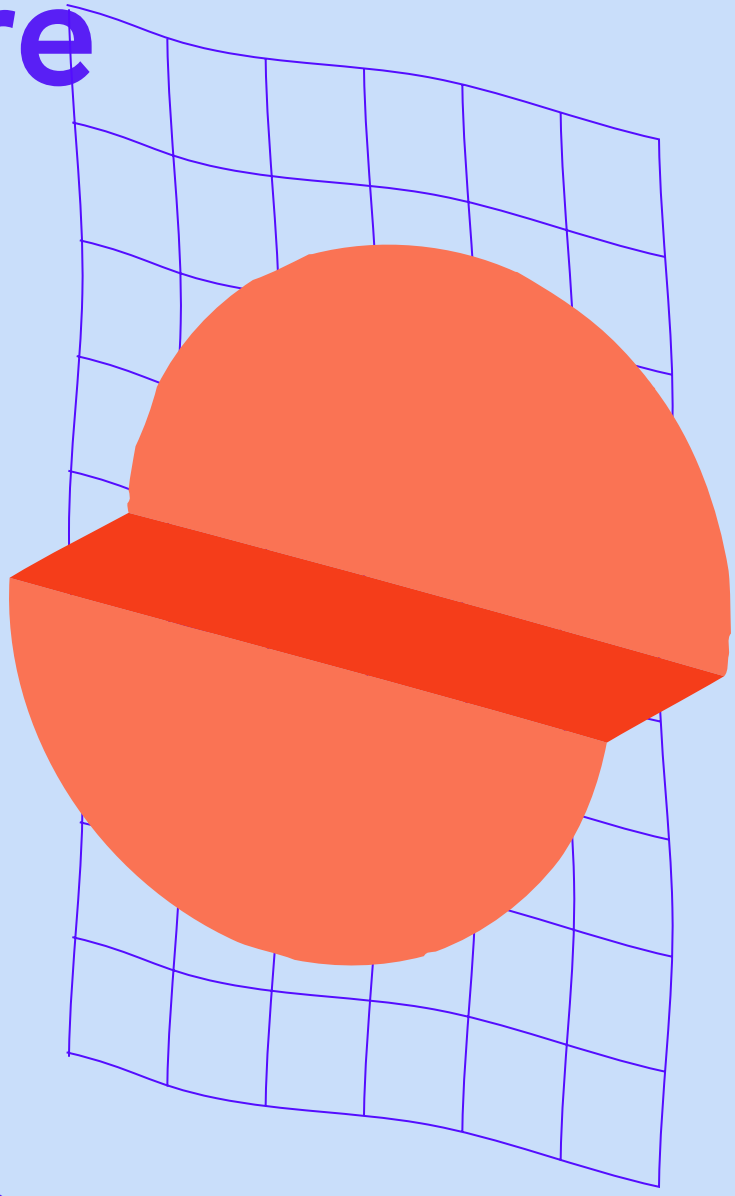
Welcome_

Civic Signals

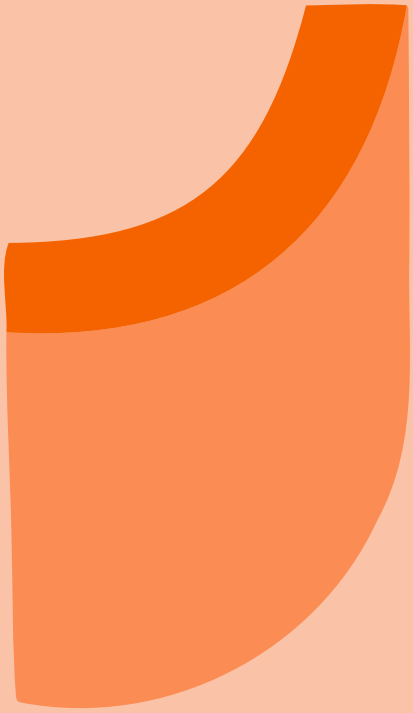
Keep people's information secure



This signal is part of Civic Signals, a larger framework to help create better digital public spaces. We believe it's a platform's responsibility to design the conditions that promote ideal digital public spaces. Such spaces should be designed to help people feel Welcome, to Connect, to Understand and to Act. These four categories encompass the 14 Civic Signals.

Table of contents

At a glance



Information security means the preservation of confidentiality and the integrity and availability of information.

Why It Matters

When information is leaked, people can be blackmailed, embarrassed or defrauded, or have their identity stolen. The organization that lost the information could be fined, or find itself the target of a class action suit. Companies who incur data breaches will suffer reputational damage, their competitive edge may be affected, and often they see drops in their share price performance.

> *You need to know how to block private information. Your setting has to be the highest security setting for any social media."*
> *– Kumanan, Malaysian focus group participant*

Putting the Signal Into Practice

- The National Institute of Standards and Technology (NIST) recently issued guidance explaining that passwords should actually not be complex, with length now being recommended. Moreover, passwords should not expire automatically, and should only be changed if the password owner is concerned that the password has been leaked. https://pages.nist.gov/800-63-3/sp800-63b.html

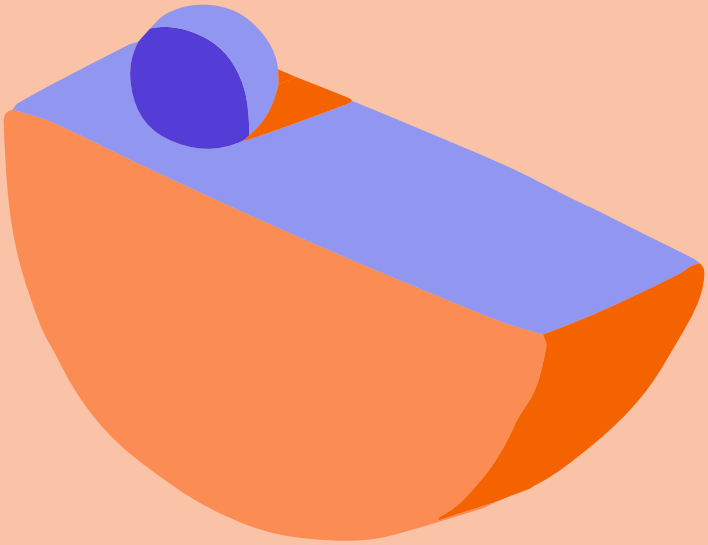
- Twitter, Paypal and Google all offer their customers two-factor authentication (2FA), which requires a code that customers receive via a separate channel such as their phone. An overview of other companies offering 2FA is here: https://www.pcmag.com/how-to/two-factor-authentication-who-has-it-and-how-to-set-it-up

- Many phones are simply too cumbersome to update – requiring that they be plugged in, that the phone not be in use, and so on. This makes it more likely that people will not download important security updates. Google appears to be making Android updates easier, though many phone manufacturers are not yet on board: https://www.techradar.com/news/google-wants-to-make-android-updates-easier-than-ever

- Organizations should also have cyber security insurance so that if they do experience a breach, the insurance company can help them to recover and also offer assistance to affected customers. Some guidelines on buying cybersecurity insurance can be found here: https://www.wsj.com/articles/the-ins-and-outs-of-cyber-security-insurance-11559700180

- Security and privacy policies should be written so that people can actually understand them. Cybersecurity researchers Karen Renaud and Lynsay Shepherd provide guidance. https://rke.abertay.ac.uk/en/publications/how-to-make-privacy-policies-both-gdpr-compliant-and-usable

Literature review



By Karen Renaud,
Abertay University

What the Signal Is

The International Organization for Standardization defines information security as "Preservation of confidentiality, integrity and availability of information."

Information security is thus related to the so-called "CIA properties." If information is secure, it is *confidential*, it has *integrity* and it is *available* to those who have the rights to access it.

Confidentiality ensures that only authorized individuals can access the information, and that their permissions are limited to what they require. For example, some individuals will only be able to read information, while others may be allowed to make changes.

Preserving *integrity* requires the system to protect information from unauthorized changes, and these include both intentional and malicious alterations as well as genuine mistakes.

Availability ensures that information is available and accessible to authorized users. When information is unavailable it impedes normal organizational functioning. Given that governments and companies have moved much of their service provision online, someone who can no longer use their

information may not be able to file their tax return, access their bank account, or share personal photos with family members.

Consider how the CIA properties could be compromised. Someone's password could be leaked or guessed, allowing another person to impersonate them – this violates *confidentiality*. If the impersonator changes or deletes the information, its *integrity* is suspect. Finally, if a hacker installs malware or a virus on a computer and encrypts all the files, the *availability* of the information is compromised.

These examples all demonstrate deliberate efforts to attack the security of information. Yet information can also be compromised in other ways. If someone knocks water over their computer, the information they hold on the hard drive will probably be destroyed and will no longer be *available*. If someone loses their computer, the *confidentiality* of the information held on that computer might well be compromised. Finally, if an undetected software bug makes unexpected changes to stored information, *integrity* has been compromised. These three dimensions are depicted in Figure 1.

The most essential principle in ensuring that these core properties of information are upheld is to control access to information. This is a two-step process. When someone wants to access information,

Step 1: They identify themselves and provide proof that they are entitled to claim that identity.

Step 2: The system restricts their access to the information they are authorized to access.

Related Concepts

Cyber Security: Information security is increasingly referred to as "cyber security." These two terms, while strongly related, are different. Information security applies to the securing of information across all contexts, ranging from paper to computerized records. Cyber security, on the other hand, refers to the securing of personal information stored on devices connected to the internet, or transmitted via the internet. A full explanation is provided by information security experts Basie von Solms and Rossouw von Solms. They explain that cyber security is contained within information security, and cyber security has additional dimensions related to the connectivity of devices to the internet.

