information shared in their spaces. This is an important piece of how expectations will be formed, but is not the only element. As discussed previously, the features of a space itself - its members, its 'walls', its rules, and how users understand the inner workings of platforms, not only their terms of service - all affect expectations.⁷³

For each of the following features of an online space, would it make you think it was more or less private, or would it make no difference?



68. Warfel, E.A. Perceptions of privacy on Facebook. Rochester Institute of Technology, 2008. Available at <https://scholarworks.rit.edu/theses/3076/> [accessed 03 August 2020]
 69. Warfel, E.A. Perceptions of privacy on Facebook. Rochester Institute of Technology, 2008. Available at <https://scholarworks.rit.edu/theses/3076/> [accessed 03 August 2020]
 70. Farrall, K.N. Global Privacy in Flux: Illuminating Privacy across Cultures in China and the U.S. International Journal of Communication 2 ,2008, 993-1030. Available at <https://ijoc.org/index.php/ijoc/article/viewFile/370/228> [accessed 30 July 2020]
 71. Warfel, E.A. Perceptions of privacy on Facebook. Rochester Institute of Technology, 2008. Available at <https://scholarworks.rit.edu/theses/3076/> [accessed 03 August 2020]
 72. Thanks to C. Véliz for this challenge
 73. Thanks to roundtable participants for clarifying comments and challenges on this point. July, 2020

No space is entirely 100% public or entirely 100% private - different social and technical contexts, expectations of users, ownership of and access to the space, all intersect to establish the degree to which a space is or is not private.

We envision a framework in which 'reasonable expectation', where unclear, would be subject to judicial scrutiny. The legal system frequently deals with concepts which are not fully defined, but is able to apply them based on the legal and social context within which they are relevant. Thus this element also allows for some contextual variance in definitions of privacy, where appropriate, as expectations and legal frameworks can vary accordingly.⁷⁴

Our polling indicated that the following features may be most relevant to determining people's expectation:

- Whether a space is encrypted (53% say it makes a space more private)
- If what is shared within that space is visible to others outside of the space (44% say it makes a space less private)
- If the space can be searched for and found by anyone (40% say it makes a space less private)
- Whether access is controlled by existing members (38% say it makes a space more private)
- If the space is small (38% say it makes a space more private)
- Whether members of a space know each other (37% say it makes a space more private)

In short, it is not that the only spaces which we should think of as private are those in which a user in fact has total control of their information. Rather, if a user reasonably expects to have that control, then the information within that space should be treated as private: that information should not be accessed or used without their knowledge, except in exceptional circumstances.

74. Farrall, K.N. Global Privacy in Flux: Illuminating Privacy across Cultures in China and the U.S. *International Journal of Communication* 2 ,2008, 993-1030. Available at <https://ijoc.org/index.php/ijoc/article/viewFile/370/228> [accessed 30 July 2020]

PART 3 POLICY AND PRACTICE

In this section, we set out some of the ramifications of our proposed definition for policy and practice. We examine how users can conceive of spaces and how platforms should design spaces, as well as how policymakers should regulate them and how law enforcement should approach them.

In our paper, *What's in a name?*, we presented a three-part test which approaches to anonymity must fulfil: namely that solutions for identity verification must:

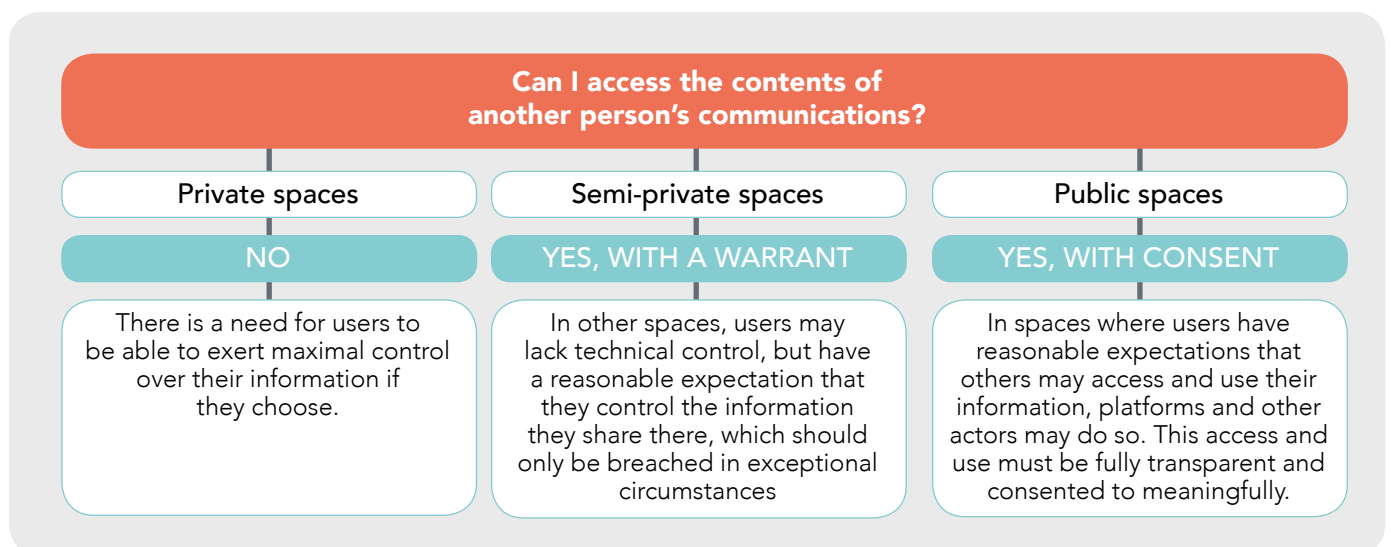
1. Protect internet users' ability to choose anonymity online, and emphasise its importance in preserving freedom of expression.
2. Allow accountable institutions tasked with preserving security to exercise their powers effectively.
3. Ensure users are able to fully consent to their identities being known by other third-parties.⁷⁵

We propose that a similar tripartite test can be used for examining the problem of private spaces online, based on the definition we have offered. We offer three answers to the question of who may access people's information that they share in spaces online, which apply in different circumstances.

We discuss these in more detail below:

THE NEED FOR PROTECTED SPACES

There is a need for users to be able to exert maximal control over their information if they choose. Users should have access to spaces which offer clear privacy - where they are able to understand and control who has access to information which they are sharing, and where data is end-to-end encrypted. This need not be the case for all messaging services, but where it is not the case, this should be clearly communicated to users and alternatives offered.