Cyber Safety: A strongly related concept is "cyber safety." Many people conflate information security and cyber safety, but they are actually subtly different. While information security is related to the security of information and devices, cyber safety is related to the *safety* of the individual making use of the computer. Psychologist Tanya Byron explains that cyber safety is related to the *content* users see, their own personal *conduct* online and the *contact* made between users in the online world. These three dimensions are depicted in Figure 1. The preservation of cyber safety might rely on the deployment of traditional information security measures, but the risk is to the human in this case, making it a very different concept. We address cyber safety in the Civic Signal of Ensure People's Safety.

Information security and cyber safety share one characteristic: It is impossible for information to be 100% secure and it is

equally impossible for the user to be 100% safe while online. This reality is paralleled in the physical world. It is impossible to live without risk. We all have to do our best to mitigate the most pertinent risks, and then tolerate or avoid the rest.

Privacy: The other related concept is "privacy." This is linked to confidentiality, but, again, is different. Alan Westin, a public law and government expert, explains that "privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others". These three dimensions are depicted in Figure 1.

Privacy is an individual concern and a human right, as laid out by the United Nations Charter in 1948. People have the right to decide whether or not they grant access to their personal data. If they do decide to grant such access to an organization, the organization has a duty to keep such information confidential. In many countries, a failure to do so could lead to punitive fines being imposed, with the European Union's General Data Protection Regulation (GDPR) being a case in point.

Privacy is personal, while confidentiality is an organizational concern. Cyber privacy, once again, refers to the privacy of personal information stored and transmitted via the internet.

There is a common pattern in how systems grant access to information. A person might be asked for some personal or sensitive information. The requester could be a company, a doctor or an employer. If the person has the right to privacy, he/she has the right to make a decision about whether or not to divulge this information. He or she could decide to accede to the request or deny it. When privacy is violated, the company will automatically harvest the information, without asking for, or gaining, the information owner's permission.

It has become very difficult to preserve cyber privacy in the era of the Internet of Things (IoT). These devices are connected to the internet, and enhance personal convenience. They also gather very personal information about how we live our lives and are able to violate our privacy to an unprecedented degree.

While the need for information security is well understood, it is a lot harder for individuals to take their cyber privacy seriously. Even if people say they are concerned about their privacy, they generally do not take the actions required to preserve it. This is so even if they are shown evidence of privacy violations. This phenomenon, referred to as the "privacy paradox," has been demonstrated in the IoT domain by computer scientists and privacy researchers Noura Aleisa and Karen Renaud with information security governance expert Ivano Bongiovanni.

Figure 1[1] compares and contrasts the three

1 Figure 1: Information Security, Privacy and Cyber Safety

core concepts to summarize the discussion so far.

Why It's Important

If information is not secured, the organization that lost that information could be fined, or find itself the target of a class action suit. For the person whose information has been leaked, the consequences could be severe. Someone could use the information to blackmail or embarrass them, to steal their identity or to defraud them.

Companies who incur data breaches will suffer reputational damage and their competitive edge may be affected. This is likely to last for a long time, with the Equifax data breach being a good example. The personal and financial details of 143 million customers were lost. This happened in 2017, and the court cases are still ongoing in 2020.

Tech writer and privacy advocate Paul Bischoff analyzed the long-term performance of companies who experienced large data breaches, and discovered that they underperformed their rivals in the long term. Companies that leak credit card details see larger drops in their share price performance.

How We Can Move the Needle

To maintain organizational information security requires a risk management approach. Risk can be managed in four ways: organizations can mitigate, transfer, tolerate, or avoid.

Mitigation: Various measures are deployed to reduce vulnerabilities or to cope if the threat becomes reality. A range of technical measures should be used on organizational systems. There are basic hygiene aspects, such as the installation of anti-virus software on all machines and the making of regular backups (ensuring availability). Organizations should store all their data in encrypted format so that if a hacker does break through their defenses, the confidentiality and integrity of the data will not be lost. Software patches are issued regularly by operating system providers – it is essential for these to be applied as soon as they are issued.

The WannaCry malware attack of 2017 succeeded largely because these updates were not carried out, and a number of computers across Europe were vulnerable and could be breached.

On the employee side, the use of information security policies is common, but a mere policy is not going to be sufficient. This is especially true if the policy tells people to do things that are impossible. For example, employees are often told to (1) choose strong (i.e. complex) passwords, (2) never write them down, and (3) change them regularly. This is problematic for two reasons:

It is impossible to comply when people have dozens of passwords to manage, as Microsoft's Principal Researcher Cormac Herley points out. Computer scientist Karen Renaud argued, in 2012, that people are not deliberately thwarting rules but rather that they cannot comply with all the rules, especially those related to passwords.

These are also outdated rules. In 2017, the National Institute of Standards and Technology (NIST) published a report

which explained that passwords should actually not be complex, with length now being recommended. Moreover, passwords should not expire automatically, and only be changed if the password owner is concerned that the password has been leaked. The latest advice also recommends writing down passwords and securing the record or, even better, using a password manager. The best thing any organization can do is to issue all staff with a free password manager. These are relatively inexpensive and an easy way of improving security.

It is important that security not prevent employees from achieving their goals. So, for example, if employees are working to tight deadlines they might want to take a document home to work on it. If the organization bans the use of USB sticks and disables all USB ports, it is likely that the employee will find another way to take the file home. He might email it to himself, which is very insecure, and then the security measure has actually reduced security.

Organizations should consider the tasks their employees have to carry out. If they ban one enabling technology, they should always replace it with a secure technology which is equally easy to use. In this case, the organization could provide cloud storage, and VPN access when they outlaw the use of USB thumb drives.

Transfer: The risk is transferred, either by outsourcing the activity that is deemed to be too risky, or by insuring against the eventuality. For example, some organizations believe that it is too risky to store their customers' credit card numbers, so they use another service such as Paypal, essentially outsourcing the risky activity. Another example is the use of cloud-based services to store, back up, and maintain files.

Tolerate: In some cases, there is no way to reduce the threat in a cost effective and feasible way, so it is tolerated. During the COVID-19 pandemic, many of us worked from home, which meant people took work computers out of secured environments and connected to their own WiFi networks, which may not have been properly secured. The alternative would have been to lose their labor altogether, which was clearly not possible.

Avoid: The risky activity is prevented. For example, some organizations disable all USB ports on their computers so that no one can plug in a USB thumb drive. This prevents USB drives, which might well have malicious software on them, from infecting their computers.

Achieving information security in a modern era when almost all information is stored digitally has two dimensions: technological and human-related.

There are many technological measures deployed specifically to block those seeking access to information they are not authorized to see. Recently machine learning techniques have been used to detect and put a stop to the activities of intruders. Yet technology, while necessary, is not sufficient. Phishing attempts, for instance, require recipients to be aware of and not fall for the attempts.

On the human side, people want to believe that they are less vulnerable to risks than they actually are. This may lead them to be careless or complacent and neglect to take actions they ought to take to secure their information. Reformed hacker Kevin Mitnick and freelance author William Simon published one of the first books on social engineering in 2003, detailing a

range of techniques used by hackers and social engineers to persuade employees to divulge confidential information to them. They highlight the need to make employees aware of these kinds of deceptions so that forewarned becomes forearmed.

Some companies have implemented two-factor authentication to help people secure their information. Twitter, Paypal and Google all offer this to their customers. Essentially, when a customer logs in, they receive a code via another channel, perhaps a text message to their phone. They then enter this code to be permitted to enter the website. This means that if they click on a phishing message and accidentally give away their credentials, the hacker will still not get into their account because they don't have access to their smartphone.

Other organizations simply email people a link every time they want to log in, removing the need for them to provide a password at all. This makes it even more important for the email account to be protected by a strong password, however.

In the organizational context, because employees have legitimate access to information, they may be targeted by outsiders attempting to persuade them to divulge information, or to carry out some actions on the outsider's behalf. This is called *social engineering*. It is very important for organizations to ensure that their employees are aware of the risks and have the requisite skills to act securely and specifically to resist social engineering attempts.

Moreover, it is crucial for systems and processes to be designed so that employees are able to behave securely, as first highlighted by computer scientists Anne Adams and Martina Angela Sasse in 1999.

While technological solutions to preserve information security are improving all the time, humans behaving insecurely remains a conundrum. User experience designer Ryan West has suggested a number of ways in which we can improve human security behaviors, including:

Understanding Risk: We should help people to understand the actual risk of their information security being compromised. The problem is that security is something of an abstract concept, so we have to come up with innovative ways to help people to understand it in more concrete ways. For example, usable security academics Melanie Volkamer, Karen Renaud and Benjamin Reinheimer developed a system called TORPEDO. When this system finds a link in an email, it disables the link and issues an informative message to the user. If the link looks deceptive, the system will include a warning about the dangers of clicking on the message. This helps the user to avoid being deceived.

Some browsers, like Chrome, will also warn users if they attempt to access a site that is known to be malicious. These warnings are particularly effective because they are "just-in-time" – issued as and when the person needs the warning.

A proviso is that it is important not to habituate users to warnings, because then they are relegated to the "noise" that inhabits our daily lives and will be ignored. Warnings must be accurate, timely and infrequent if they are going to help users.

One good way of communicating this risk is to relate information security to something that is more familiar, a risk people are used to managing – something like household security. You could liken the key on the front

door to the password that controls access to people's information. The bars on the door are reminiscent of installing anti-virus software.

Don't make people afraid: Governments and organizations often believe that people have to be scared into taking actions to secure their information. Consider this example of a scary information security message, which is fairly typical, trying to motivate people with fear or dread.

However, cybersecurity academics Karen Renaud and Marc Dupuis warn that this might not be the best way to motivate action. It is likely far better to make sure that people know what actions they need to take, and to ensure that they know how to do this.