75. Smith, J. and others. *What's in a name? A forward view of anonymity*. Demos, 2020. Available at <https://demos.co.uk/project/whats-in-a-name/> [accessed 30 July 2020]

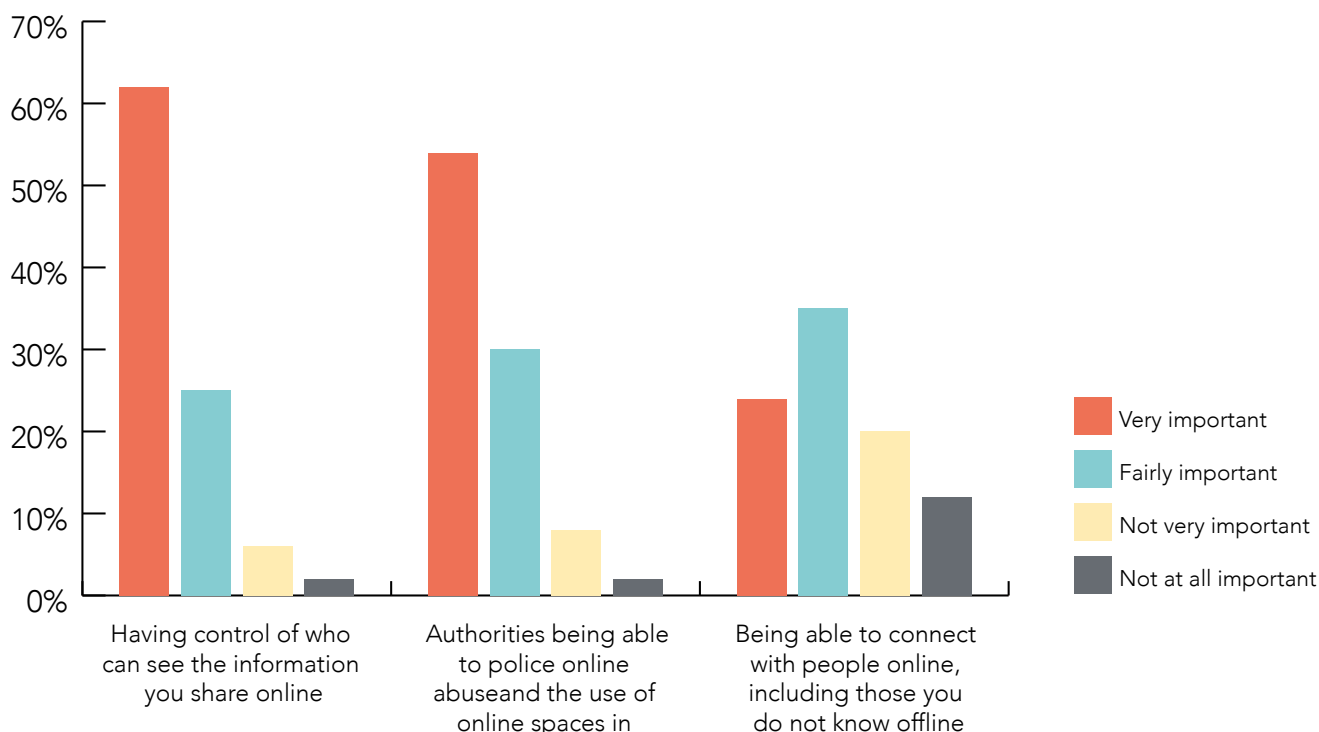
There is a clear desire and need for spaces which are designed to maximise user control of their information within them. Our polling found that 62% said having control of their information was very important to them, in contrast to 54% who said authorities' ability to police online spaces was very important and 24% who found building connections online very important. This indicates that private spaces may be the most valued, followed by semi-private spaces, followed by public spaces (according to the schema set out above). Our poll found that 38% of people would like content posted both on social media and in private communications to be end-to-end encrypted, and that 66% said that whether a space was encrypted or not was important to them in choosing whether they used a space. However, these preferences were not contextualised with the risk of harms within end-to-end encrypted spaces, and so respondents may not have had this in mind.

Increasing personal control over information is not without safety implications. Many platforms,

including WhatsApp, Facebook Secret Messenger, and Telegram, already offer end-to-end encryption, and there are plans to expand its use more widely - notably on Facebook Messenger.⁷⁶ Governments, including the UK, have called on Facebook not to go ahead with these plans without ensuring that "a means for lawful access to the content of communications" is preserved in order for CSEA and terrorism to be prevented, identified and prosecuted.^{77,78} Civil society groups have also expressed serious concern about the expansion of end-to-end encryption due to the restrictions it would place on law enforcement tackling online CSEA.^{79,80} By making end-to-end encryption the default, it has been estimated that '70% of Facebook's reporting - 12 million reports globally - would be lost [if Facebook implements encryption as planned].'⁸¹

Proposals to allow law enforcement to access even end-to-end encrypted messages have been put forward: if it were possible to achieve access in exceptional cases, in a principled way, based on

How important, if at all, are the following to you?



76. Thought this is likely to take several years - see Greenberg, A. Facebook Says Encrypting Messenger by Default Will Take Years. Wired, 2020. Available at <https://www.wired.com/story/facebook-messenger-end-to-end-encryption-default/> [accessed 03 August 2020]

77. Wong, J.C. US, UK and Australia urge Facebook to create backdoor access to encrypted messages. The Guardian, 2019. Available at <https://www.theguardian.com/technology/2019/oct/03/facebook-surveillance-us-uk-australia-backdoor-encryption> [accessed 03 August 2020]

78. The Irish News. UK claims Facebook encryption plan poses 'grave' risk to public safety. 2019. Available at <https://www.irishnews.com/magazine/technology/2019/12/23/news/uk-claims-facebook-encryption-plan-poses-grave-risk-to-public-safety-1798198/> [accessed 03 August 2020]

79. DCMS Sub-Committee on Online Harms and Disinformation. Oral evidence: Online Harms and Disinformation. House of Commons, 2020. Available at <https://committees.parliament.uk/oralevidence/459/pdf/> [accessed 03 August 2020]

80. NSPCC. Letter to Mark Zuckerberg. 2020. Available at <https://www.nspcc.org.uk/globalassets/documents/policy/letter-to-mark-zuckerberg-february-2020.pdf> [accessed 14 September 2020]

81. NCMEC, in US/UK/Aus Gov letter: Wong, J.C. US, UK and Australia urge Facebook to create backdoor access to encrypted messages. The Guardian, 2019. Available at <https://www.theguardian.com/technology/2019/oct/03/facebook-surveillance-us-uk-australia-backdoor-encryption> [accessed 03 August 2020]

legal authorisation, without unduly putting users at risk, this kind of access could mean a way of tackling serious harms without disproportionately affecting privacy.⁸² One such proposal has been made by Ian Levy and Crispin Robinson for allowing exceptional access: 'It's relatively easy for a service provider to silently add a law enforcement participant to a group chat or call... You end up with everything still being end-to-end encrypted, but there's an extra 'end' on this particular communication.'⁸³ This proposal also argues that without such access, reliance on vulnerability exploitation by law enforcement risks vulnerabilities not being disclosed and fixed, to the detriment of general security.⁸⁴

Allowing even for lawful access to encrypted information, however, poses a serious risk to the security of that information. An Open Letter responding to this proposal from a coalition of civil society, experts and tech companies, wrote that: 'if implemented, it will undermine the authentication process...introduce potential unintentional vulnerabilities, and increase risks that communications systems could be abused or misused.'⁸⁵ The letter described how access of this kind would pose particular risks to groups such as victims of gender-based violence and people at risk of violence from repressive states, and highlights that such a move could significantly undermine security through intentional or unintentional system changes. Vulnerability hoarding would also not be fully preventable.⁸⁶

As David Kaye, the UN Special Rapporteur on freedom of expression writes in his report on encryption online: 'intentionally compromising encryption, even for arguably legitimate purposes, weakens everyone's security online.'⁸⁷ He concludes that 'States should not restrict encryption and anonymity, which facilitate and often enable the

rights to freedom of opinion and expression... States should avoid all measures that weaken the security that individuals may enjoy online, such as backdoors, weak encryption standards and key escrows.'⁸⁸ These sentiments, namely that law enforcement may pursue legitimate aims through other methods, while preserving the security for people's private communications that is essential for user protection, have been echoed by Human Rights Watch (HRW).⁸⁹ Similarly, over 110 human rights groups globally, including HRW, the ACLU and Privacy International have called for the protection of the integrity of end-to-end encryption.⁹⁰ Privacy should not be seen as antithetical to protection, but as part and parcel of protecting people online.⁹¹ Widespread encryption use also provides cover to those using the technology to avoid detection, and whose use of niche encrypted apps, or enabling of encryption of particular conversations, may otherwise arouse suspicion.⁹²

Encryption protects people from harm; it also enables those conducting harm to evade detection. How do we approach resolving this tension?

We can seek to mitigate the harms which could arise from communication through the design of the space and the activities within the space - rather than seeking control over the contents of communications themselves. 'Privacy by design' and 'safety by design' mean that when online spaces are being designed, this should happen in consultation with experts to ensure that the technical infrastructure and user interfaces are optimised to promote privacy and safety. For instance, tech platforms and law enforcement already use a number of techniques to identify criminal behaviour on end-to-end encrypted platforms, including the identification of suspicious behaviour such as the creation of mass accounts,⁹³

82. Levy, I. and Robinson, C. Principles for a More Informed Exceptional Access Debate. Lawfare blog, 2018. Available at <https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate> [accessed 21 August 2020].

83. Levy, I. and Robinson, C. Principles for a More Informed Exceptional Access Debate. Lawfare blog, 2018. Available at <https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate> [accessed 21 August 2020].

84. Levy, I. and Robinson, C. Principles for a More Informed Exceptional Access Debate. Lawfare blog, 2018. Available at <https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate> [accessed 21 August 2020].

85. Franklin, S.B. and Thompson, A. W. Open Letter to GCHQ on the Threats Posed by the Ghost Proposal. Lawfare Blog, 2019. Available at <https://www.lawfareblog.com/open-letter-gchq-threats-posed-ghost-proposal> [accessed 21 August 2020]

86. Krahulcova, L. China tips the scale of global cybersecurity by hoarding vulnerabilities. Access Now, 2018. Available at <https://www.accessnow.org/china-tips-the-scale-of-global-cybersecurity-by-hoarding-vulnerabilities/> [accessed 10 September 2020]

87. Kaye, D. Report on encryption, anonymity, and the human rights framework. OHCHR, 2015. Available at <https://www.ohchr.org/en/issues/freedomofopinion/pages/callforsubmission.aspx> [accessed 03 August 2020]

88. Kaye, D. Report on encryption, anonymity, and the human rights framework. OHCHR, 2015. Available at <https://www.ohchr.org/en/issues/freedomofopinion/pages/callforsubmission.aspx> [accessed 03 August 2020]

89. Vesteinsson, K. Governments to Facebook: Stop Making Encryption Easy. Human Rights Watch, 2019. Available at <https://www.hrw.org/news/2019/10/04/governments-facebook-stop-making-encryption-easy> [accessed 24 August 2020]

90. Hall, J.L. Open Letter: Facebook's End-to-End Encryption Plans. Center for Democracy and Technology, 2019. Available at <https://cdt.org/insights/open-letter-facebooks-end-to-end-encryption-plans/> [accessed 03 August 2020]

91. Runnegar, C. Encryption and Law Enforcement Can Work Together. Available at <https://www.internetsociety.org/blog/2017/10/encryption-law-enforcement-can-work-together/> [accessed 10 September 2020]

92. Privacy Camp. "Actually, In Google We Trust"? A 'Deconstructing' Conversation on Russian Internet Activism. 2020.

Available at https://privacycamp.eu/?page_id=1949 [accessed 03 August 2020]; EFF. What Should I Know About Encryption? Surveillance Self-Defense, 2018. Available at <https://ssd.eff.org/en/module/what-should-i-know-about-encryption> [accessed 30 July 2020]

93. DCMS Sub-Committee on Online Harms and Disinformation. Oral evidence: Online Harms and Disinformation. House of Commons, 2020. Available at <https://committees.parliament.uk/oralevidence/459/pdf/> [accessed 03 August 2020]

examining metadata,⁹⁴ user reporting⁹⁵ and verifying the identity of those using the platform.⁹⁶ These kinds of techniques should be invested in, and transparently developed in consultation with and subject to review by child protection experts.

However, as these techniques operate at one level removed from the content of a message, methods have also been suggested for applying detection mechanisms for harmful data to encrypted messages, without weakening or breaking their encryption, or otherwise significantly compromising the privacy of the message.

Consider PhotoDNA, a technology currently used by Microsoft, Google, Facebook, Twitter and others to detect CSEA material uploaded to their platforms.⁹⁷ To work out whether an image is a known piece of CSEA material, PhotoDNA calculates a unique fingerprint for it, and compares this to the fingerprints of a large database of known abuse material, which is maintained by an American organisation, the National Centre for Missing and Exploited Children (NCMEC).⁹⁸ The system is designed to allow matches to be made even where an image has been resized, rotated or otherwise superficially altered. If a match is found, that message is flagged for review and appropriate action can be taken. Encryption poses a challenge to PhotoDNA as it is currently implemented, as it assumes that the server calculating the fingerprint for an image has access to the original image. If an image or video has been encrypted, the algorithm can't calculate its fingerprint.

There are potentially a couple of ways in which this detection could work without compromising privacy. The first is to detect CSEA material earlier, before it is encrypted. This would involve running the PhotoDNA algorithm on the device used to send the message, scanning any images present, and comparing their hashes to the database of known abuse material. Agencies checking the image against NCMEC's database would not see the image itself, but only the fingerprint - a string of letters and numbers.

This approach of 'on-device hashing' would preserve privacy - control of the information in a message is not ceded to a third party - but raises some serious questions around how it would be implemented. The exact process by which PhotoDNA works is presently not public knowledge - potentially with the reasoning that distributing a copy of the algorithm would allow people to test for loopholes, and find ways to evade detection. As cryptographer Matthew Green points out:

*"While it might be possible to cram [detection algorithms] onto a user's phone, it's hugely more difficult to do so on a billion different phones, while also ensuring that nobody obtains a copy of it."*⁹⁹

A second, more secure approach involves the use of 'secure, multi-party computation' (MPC) techniques, such as homomorphic encryption, which allow computation such as PhotoDNA to be carried out on encrypted data, without needing to parse the original image. This technique was described by a participant at our roundtable as being like: having a good idea what present you are getting for Christmas, looking at the parcels under the tree, and working out which present it is by size, shape and sound without having to unwrap and see what is inside any of the presents.¹⁰⁰ However, while there are promising advances being made in this area, cutting edge approaches are currently both untested at scale, require huge amounts of data transfer to work, and may not be compatible with as strong encryption of users' information.¹⁰¹

Given that employing these methods would mean that some information about the contents of a message would be shared with third parties, those messages would not technically be completely private, under our definition. However, they would be much closer to private than the standard 'semi-private' space we have defined, as the information users cede control of is limited to whether the contents of a message contain illegal content or not, rather than the contents themselves.

94. EFF, A Deep Dive on End-to-End Encryption: How Do Public Key Encryption Systems Work? Surveillance Self-Defense, 2018. Available at <https://ssd.eff.org/en/module/deep-dive-end-end-encryption-how-do-public-key-encryption-systems-work> [accessed 30 July 2020]

95. Newman, L.H. Encrypted Messaging Isn't Magic. Wired, 2018. Available at <https://www.wired.com/story/encrypted-messaging-isnt-magic/> [accessed 03 August 2020]; E&T. Facebook commits to end-to-end encryption in Messenger, despite government concerns. 2019. Available at <https://eandt.theiet.org/content/articles/2019/11/facebook-messenger-launching-broad-end-to-end-encryption-test-despite-protestations/> [accessed 03 August 2020]

96. Statt, N. Zoom says free users will get end-to-end encryption after all. The Verge, 2020. Available at <https://www.theverge.com/2020/6/17/21294355/zoom-security-end-to-end-encryptoin-beta-release-july-2020-new-feature> [accessed 03 August 2020]

97. Farid, H. Reining In Online Abuses. Technology and Innovation: 19, 2018, pp. 593-599. Available at <https://farid.berkeley.edu/downloads/publications/nai18.pdf> [accessed 03 August 2020]

98. This is within a database held by the US-based National Centre for Missing and Exploited Children, or 'NCMEC'.

99. Green, M. Can end-to-end encrypted systems detect child sexual abuse imagery? 2019. Available at <https://blog.cryptographyengineering.com/2019/12/08/on-client-side-media-scanning/> [accessed 03 August 2020]

100. With thanks to Fred Langford for this analogy. July, 2020.

101. Riazi, M. and others. XONN: XNOR-based Oblivious Deep Neural Network Inference. 2019, Table 6. Available at <https://eprint.iacr.org/2019/171.pdf> [accessed 03 August 2020]. Thanks also to Fred Langford for advising on this point. July, 2020.