Reduce the cost of implementing security: This means designing systems so that behaving securely does not impose an unrealistic cost on users. As an example, consider the cost of updating the software on a smartphone. Many phones require the phone to be plugged into the power supply, the phone cannot be used while it is being updated, it takes up space on the phone's memory and sometimes breaks applications that were running perfectly before the phone was updated. These are real costs, and make it more likely that people will decide not to update the phone, meaning that they will be vulnerable. This process should be re-designed so that it is less costly.

Balance resistance with resilience: It is impossible to be 100% secure, and sometimes information security efforts will fail, and information will be compromised. It is important for the owner of the information to have made plans to be resilient when such an event occurs, as pointed out by psychologist Verena Zimmermann and computer scientist Karen Renaud. The best way for people to achieve this is to ensure that they have made backups so that if information is lost they can recover it. Enhancing personal resilience might also involve buying insurance so that if someone steals their identities, people have help to deal with the fallout. But the onus for resilience can't all be on individuals. Organizations should also have cyber security insurance so that if they do experience a breach the insurance company can help them to recover and also offer assistance to affected customers.

Support: Customers and employees are largely denigrated and blamed when they do not behave securely. This does not help to improve the situation, Humans are by nature effort misers, so the harder it is to do something, the less likely it is that we will expend the effort. This is not laziness – it is simply the way we are built. Companies have to find ways to support their employees and customers, and remove as much friction as possible from the required information security behaviors.

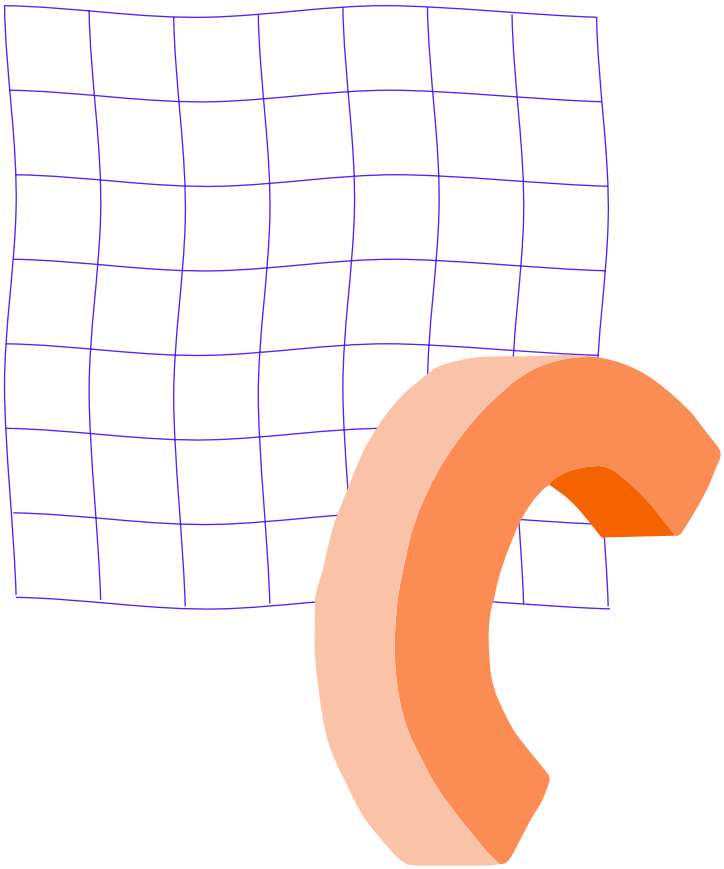
It is also important to write security and privacy policies so that people can actually understand them. Cybersecurity researchers Karen Renaud and Lynsay Shepherd proposed a way of improving privacy policy presentation, which can be useful for those writing these policies.

How to Measure

Many ordinary citizens and organizations measure security as "the absence of incidents." This is unwise, because it might well lead people to consider themselves secure

simply because their information has not yet been compromised, or because they don't realize that someone has compromised their information.

The International Standards Organization's Elizabeth Gasiorowski-Denis summarizes the recently updated ISO/IEC 27004:2016 information security management standard. This is a comprehensive standard but not as applicable to smaller companies. How can they measure their information security? Companies can hire ethical hackers to carry out penetration tests to assess their information security. Cybersecurity researchers Jacqueline Archibald and Karen Renaud proposed a framework for penetration testing the employees within an organization too, called PoinTER. These two activities will reveal vulnerabilities which can then be corrected, but they should be carried out regularly to ensure that the standards are being maintained.



Foundational Works

- Adams, A. & Sasse, M. A. (1999). **Users are not the enemy**. Communications of the ACM, 42(12), 40-46.
- Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., Richer, J. P., Lefkovitz, N. B., Danker, J. M., Choong, Y.-Y., Greene, K. K., & Theofanos, M. F. (2017). **NIST Special Publication 800-63B, Digital Identity Guidelines**. National Institute of Standards and Technology. https://pages.nist.gov/800-63-3/sp800-63b.html
- United Nations. (1948). **Universal Declaration of Human Rights**. https://www.un.org/en/universal-declaration-human-rights/
- von Solms, B.., & von Solms, R. (2018). **Cybersecurity and information security – what goes where?** Information & Computer Security, 26(1), 2-9.

Further Reading

- Aleisa, N., Renaud, K., & Bongiovanni, I. (2020). **The privacy paradox applies to IoT devices too: A Saudi Arabian study.** Computers & Security, 96, 1-17.
- Archibald, J. M. & Renaud, K. (2019). **Refining the PoinTER "human firewall" pentesting framework.** Information and Computer Security, 26(4), 575-600.
- Bischoff, P. (2020, April 20). **How data breaches affect stock market share prices**. Comparitech. https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/
- Byron, T. (2008). **Safer children in a digital world: The report of the Byron review**. http://childcentre.info/robert/extensions/robert/doc/6f4474a71e4794a8c119a0c8fb8ab8ef.pdf
- **General Data Protection Regulation**. (2018). Intersoft Consulting. https://gdpr-info.eu
- Gasiorowski-Denis, E. (2016, December 16). **How to measure the effectiveness of information security**. International Organization for Standardization. https://www.iso.org/news/2016/12/Ref2151.html
- Herley, C. (2009, September 8-11). **So long, and no thanks for the externalities: The rational rejection of security advice by users**. Proceedings of the 2009 New Security Paradigms Workshop, Oxford, U.K., 133-144.
- Mitnick, K. D. & Simon, W. L. (2003). **The art of deception: Controlling the human element of security**. John Wiley & Sons.

- Renaud, K. & Dupuis, M. (2019, September 23-26). **Cyber security fear appeals: Unexpectedly complicated**. Proceedings of the 2019 New Security Paradigms Workshop, San Carlos, Costa Rica.

- Renaud, K. & Shepherd, L. (2018, June 11-12). **How to make privacy policies both GDPR-compliant and usable**. 2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Glasgow, U.K.

- Renaud, K. (2012, May). **Blaming noncompliance is too convenient. What really causes information breaches?** IEEE Security & Privacy.

- West, R. (2008). **The psychology of security**. Communications of the ACM, 51(4), 34-40.

- Westin, A. F. (1968). **Privacy and freedom**. Washington and Lee Law Review, 25(1), 166.

- Volkamer, M., Renaud, K., & Reinheimer, B. (2016, May). **TORPEDO: TOoltip-poweRed Phishing Email DetectiOn**. 31st IFIP International Information Security and Privacy Conference (SEC), Ghent, Belgium, 161-175.

- Zimmermann, V. & Renaud, K. (2019). **Moving from a "human-as-problem" to a "human-as-solution" cybersecurity mindset**. International Journal of Human-Computer Studies, 131. 169-187.

Expert Q&A

Three key questions with **Karen Renaud**, Abertay University

How does this principle help create a world we'd all want to live in?

In a hyper-connected world we gain great benefits from being plugged into the internet highway. Yet our information and our privacy are at risk. The principle of information security, and the obligation of companies to ensure that our information is kept secure, help to prevent privacy violations and other harms that could result if information is not kept confidential and available, and if its integrity cannot be relied upon.

If information security is preserved, cyber criminals and social engineers will find it harder to carry out their nefarious activities, and businesses will not have their operations discontinued due to cyber attacks.

If you were to envisage the perfect social media, messaging or web search platform in terms of maximizing this principle, what would it look like?

A social media platform that respects this principle would have two features. The first is that it would ensure that people using this service are fully informed about what personal information will be gathered about them, and about their usage of the site. Many of these platforms write their privacy policies in such a way that their users do

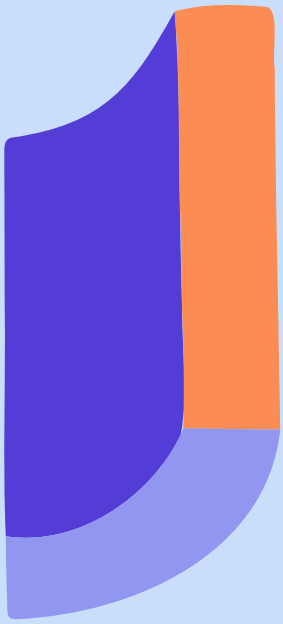
not have a clue as to the range of data that is being collected about them. This is the privacy principle.

The second feature is that user data is properly secured. Sensitive data like passwords should be encrypted so that they are not leaked in case of a data breach. This is the security principle.

How would you measure a messaging, social media, or web search platform's progress against this principle?

Measurement is extremely difficult. These kinds of applications are usually opaque to users in terms of being able to measure the extent to which the users' privacy and security are respected. It might be that legislation is required, and regular audits carried out, to reveal exactly what the applications are doing with their users' data. Moreover, someone should carry out a forensics analysis to ensure that the company actual treats the data the way they say they will, according to their own privacy policy.

Survey results



By Jay Jennings, Taeyoung Lee, Tamar Wilner, and Talia Stroud,
Center for Media Engagement

We conducted a survey with participants in 20 countries to understand more deeply how the signals resonated with people globally. Please find more about the methodology here.