There is thus an urgent need to test and find solutions which allow CSEA and terrorist activity to be detected, while preserving the protection of, privacy offered by and availability of end-to-end encryption.¹⁰²

LEGAL ACCESS TO PRIVATE COMMUNICATIONS

In other spaces (e.g. private messages) users may have a reasonable expectation that they control the information they share there, which should only be breached in exceptional circumstances.

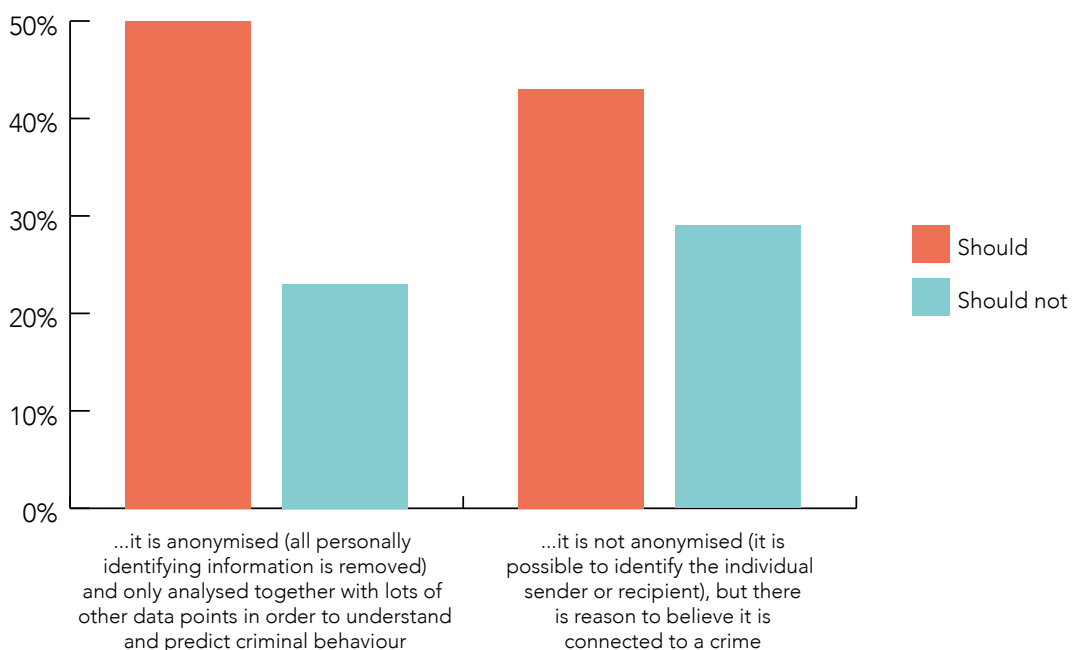
In general, information which is not accessible to law enforcement without using intrusive measures requires legal permission to be accessed. Currently, there are three main kinds of ‘private’ information that social media platforms such as Facebook and Twitter can hand over to law enforcement - the contents of communications, metadata of such communications, and personal, non-public information about the user who sent the communication. Both Facebook and Twitter will generally only hand over such information in response to a valid legal compulsion (such as a court order, subpoena or warrant, depending on the situation), except in particular emergency cases where immediate risk warrants disclosure of information.^{103,104}

Public attitudes are notably different for law enforcement access to online spaces compared to platform access. 50% think law enforcement should be able to access anonymised data about personal messages for the purposes of crime prevention. 39% would accept intelligence services accessing people’s personal messages if it meant people would be kept safer - a minority, but the highest proportion of public acceptance across different groups who could have such access.

84% said that authorities being able to police online abuse and the use of online spaces in criminal activities was important to them. When asked if law enforcement should have access to personal messages sent between individuals online if it was not anonymised, but there is reason to believe it is connected to a crime, 43% said they should, 29% said not, and 28% didn’t know. However, 67% said that they would be upset if intelligence services accessed the (non-anonymised) contents of their communications without them giving explicit permission.

This shows that there is support for tackling harms in private spaces, but more so when that support is targeted at specific people who are suspected of criminal activity, and less so when that would involve third parties accessing one’s own messages.

Do you think law enforcement should or should not be able to access personal messages between individuals sent online if:



102. CASM. Technology Briefing Series: Briefing 1: Online Child Sexual Abuse Imagery. Demos, 2018. Available at <https://demosuk.wpengine.com/wp-content/uploads/2018/01/Technology-Briefing-1-Online-CSAI-19.01-1.pdf> [accessed 03 August 2020]

103. Facebook. Information for Law Enforcement Authorities. Safety Center, 2020. Available at <https://www.facebook.com/safety/groups/law/guidelines/> [accessed 30 July 2020]

104. Twitter. Guidelines for law enforcement. Help Center, 2020. Available at <https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support#8> [accessed 30 July 2020]

Privacy has been taken to mean, in the US context particularly, 'presumptive immunity from regulation'.¹⁰⁵ Generally, the condition for accessing private spaces or private correspondence such as letters, is a legally obtained warrant - notably under the Fourth Amendment, in the US, which establishes 'the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures'.¹⁰⁶ In *Riley vs California*, one of a number of cases where a suspect's phone had been examined without warrant, which supplied information used as evidence against them, the US Supreme Court ruled that 'our holding, of course, is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search, even when a cell phone is seized incident to arrest'.^{107,108}

Thus, as with a private dwelling, it seems that no space is likely to be 100% private - that is, in your complete control, since given certain circumstances, that control is ceded to the authorities. Under RIPA, it has been ruled that even the act of handing over an encryption key, including those held in computer memory, does not violate the privilege of self-incrimination, and so someone can be compelled under criminal penalty to do so.¹⁰⁹

However, not all legal regimes are as robust in terms of protecting privacy in such cases as in these US examples, according to Privacy International, and changes to which legal standards law enforcement must adhere in collecting data, even from US-based platforms, have meant that the more stricter principles do not apply globally.¹¹⁰ The conditions under which warrants may be granted in the UK have been criticised for being too broad, and thus even the protection of warrants can be seen as insufficient to protect the privacy of information shared in certain spaces.¹¹¹ Privacy International have argued that the use of thematic warrants, rather than warrants targeted to individuals, is contrary to English common law and the European Convention on Human Rights'

protection of the right to privacy (though the Investigatory Powers Tribunal held that the use of thematic warrants was lawful.)^{112,113} Schneier also argues that it is relatively more difficult for an unauthorized individual to physically add a tap to a phone line than it is to exploit technical vulnerabilities of online spaces, meaning that a private space online may need higher levels of protection than a private space offline.¹¹⁴

Hence, as well as ensuring that there are spaces available which offer users a high level of control, any access by law enforcement to spaces which are reasonably expected to be private should be on a targeted basis with strong legal and democratic oversight. This means that users can be protected whilst allowing online crime to be tackled.

USER CONSENT FOR THIRD-PARTY ACCESS TO PRIVATE COMMUNICATIONS

In spaces where users have reasonable expectations that others may access and use their information, platforms and other actors may do so. This expectation must be managed through transparency and access and use should be on the basis of meaningful consent.

In some spaces, users may wish platforms to oversee the contents of their communications, in order to better moderate content, or target personalised content and ads. There was some support in our poll for content moderation by human (30%) or automated (32%) moderators in private messages. This is how a significant number of 'private messaging' services currently operate, including email and one-to-one chat messengers - but often without user knowledge or clarity.

In such spaces, the nature, purpose and governance of the oversight should be transparently communicated and users should be empowered to meaningfully consent to this usage of their messages. Platforms should not be able to defend practices on the grounds that users agreed to them where it is clear that the users would have a

105. Henkin, L. Privacy and Autonomy. *Columbia Law Review* 74:8, 1974, pp. 1410-1433. Available at https://www.jstor.org/stable/1121541?read-now=1&seq=16#page_scan_tab_contents [accessed 30 July 2020]

106. Dixon, H. B. Telephone Technology versus the Fourth Amendment. American Bar Association, 2016. Available at https://www.americanbar.org/groups/judicial/publications/judges_journal/2016/spring/telephone_technology_versus_the_fourth_amendment/ [accessed 03 August 2020]

107. Supreme Court of the United States. *Riley vs California*. 134 S. Ct. 2473, 2014. Available at <https://casetext.com/case/riley-v-cal-united-states-1> [accessed 03 August 2020]

108. Dixon, H. B. Telephone Technology versus the Fourth Amendment. American Bar Association, 2016. Available at https://www.americanbar.org/groups/judicial/publications/judges_journal/2016/spring/telephone_technology_versus_the_fourth_amendment/ [accessed 03 August 2020]

109. Fae, J. RIPA ruling closes encryption key loophole. *The Register*, 2008. Available at https://www.theregister.co.uk/2008/10/14/ripa_self_incrimination_ruling/ [accessed 03 August 2020]

110. Privacy International. PI response to confused governments' confusing declaration of war and victory on encryption. 2019. [accessed 03 August 2020] <https://privacyinternational.org/news-analysis/3245/pi-response-confused-governments-confusing-declaration-war-and-victory>

111. Privacy International. No, the UK Hasn't Just Signed a Treaty Meaning the End of End-to-End Encryption. 2019. Available at <https://privacyinternational.org/news-analysis/3242/no-uk-hasnt-just-signed-treaty-meaning-end-end-end-encryption> [accessed 03 August 2020]

112. Privacy International. The Queen on the application of Privacy International v. Investigatory Powers Tribunal (UK General Hacking Warrants). 2019. Available at <https://privacyinternational.org/legal-action/queen-application-privacy-international-v-investigatory-powers-tribunal-uk-general> [accessed 21 August 2020]

113. Privacy International. FAQ: Privacy International UK Supreme Court Judgment. 2019. Available at <https://privacyinternational.org/long-read/2898/faq-privacy-international-uk-supreme-court-judgment> [accessed 21 August 2020]

114. Schneier, B. Evaluating the GCHQ Exceptional Access Proposal. *Lawfare Blog*, 2019. Available at <https://www.lawfareblog.com/evaluating-gchq-exceptional-access-proposal> [accessed 21 August 2020]

reasonable expectation of privacy. Agreement may in these cases have been due to the complexity or vagueness of the terms of service or obfuscation of how platforms operate regards to the use of user information, e.g. for profiling and targeting.¹¹⁵

Currently, this understanding is not present. 69% of people in our poll said they considered sending an email to one person to be private - the highest proportion of any activities in online spaces we asked about. Even for an email, widely regarded as private, if not end-to-end encrypted (which many are not) the contents can be observed not only by the recipients but by the email provider. By contrast, 56% think that a one-to-one WhatsApp message is private, although WhatsApp messages are end-to-end encrypted, which offers a level of control which many email services do not.

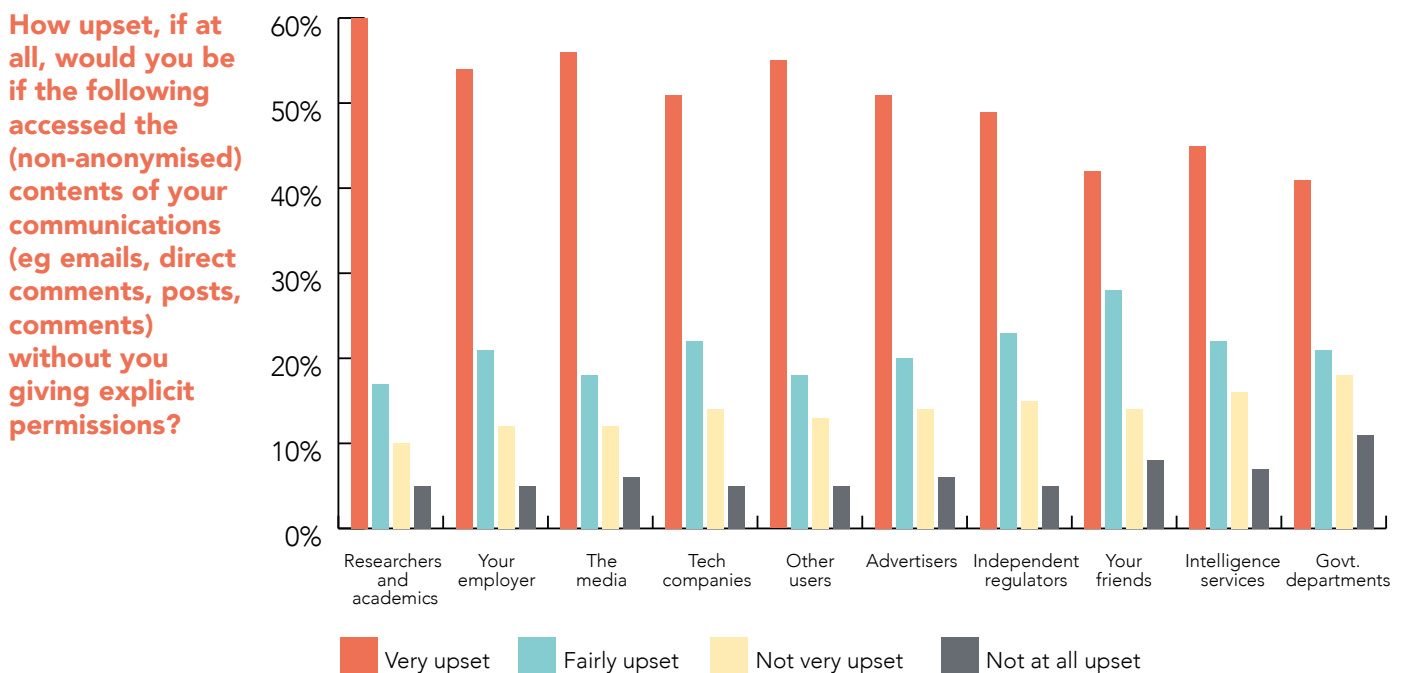
In our poll, a large number of respondents said that they did not know how to define a private space online. A few linked this to their lack of use of online spaces or familiarity with technology; others varied from 'not sure' to 'really have no idea'. This uncertainty indicates that users are not fully equipped by the platforms and services they use to have confidence in how spaces operate, and how their information is used:

I really have no idea, it is all too complicated
Male, 60+

I'm not sure as I don't use them
Female, 25-39

Users value the privacy of their information from the platforms that run the services they use. There are strong feelings that people's information shared in private spaces should not be accessed without their explicit permission. Our poll found that 73% said that they would be upset if tech companies accessed the (non-anonymised) contents of their communications without them giving explicit permission, with 51% saying they would be 'very upset' at tech companies doing so. 66% of people would not accept tech companies accessing private messages if it meant people would be kept safer - even though this is what tech companies are doing in many different spaces. 36% thought that platforms should not be able to access even anonymised data, when it is used only for commercial purposes.