The survey asked people to evaluate whether it was important for platforms to "keep people's information secure," and asked people to assess how well the platforms perform with respect to this signal. People were only asked about the platforms for which they are "superusers," by which we mean people who identify the platform as their most used social media, messaging, or search platform.

We analyzed how different demographic and political groups rate the importance of this signal, as well as the platforms' performance. In particular, we looked at age, gender, education, ideology, and country.

We did this analysis for five platforms: Google, Facebook, YouTube, Facebook Messenger, and WhatsApp.[1] Only statistically significant results are shown and discussed.

1 The analyses include only countries where at least 200 people responded that the social/ message/ search platform was the one that they use most frequently, and then only those platforms where we had data for at least 1,000 people. For Google, this includes all 20 countries. For Facebook, this includes 18 countries and excludes Japan and South Korea. For YouTube, this includes Brazil, Germany, Ireland, Japan, Malaysia, Singapore, South Africa, South Korea, and the United States. For Facebook Messenger, this includes Australia, Canada, France, Ireland, Norway, Poland, Romania, Sweden, the U.K., and the United States. For WhatsApp, this includes all countries except Canada, Japan, Norway, Poland, South Korea, Sweden, and the United States. Note that the total number of respondents varies by platform: Google = 19,554; Facebook = 10,268; YouTube = 2,937; Facebook Messenger = 4,729; and WhatsApp = 10,181. The larger the sample size, the smaller the effect that we are able to detect.

Importance of the Signal

We first examined whether platform superusers thought that the signal was important. This was the most important of all 14 signals for Facebook users in 13 countries, WhatsApp users in 11 countries, Facebook Messenger users in eight countries, YouTube users in two countries, Google users in one country, and Instagram users in one country.

Importance ranking: Keep people's information secure

A ranking of "1" means that the signal was seen as the most important of the 14 signals for superusers of a given platform in a given country based on a survey of over 20,000 people across 20 countries.

	Facebook	Youtube	Instagram	WhatsApp	FB Messenger	Google
Argentina	1		1	1		2
Australia	1	1		1	1	2
Brazil	7	9	5	4		4
Canada	1				1	2
France	3			1	3	2
Germany	1	4	6	1		2
Ireland	1	2		1	1	2
Italy	1			1		2
Japan		3				3
Malaysia	9	8	9	5		4
Mexico	2			1		2
Norway	1				1	2
Poland	10				5	8
Romania	1			1	1	1
Singapore	1	5		1		2
South Africa	1			1		2
South Korea		9				2
Sweden	1		2		1	3
UK	1			1	1	2
US	1	1			1	2

Signal is most important

1 2 3 4 5 6 7 8 9 10 11 12 13 14

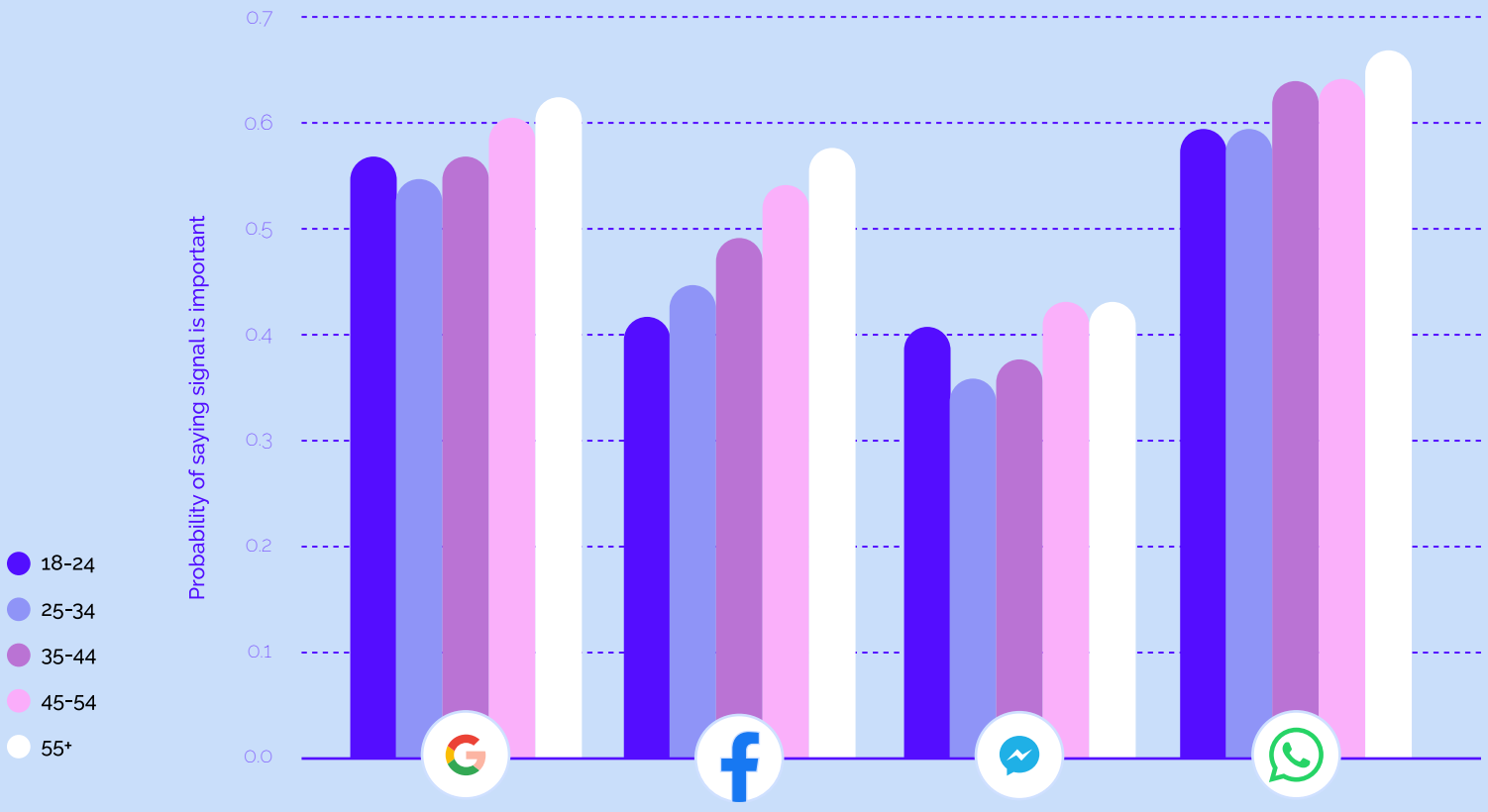
Signal is least important

Data from the Center for Media Engagement. Weighted data. Asked of those who indicated that a given social media, messaging or search platform was their most used. Question wording: Which of the following do you think it is important for [INSERT SOCIAL, MESSAGING OR SEARCH PLATFORM] to do? Please select all that apply. Data only shown for those countries where at least 200 survey respondents said that the platform was their most used social media, messaging, or search platform.

Importance of the Signal by Age[2]

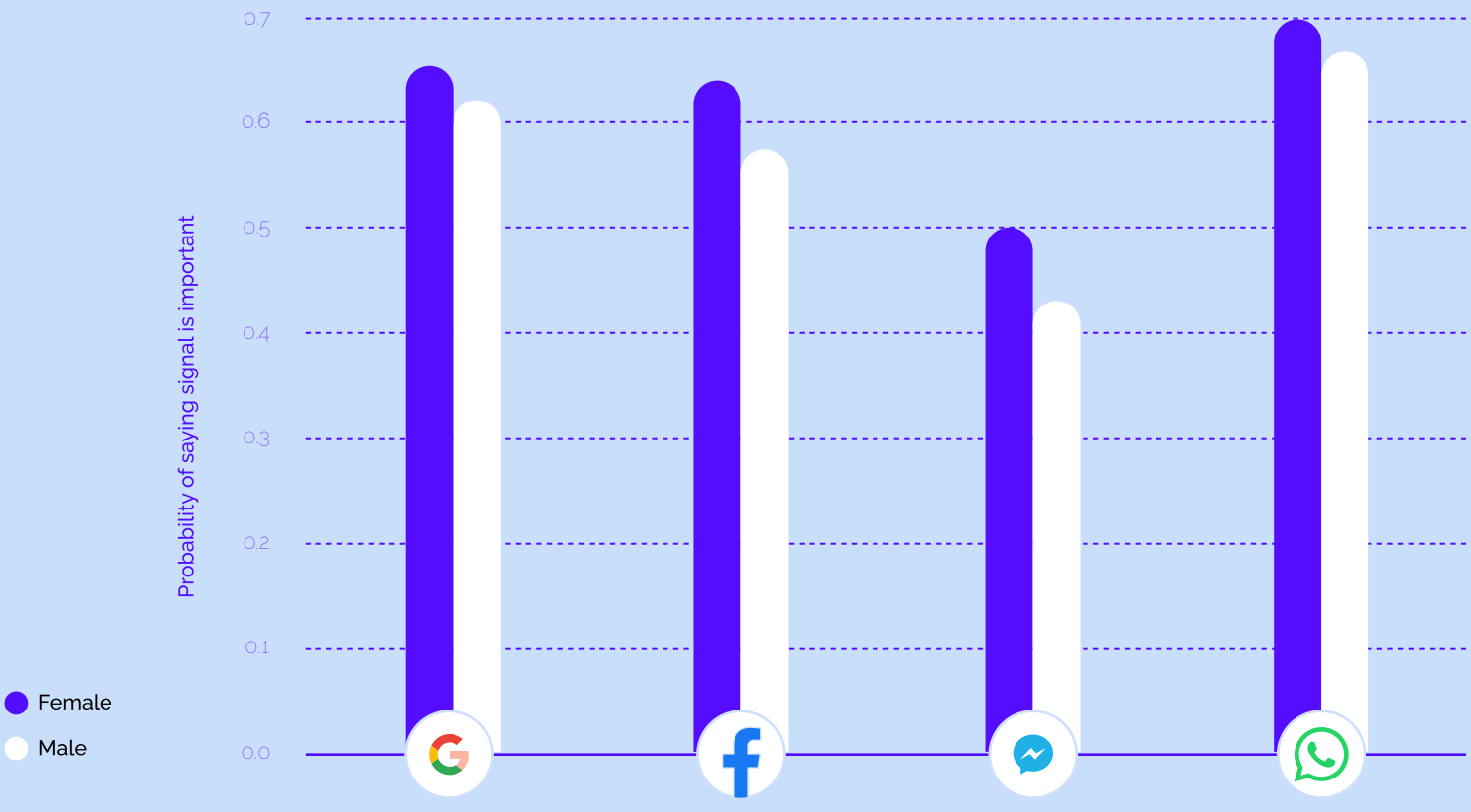
Age predicted whether superusers thought that "keeping people's information secure" was important for four of the five platforms: Google, Facebook, Facebook Messenger, and WhatsApp. For Google, those 45 and above reported that the signal was more important than those who were younger. For Facebook, those who were older reported that the signal was more important than those who were younger. For Facebook Messenger, those 45 and above believed that "keeping people's information secure" was more important than those 25-44. For WhatsApp, those 55+ thought that the signal was more important than those 18-44.

2 Results shown are predicted probabilities, calculated from a logistic regression analysis predicting that the signal is important based on age, gender, education, ideology, and country, each treated as a categorical variable. The baseline (based on the excluded categories) is a 55+ year old male with high education and middle ideology from the United States (except for WhatsApp, where the baseline is South Africa).



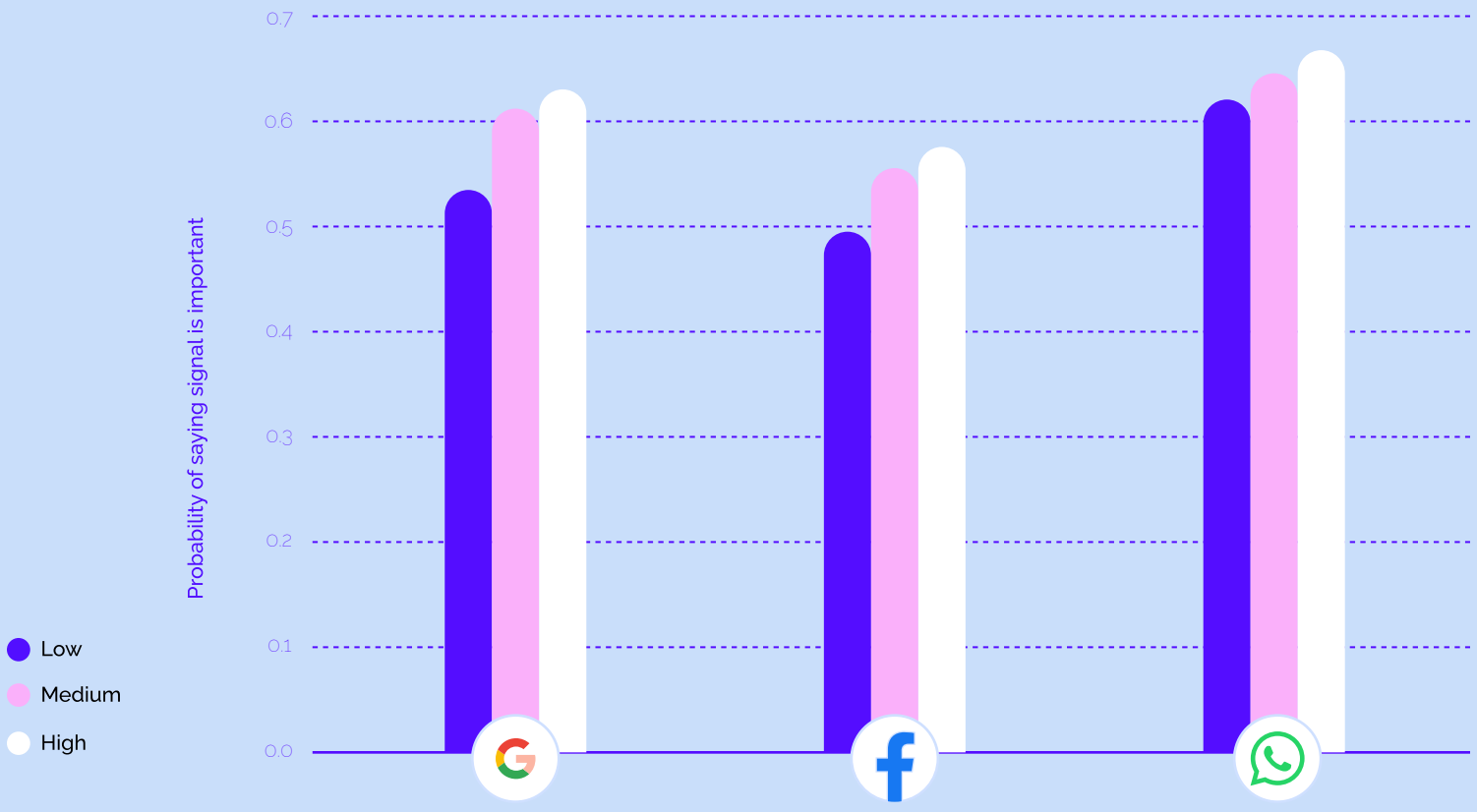
Importance of the Signal by Gender

Men and women differed in the importance they ascribed to “keeping people’s information secure” for Google, Facebook, Facebook Messenger, and WhatsApp. For all four, women were more likely than men to say that the signal was important.



Importance of the Signal by Education

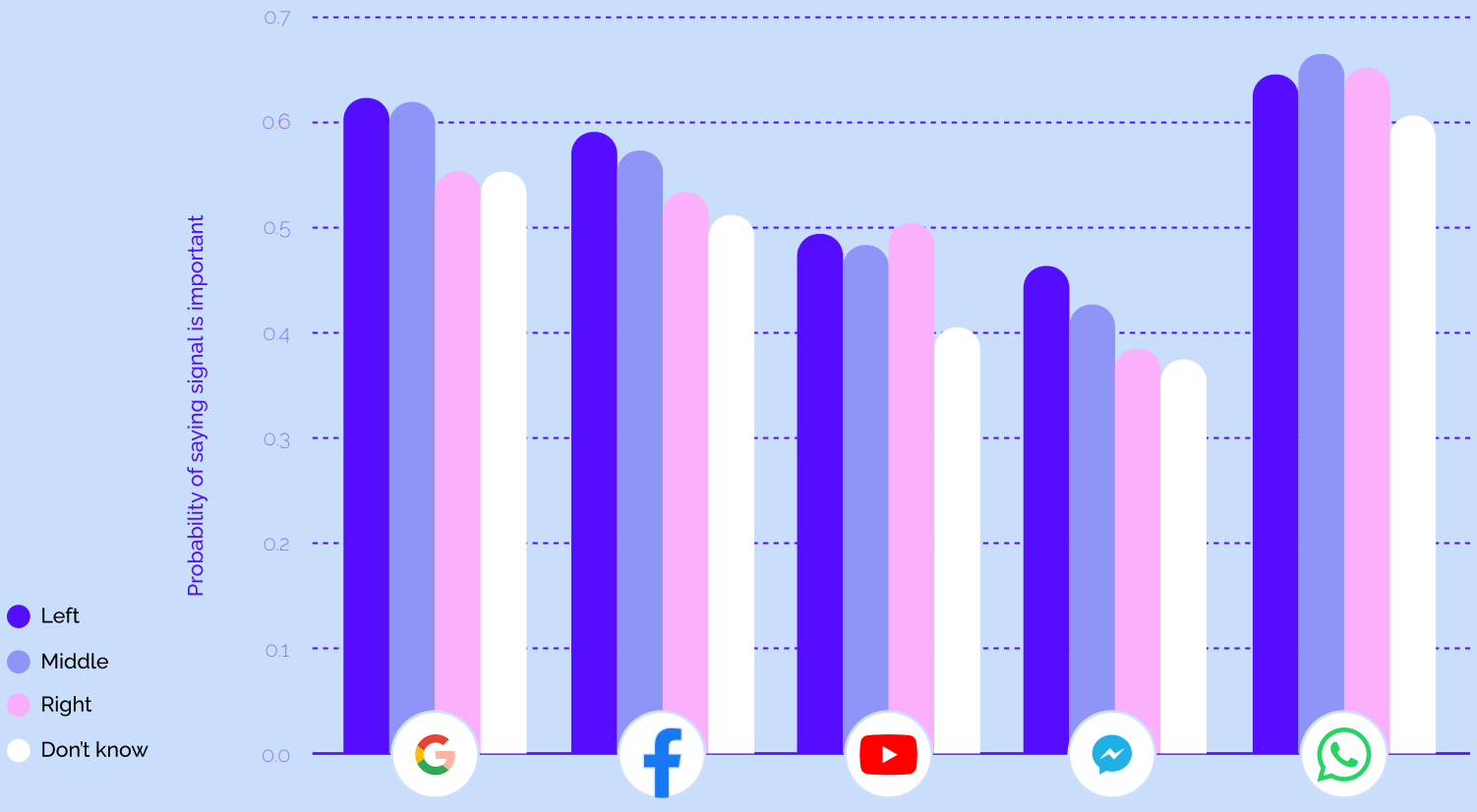
The importance of "keeping people's information secure" varied by education only when superusers were evaluating Google, Facebook, and WhatsApp. Here, those with higher levels of education were more likely to think that the signal was important than those with lower levels of education.