Similarly, a YouGov poll for Solent University found that 63% of people said they would be uncomfortable with their messages or emails 'deciding what content (e.g. search results, news items, adverts, etc.) [they] see online.'¹¹⁶ This may be related to people's low trust in platforms (the YouGov poll found 71% of people said they did not trust Facebook to protect personal data)¹¹⁷, or due to expectations of control of private messages, as discussed above. Either way, this highlights the worrying lack of transparency around what content platforms access and for what reasons.

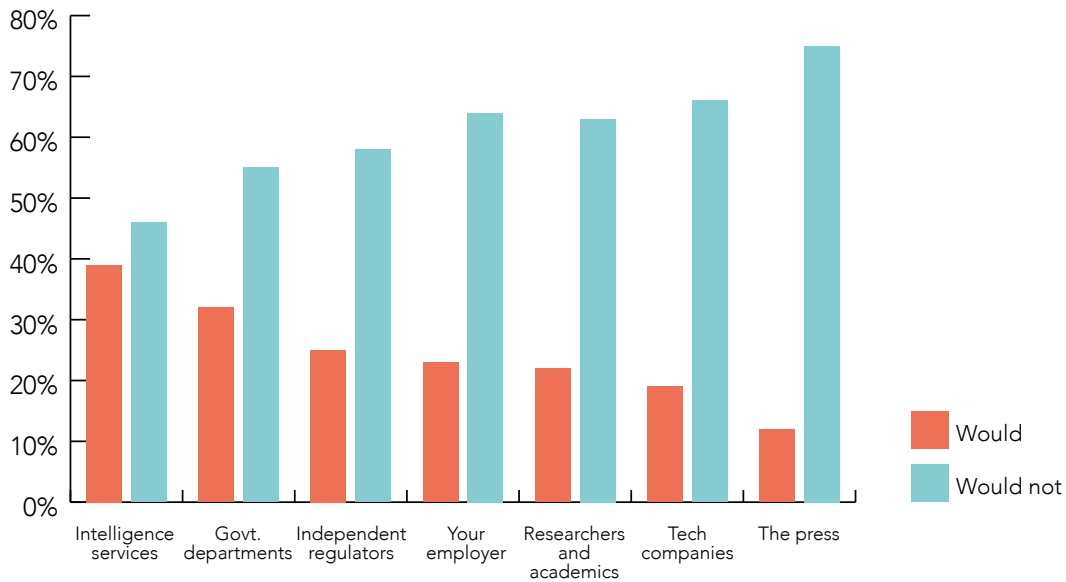


115. Thanks to participants in our roundtable for expanding this point. July, 2020

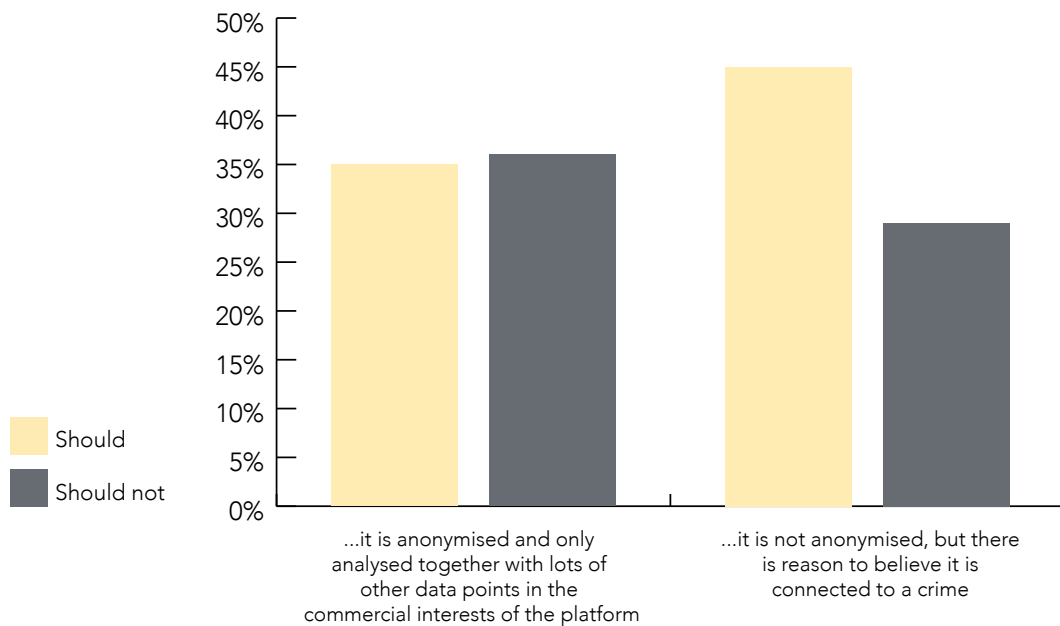
116. Benjamin, G. Digital Society: Regulating Privacy and Content Online. Solent University, 2020. Available at <https://digitalcultu.re/policy/digitalsociety/digitalsocietyreport.html#appendix> [accessed 10 September 2020]

117. Benjamin, G. Digital Society: Regulating Privacy and Content Online. Solent University, 2020. Available at <https://digitalcultu.re/policy/digitalsociety/digitalsocietyreporhtml#appendix> [accessed 10 September 2020]

For each of the following would you say you would or would not accept them being able to access people's private messages if it meant that people generally would be kept safer?



Do you think platforms should or should not be able to access personal messages between individuals sent online if:



Actions by platforms such as Facebook to allow users to select which groups of other users can see what they share are a necessary first step. However, other users are not the only parties who may be privy to information - privacy also requires privacy from those who run the systems.

Where information is being or may be accessed and used by third parties, the nature and conditions of this access, and what control the user can - or cannot - exercise over it must be communicated upfront and in plain terms to users. It should be clear what information is accessible about a post to other parties - text contents, images, metadata - and why this information is accessible: whether information is being accessed for commercial purposes or for harm reduction purposes. Devolved ownership or decentralisation of online spaces, such as that offered by spaces like Mastodon, may offer greater privacy of online spaces than the dominant platforms can, simply by virtue of their business models.¹¹⁸

There are also ramifications for this need for user understanding and consent for others who might access information that users share online. The results of our poll show that people would be most upset if researchers and academics accessed the non-anonymised contents of their communications without their explicit permission. The importance of clarity, consent and trust is often foregrounded in ethical guides for journalists operating in closed groups and should be incorporated into research practices more widely.^{119,120}

The kind of space that users operate in online affects the kind of activity they engage in and the kind of information they will share. Not having a transparent account of the parameters of the spaces

It should be clear what information is accessible about a post to other parties - text contents, images, metadata - and why this information is accessible: whether information is being accessed for commercial purposes or for harm reduction purposes.

they use means that people are unable to make fully informed choices, and so may modulate their behaviour in accordance with uncertainty about who can see their information. In turn, this process deprives them of the opportunity to fully participate in both private and public spaces in fruitful ways. Efforts to increase transparency, however, should not be simply assumed to have worked: providing people with information to interpret should be accompanied by proactive measures to help users, especially those who might be less digitally included, engage with the substance of what that information means for them.¹²¹

Debates on privacy online often focus on the need to protect end-to-end encryption, and indeed, the guarantees that technical security offers to users are crucial. However, the fact of accessibility to the contents of communications does not mean that users have no expectation of privacy, from platforms as well as other users, and so should not mean that users are not offered any privacy. Platforms should thus have a burden of proof to demonstrate, where they are accessing people's messages for commercial use, that their users have no reasonable expectation that that information is private from the company. This would include, but not be limited to, clear terms of service.

118. Pers. comm., 2020

119. Frankel, M. The promises and pitfalls of reporting within chat apps and other semi-open platforms: A journalist's guide. Nieman Lab, 2018. Available at <https://www.niemanlab.org/2018/07/a-journalists-guide-to-the-promises-and-pitfalls-of-reporting-within-open-and-closed-and-semi-open-platforms/> [accessed 30 July 2020]

120. Wardle, C. First Draft's Essential Guide to Closed Groups, Messaging Apps and Online Ads. First Draft, 2019. Available at <https://firstdraftnews.org/latest/closed-groups-messaging-apps-and-online-ads-the-new-battlefields-of-disinformation/> [accessed 30 July 2020]

121. Thanks to participant roundtables for this point, July, 2020.

PART 4

RECOMMENDATIONS

THE NEED FOR PROTECTED SPACES

- End-to-end encryption as a tool for ensuring privacy should be protected. In our view, current proposals for exceptional access do not provide adequate technical protection for the rights of users against extrajudicial access by state or non-state actors. Therefore, alternative social and technical solutions to the problems of illegal content in end-to-end encrypted spaces should be invested in and built through collaboration and open discussion between government, tech platforms and civil society.
- The government, and technology firms should urgently fund research into improving techniques which allow for processing needed to prevent harm without requiring decryption. This could form part of a duty of care on platforms to demonstrate they are taking meaningful action on online harms occurring in end-to-end encrypted spaces. To limit the danger that powerful detection technologies such as PhotoDNA are employed to detect other forms of expression, those putting them to use must be clear about the database to which images are being compared. If companies are unwilling to do this, redress could be sought through regulation.
- When online spaces are being designed, this should happen in consultation with experts to ensure that the technical infrastructure and user interfaces are optimised to promote privacy and safety.
- Where platforms have access to information and the contents of communications, how they fulfil a statutory duty of care will be different from those cases in which they do not. Platforms and regulators should use a graded understanding

of the degrees of privacy a space has in order to inform the kinds of responses to online harms that would be appropriate in that space.

LEGAL ACCESS TO PRIVATE COMMUNICATIONS

- Platforms should provide data relating to people's personal communications (including content or metadata) to law enforcement only in a targeted way, in response to an authorised request with judicial oversight. Legal frameworks for authorising such access must be consistent with human rights law.

USER CONSENT FOR THIRD-PARTY ACCESS TO PRIVATE COMMUNICATIONS

- Platforms should have a burden of proof to demonstrate, where they are accessing people's messages for commercial use, that their users do not have a reasonable expectation that that information is private from the company. This would include, but not be limited to, clear terms of service.
- Platforms should ensure that information about the control and accessibility of spaces, including moderation of content, is available to users of their services, who should be empowered to fully engage with and meaningfully consent to the terms offered.¹²²
- There should be independent oversight of how user control of information in a private space is maintained and this should be explained before and after a user has entered into an agreement with a platform.
- Where activity as well as content - people's clicks, searches and so forth - is being tracked, this should also be transparent.¹²³

122. Farrall, K.N. Global Privacy in Flux: Illuminating Privacy across Cultures in China and the U.S. *International Journal of Communication* 2, 2008, 993-1030. Available at <https://ijoc.org/index.php/ijoc/article/viewFile/370/228> [accessed 30 July 2020]

123. Carmi, E. Media Distortions: Understanding the Power Behind Spam, Noise, and Other Deviant Media. *Digital Formations*. Available at <https://doi.org/10.3726/b15334> [accessed 30 July 2020]

- Opt-outs of third party access to data should be as simple to execute as changing the privacy settings of a post from 'public' to 'friends only'.
- Companies which met these standards, as judged by an independent body, could be eligible for a 'kitemark' that indicated their appropriate management of private spaces online.
- Researchers, when seeking to access data from platforms should be transparent about their activities and intentions, and give users the option, where possible, to retain or consent to hand over control of their information.

INTERNATIONAL STANDARDS

- There is a need for a framework of standards on protecting private and public spaces online and combating harms within them to which platforms are held to be defined internationally, by international institutions, in collaboration with civil society.¹²⁴ This collaboration could be funded by an additional digital services tax on platforms gathered by national governments, and contributed to an international institution, such as the UN.

124. Thanks to participants at the roundtable for raising this point. July, 2020

APPENDIX

POLLING RESULTS

Base: Nationally representative sample of 1,035 UK adults interviewed online 5 May 2020 - 8 May 2020. Data are weighted to the profile of the population.

Q1. HOW FREQUENTLY, IF AT ALL, DO YOU DO THE FOLLOWING?

	All the time	Often	Sometimes	Rarely	Never
	%	%	%	%	%
Message one person on WhatsApp	32	25	13	5	25
Send an email to one person	29	33	27	9	3
Message one person on Facebook Messenger	20	24	20	8	28
Post a message on your Facebook timeline	11	18	23	16	32
Message a group on Facebook Messenger (e.g. of 10 people)	10	17	16	13	45
Direct message one person on Instagram	10	13	13	9	56
Message large groups on Whatsapp (e.g. more than 100 members)	9	13	13	8	58
Post on a public Instagram account	8	10	15	9	58
Post on a private Instagram account	8	12	15	8	57
Hold a group call on Google Hangouts	4	9	12	8	67

Q2. IN GENERAL, HOW PRIVATE DO YOU THINK THE CONTENT SHARED IS WHEN SOMEONE DOES THE FOLLOWING?

	Very private	Fairly private	Not very private	Not at all private	Don't know	Private (comb.)	Not private (comb.)
	%	%	%	%	%	%	%
Sends an email to one person	31	38	14	7	9	69	21
Messages one person on WhatsApp	24	32	16	11	17	56	27
Messages one person on Facebook Messenger	17	36	19	14	14	53	33
Direct messages one person on Instagram	14	29	18	15	24	53	33
Posts on a private Instagram account	10	30	21	16	23	40	37
Messages a group on Facebook Messenger (e.g. of 10 people)	6	24	29	25	15	31	54
Posts a message on their Facebook timeline	9	16	29	33	12	25	62
Messages large groups on Whatsapp (e.g. more than 100 members)	6	16	25	35	18	22	60
Holds a group call on Google Hangouts	5	17	24	26	28	22	50
Posts on a public Instagram account	4	11	19	45	21	15	64

Q3. FOR EACH OF THE FOLLOWING FEATURES OF AN ONLINE SPACE, WOULD IT MAKE YOU THINK IT WAS MORE OR LESS PRIVATE, OR WOULD IT MAKE NO DIFFERENCE?

By 'online space' we mean things like social media (e.g. Facebook), forums (e.g. Reddit) or private messaging platforms (e.g. WhatsApp).