Importance of the Signal by Ideology[3]

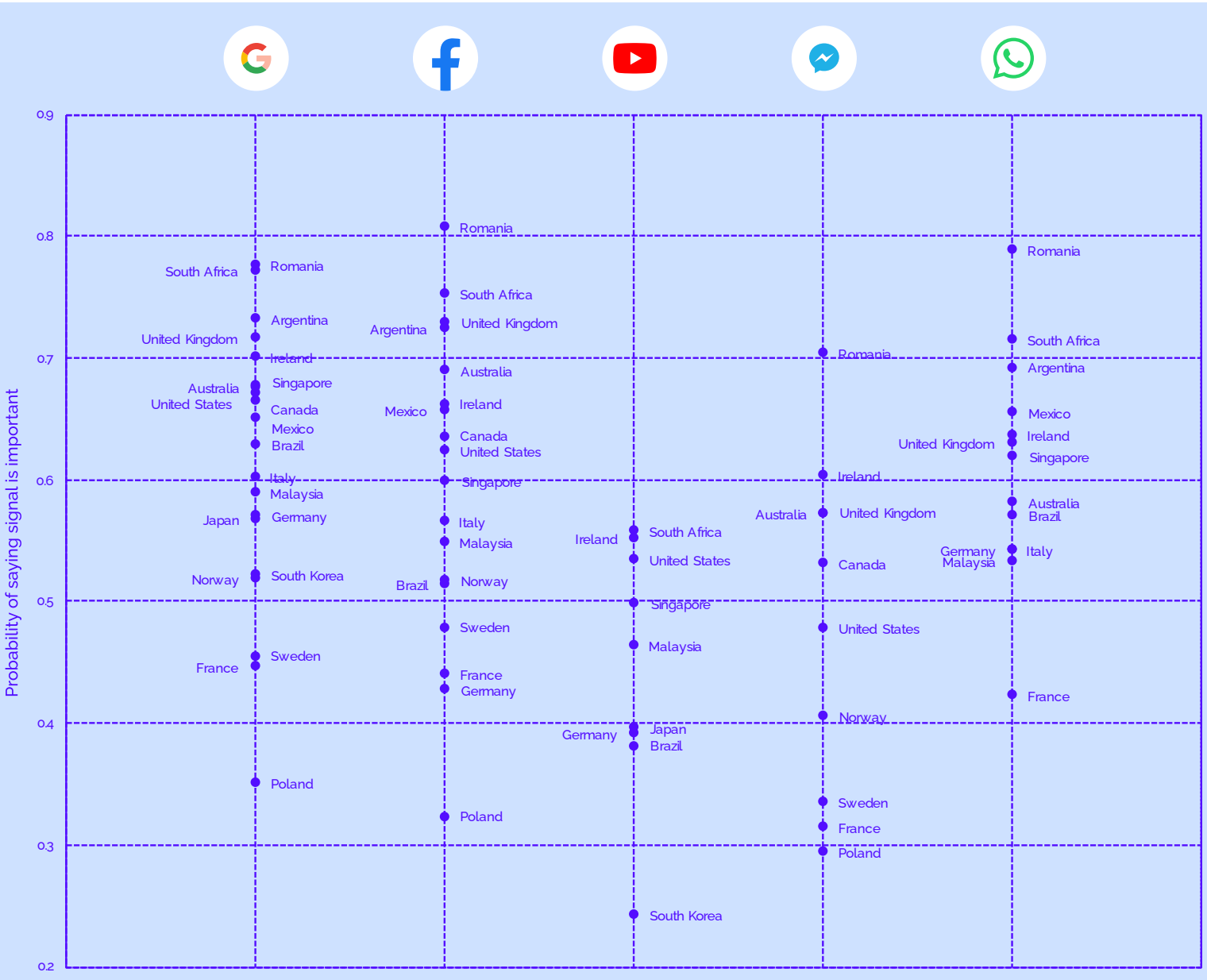
Ideology predicted whether superusers thought that "keeping people's information secure" was important for all five of the platforms we examined. For Google, Facebook, and Facebook Messenger, those on the left and in the middle thought that this signal was more important than those on the right or those who didn't know their ideology. For YouTube and WhatsApp, those who didn't know their ideology rated the signal as less important than those with other ideologies.

3 Ideology was asked on a 10-point scale and people were given the option of saying "don't know." This was recoded into 4 categories (1 through 3, 4 through 7, 8 through 10, and "don't know").



Importance of the Signal by Country

There was significant variation by country for all five of the platforms we examined based on how important superusers thought that "keeping people's information secure" was. The chart below shows the probability of saying that the signal is important by platform and by country. Overall, superusers in Romania, South Africa, Argentina, the United Kingdom, and Ireland were more likely to endorse this signal as important across platforms. Fewer superusers endorsed the signal as important across platforms in Poland, France, Germany, Sweden, Norway, and South Korea.



Platform Performance on the Signal

For specific platforms, superusers were first asked to say on which of the signals they thought that the platform was doing well, and then on which of the signals they thought that the platform was doing poorly. We then categorized people's responses as (0) believe that the platform is doing poorly, (1) believe that the platform is doing neither well nor poorly, or (2) believe that the platform is doing well. Superusers tended to rate the platforms as performing not particularly badly nor particularly well. WhatsApp and Google tended to be rated more highly than Facebook.

Performance index: Keep people's information secure

Responses of "2" indicate that everyone in a particular country thought that the platform was performing well on a signal; responses of "0" indicate that no one in a particular country thought that the platform was performing well on a signal based on a survey of over 20,000 people across 20 countries.

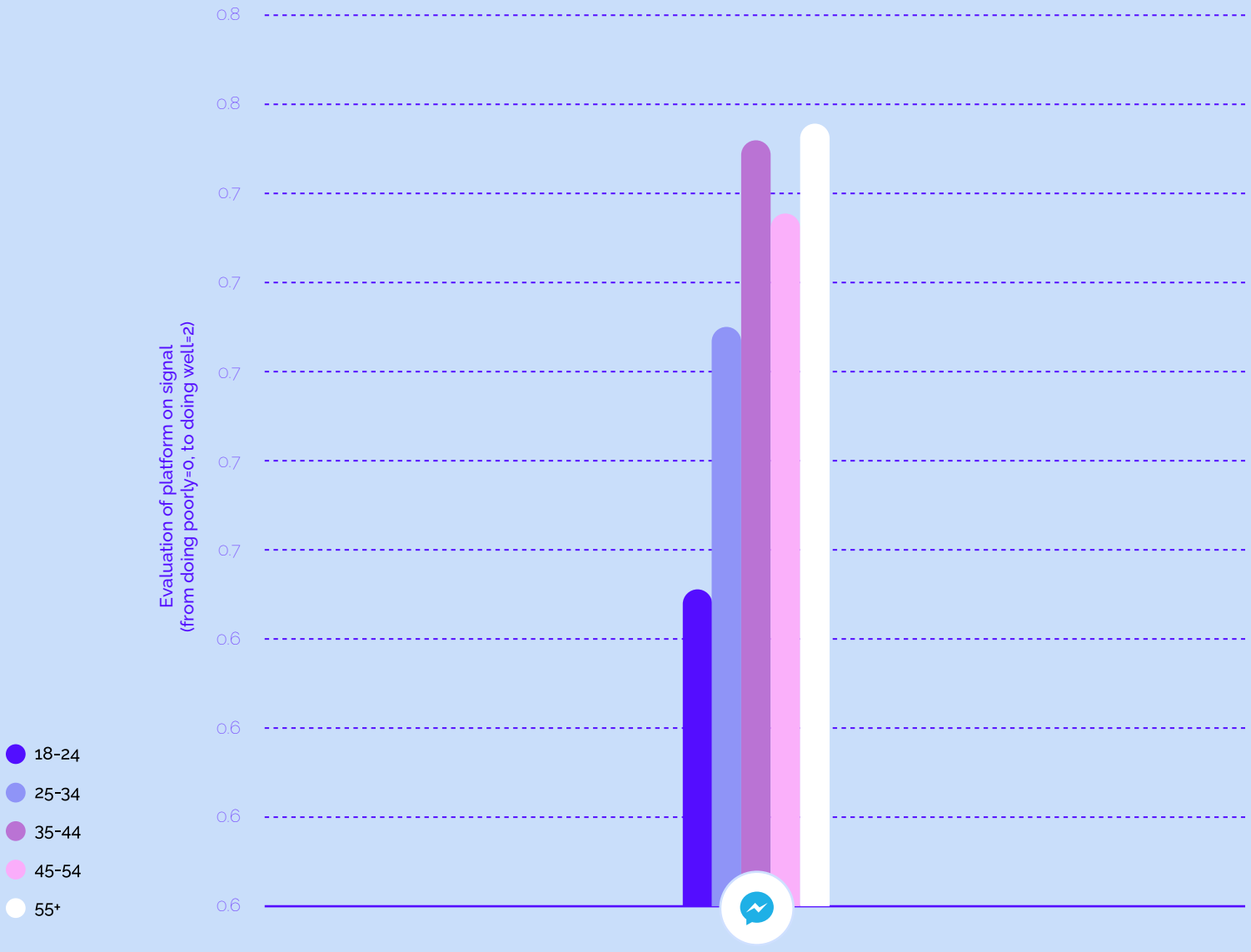
	Facebook	Youtube	Instagram	WhatsApp	FB Messenger	Google
Argentina	1.0		1.1	1.2		1.0
Australia	0.7	0.9		1.2	0.9	1.0
Brazil	1.0	1.1	1.1	1.1		1.2
Canada	0.7				0.9	1.0
France	0.8			1.0	0.9	0.9
Germany	0.8	0.9	0.9	0.9		0.8
Ireland	0.8	1.0		1.2	1.0	1.1
Italy	0.8			1.1		1.0
Japan		1.0				1.1
Malaysia	0.9	1.1	1.0	1.1		1.1
Mexico	0.9			1.2		1.1
Norway	0.8				1.0	0.9
Poland	1.0				1.0	1.1
Romania	0.9			1.3	1.1	1.1
Sigapore	0.8	1.0		1.1		1.0
South Africa	0.9			1.3		1.1
South Korea		0.9				1.0
Sweden	0.7		1.0		0.9	0.8
UK	0.7			1.2	0.9	0.9
US	0.8	0.9			0.8	0.9

Data from the Center for Media Engagement. Weighted data. Asked of those who indicated that a given social media, messaging or search platform was their most used. Question wording - Which of the following do you think [INSERT SOCIAL, MESSAGING OR SEARCH PLATFORM] does well at? Please select all that apply. And which of the following do you think [INSERT SOCIAL, MESSAGING OR SEARCH PLATFORM] does poorly at? Please select all that apply. Data only shown for those countries where at least 200 survey respondents said that the platform was their most used social media, messaging, or search platform.

Platform Performance on the Signal by Age[4]

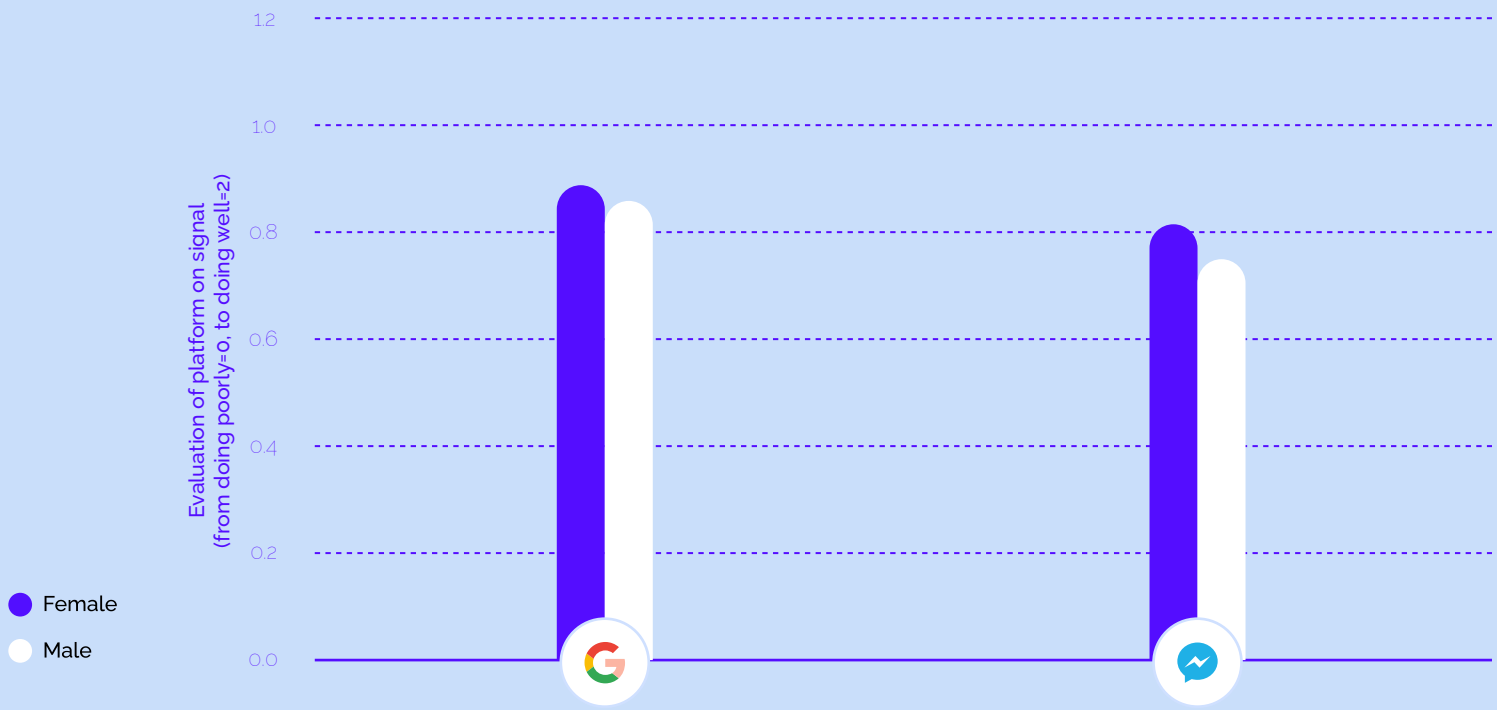
Only for Facebook Messenger, age significantly predicted what superusers thought about how well the platform was doing at "keeping people's information secure." Here, respondents aged 35 and above rated the platform's performance more positively than those 18-24.

4 Results shown are predicted responses, calculated from a regression analysis predicting that the signal is important based on age, gender, education, ideology, and country, each treated as a categorical variable. The baseline (based on the excluded categories) is a 55+ year old male with high education and middle ideology from the United States (except for WhatsApp, where the baseline is Germany).



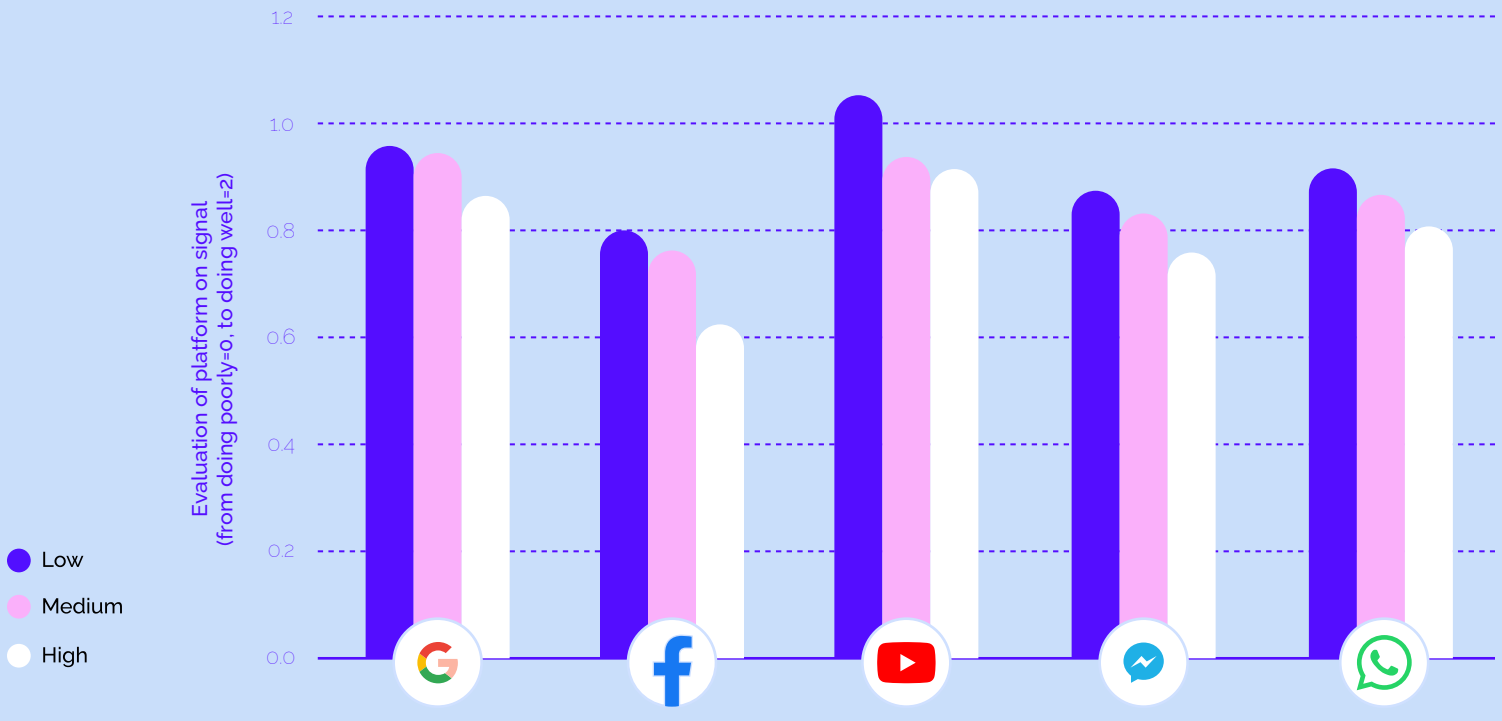
Platform Performance on the Signal by Gender

For Google and Facebook Messenger, women rated the platforms' performance on "keeping people's information secure" better than did men.