	Much more private	Slightly more private	No difference	Slightly less private	Much less private	Don't know	More private (comb.)	Less private (comb.)
	%	%	%	%	%	%	%	%
The content of posts/messages is end-to-end encrypted	24	29	22	5	2	18	53	7
New members of a space have to be added by an existing member	10	28	31	9	6	16	38	15
The space is small (e.g. 10 or fewer members)	10	28	33	9	3	16	38	12
I know everyone else in the space	13	24	34	7	6	16	37	13
Content is moderated by the platform using human moderators	9	22	32	11	8	18	32	19
Content is moderated by the platform using automated software	7	22	33	10	7	21	29	17
Everyone in the space uses their real name	9	16	33	11	15	16	25	26
The space can be searched for and found by anyone using a conventional search engine	7	11	26	10	30	16	18	40
The content of posts/messages can be seen by anyone outside of the space without joining	7	11	23	9	35	15	18	44

Q4. WHICH OF THE FOLLOWING FEATURES ARE CLOSEST TO HOW YOU PERSONALLY WOULD PREFER ONLINE SPACES YOU USE TO BE?

By social media, we mean for example posting on Facebook or Instagram. By private messaging platforms, we mean for example Facebook Messenger or WhatsApp.

	I would like this feature for both social media and private messaging	I would like this feature for social media, but not private messaging	I would like this feature for private messaging, but not social media	I would not like this feature either for private messaging or social media	Don't know
	%	%	%	%	%
I know everyone else in the space	38	15	17	7	24
The content of posts/messages is end-to-end encrypted (so only the sender and the recipient can read them)	38	14	16	8	24
Everyone in the space uses their real name	35	17	16	8	23
New members of a space have to be added by an existing member	29	20	15	11	25
The space is small (e.g. 10 or fewer members)	25	18	18	8	31
Content is moderated by the platform using automated software	19	23	13	14	21
Content is moderated by the platform using human moderators	18	25	12	17	29
The space can be searched for and found by anyone using a conventional search engine	13	19	11	33	24
The content of posts/messages can be seen by anyone outside of the space without joining	13	15	11	39	22

Q5. HOW IMPORTANT, IF AT ALL, ARE THE FOLLOWING IN CHOOSING WHETHER AND HOW YOU USE ONLINE SPACES?

	Very important	Fairly important	Not very important	Not at all important	Don't know	Important (comb.)	Not important (comb.)
	%	%	%	%	%	%	%
Whether or not the content of posts/messages can be seen by anyone outside of the space without joining	40	29	11	5	16	69	16
Whether or not you know everyone else in the space	34	33	14	5	14	67	19
How, if at all, the content of posts/messages is monitored	32	34	13	4	16	67	17
The restrictions on how new members can be added	34	34	13	4	15	67	17
Whether or not the content of posts/message is encrypted	36	30	13	4	17	66	17
Whether or not everyone in the space uses their real name	29	36	16	6	14	64	22
Whether or not the space can be searched for and found by anyone using a conventional search engine	31	28	17	6	18	59	23
How many people are in the space	22	32	23	7	15	55	30

Q6. WHICH OF THE FOLLOWING COMES CLOSEST TO YOUR VIEWS?

	%
People should not be allowed to post content that most people would view as harmful in either public or private online spaces	62
People should be allowed to post content that most people would view as harmful in private online spaces, but not public online spaces	16
People should be allowed to post content that most people would view as harmful in public online spaces, but not private online spaces	12
People should be allowed to post content that most people would view as harmful in both public and private online spaces	10

Q7. DO YOU THINK LAW ENFORCEMENT SHOULD OR SHOULD NOT BE ABLE TO ACCESS PERSONAL MESSAGES BETWEEN INDIVIDUALS SENT ONLINE IF:

	Should	Should not	Don't know
	%	%	%
...it is anonymised (all personally identifying information is removed) and only analysed together with lots of other data points in order to understand and predict criminal behaviour	50	23	27
...it is not anonymised (it is possible to identify the individual sender or recipient), but there is reason to believe it is connected to a crime	43	29	28

Q8. DO YOU THINK PLATFORMS SHOULD OR SHOULD NOT BE ABLE TO ACCESS PERSONAL MESSAGES BETWEEN INDIVIDUALS SENT ONLINE IF:

	Should	Should not	Don't know
	%	%	%
...it is anonymised and only analysed together with lots of other data points in the commercial interests of the platform	35	36	29
...it is not anonymised, but there is reason to believe it is connected to a crime	45	29	26

Q9. DO YOU THINK RESEARCHERS SHOULD OR SHOULD NOT BE ABLE TO ACCESS PERSONAL MESSAGES BETWEEN INDIVIDUALS SENT ONLINE IF:

	Should	Should not	Don't know
	%	%	%
....it is anonymised and only analysed together with lots of other data points to help understand and predict important social phenomena, like how false information spreads	36	36	28
...it is not anonymised, but there is reason to believe it is connected to a crime	44	33	23

Q10. WHICH OF THE FOLLOWING COMES CLOSEST TO YOUR VIEWS?

	%
Online platforms should always prioritise safety over freedom	40
Online platforms should usually prioritise safety over freedom	19
Online platforms should prioritise safety and freedom equally	35
Online platforms should usually prioritise freedom over safety	3
Online platforms should always prioritise freedom over safety	4

Q11. HOW IMPORTANT, IF AT ALL, ARE THE FOLLOWING TO YOU?

	Very important	Fairly important	Not very important	Not at all important	Don't know	Important (comb.)	Not important (comb.)
	%	%	%	%	%	%	%
Having control of who can see the information you share online	62	25	6	2	6	87	8
Authorities being able to police online abuse and the use of online spaces in criminal activities	54	30	8	2	7	84	10
Being able to connect with people online, including those you do not know offline	24	35	20	12	9	60	31

Q12. HOW IMPORTANT, IF AT ALL, ARE THE FOLLOWING TO YOU?

	Very upset	Fairly upset	Not very upset	Not at all upset	Don't know	Upset (comb.)	Not upset (comb.)
	%	%	%	%	%	%	%
Researchers and academics	60	17	10	5	8	77	16
Your employer	54	21	12	5	9	74	17
The media	56	18	12	6	8	74	18
Tech companies	51	22	14	5	8	73	19
Other users	55	18	13	5	8	73	18
Advertisers	51	20	14	6	8	72	21
Independent regulators	49	23	15	5	8	72	20
Your friends	42	28	14	8	7	71	22
Intelligence services	45	22	16	7	10	67	23
Government departments	41	21	18	11	9	62	19

Q13. FOR EACH OF THE FOLLOWING WOULD YOU SAY YOU WOULD OR WOULD NOT ACCEPT THEM BEING ABLE TO ACCESS PEOPLE'S PRIVATE MESSAGES IF IT MEANT THAT PEOPLE GENERALLY WOULD BE KEPT SAFER?

	Would	Would not	Don't know
	%	%	%
Intelligence services	39	46	15
Government departments	32	55	13
Independent regulators	25	58	17
Your employer	23	64	13
Researchers and academics	22	63	15
Tech companies	19	66	15
The press	12	75	13

Q13. FOR EACH OF THE FOLLOWING WOULD YOU SAY YOU WOULD OR WOULD NOT ACCEPT THEM BEING ABLE TO ACCESS YOUR PRIVATE MESSAGES ONLINE IF IT MEANT THAT YOU PERSONALLY WOULD BE KEPT SAFER?

	Would	Would not	Don't know
	%	%	%
Your employer	24	61	16
Tech companies	23	62	15
The press	13	72	15
Researchers and academics	22	62	16
Independent regulators	28	55	16
Intelligence services	39	45	16
Government departments	32	50	18

DEMOS

PUBLISHED BY DEMOS OCTOBER 2020

© DEMOS. SOME RIGHTS RESERVED.

15 WHITEHALL, LONDON, SW1A 2DD

T: 020 3878 3955

HELLO@DEMOS.CO.UK

WWW.DEMOS.CO.UK