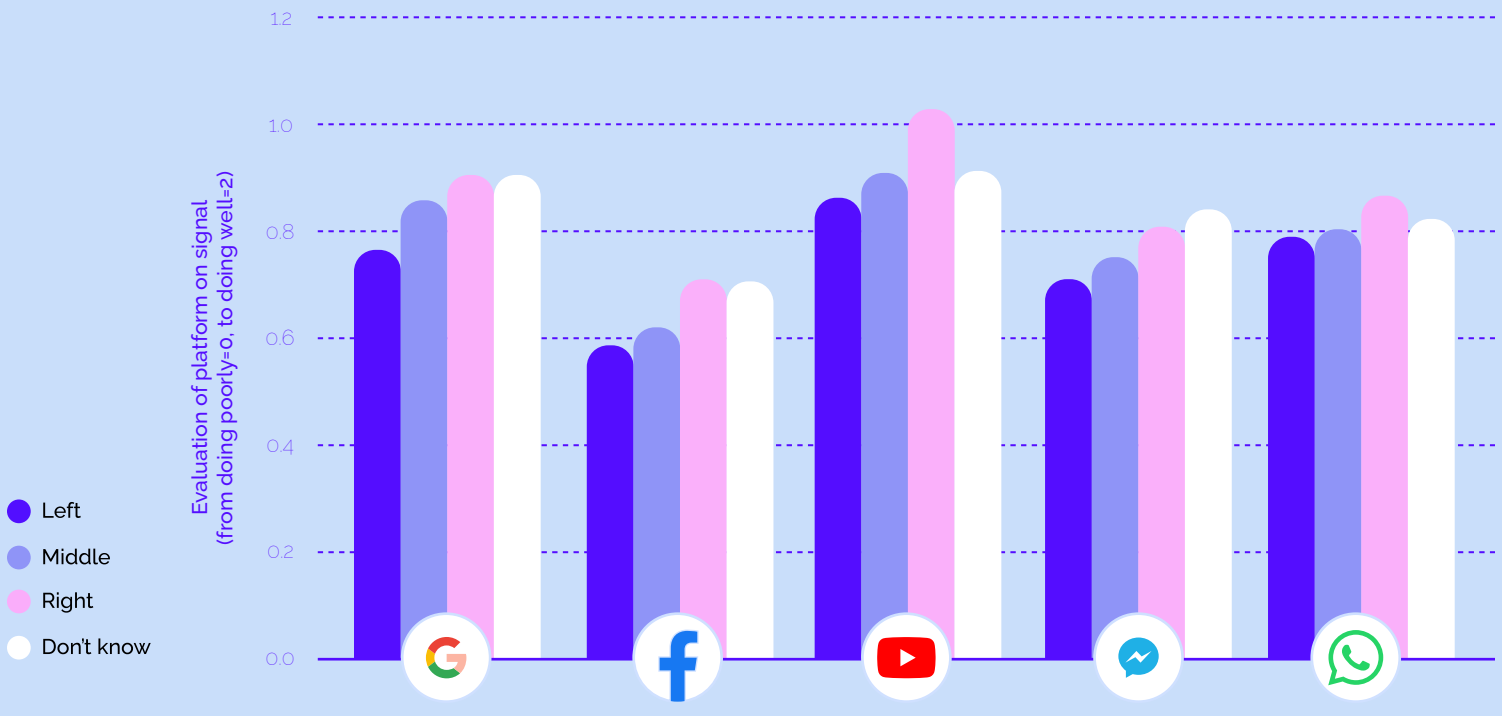
Platform Performance on the Signal by Education

For all five platforms, education significantly predicted what superusers thought about how well the platform was doing at "keeping people's information secure." In each case, less educated respondents thought that the platform did a better job than did more educated respondents.



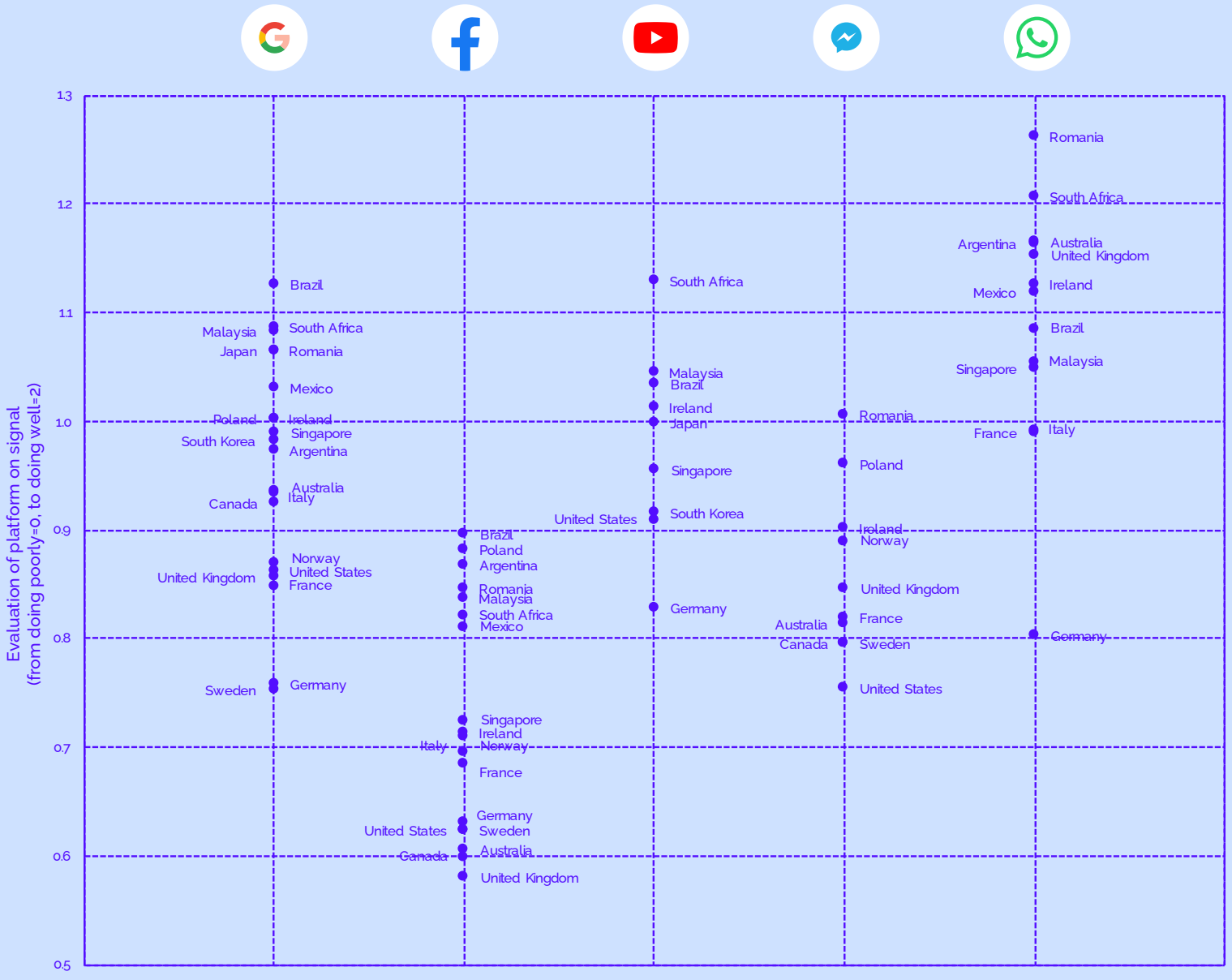
Platform Performance on the Signal by Ideology

For all five of the platforms we examined, there were differences in how superusers evaluated the platform's performance at "keeping people's information secure" by ideology. For Google, those on the right and who didn't know their ideology evaluated the platform's performance more positively and those on the left evaluated the platform's performance more negatively than did other ideologies. For Facebook and Facebook Messenger, those on the right and who didn't know their ideology evaluated the platform's performance more positively than did those on the left or those in the middle. For YouTube and WhatsApp, those on the right evaluated the platform's performance more positively than did those with other ideologies.

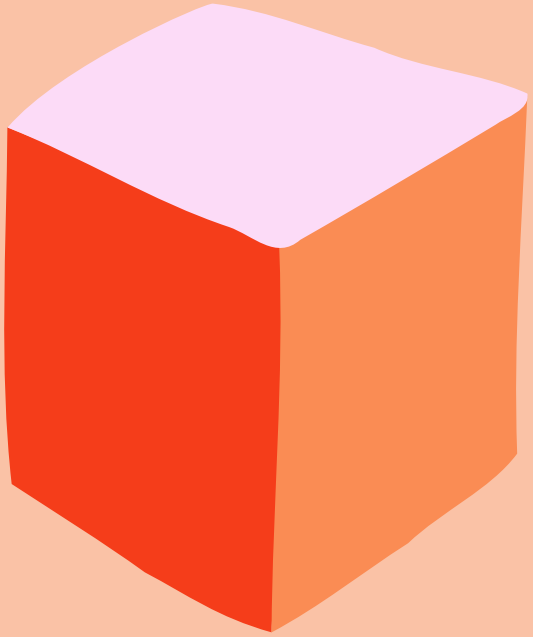


Platform Performance on the Signal by Country

There was variation by country in evaluations of platform performance. The chart below shows how superusers rated the platforms' performance in each country, controlling for age, gender, education, and ideology, from "doing poorly" (0) to "doing well" (2). In general, those in South Africa, Malaysia, Romania, and Brazil tended to say that the platforms performed better with respect to this signal than those in the Germany, Sweden, Canada, France, the United States, and the United Kingdom.



Focus group report



By Gina Masullo, Ori Tenenboim, and Martin Riedl,
Center for Media Engagement

We conducted two focus groups in each of five countries (Brazil, Germany, Malaysia, South Africa, and the United States). Please find more about the methodology here. Participants were asked to reflect on their social media experiences and the proposed signals. With respect to this signal, participants made several observations. Please note that all names included are pseudonyms.

Participants expressed concerns over the ways in which social media companies and other entities or individuals are using information about them. Some participants wanted to know more about what social media companies do with the information they have.

> *So here is the thing, Facebook is a free app, but you need to ask yourself, 'If I'm getting this app for free, what are they getting in return?' Chances are they're getting my information."*
> *– Phumzile, South African focus group participant*

"You reveal so many private things about you. And I personally find it absolutely unclear where these data are used and stored," said Yusuf, of Germany. "I do notice that thanks to my Google account and my

> *You reveal so many private things about you. And I personally find it absolutely unclear where these data are used and stored. I do notice that thanks to my Google account and my Facebook account, the advertising, which is overflowing me, is absolutely personalized. This is sometimes rather creepy." – Yusuf, Germany*

Facebook account, the advertising, which is overflowing me, is absolutely personalized. This is sometimes rather creepy."

Jéssica, of Brazil, also expressed feeling a bit surprised by ads that pop up on Facebook offering the same product that she just searched for on Google. "It's impressive. Sometimes you look up things on Google," she said. "... I wanted to buy a minibar, I left Google, I said 'It can't be possible, there's a camera here!' Then, you go to Facebook and, in the middle of your timeline, there's a minibar post. So, everything is kind of linked."

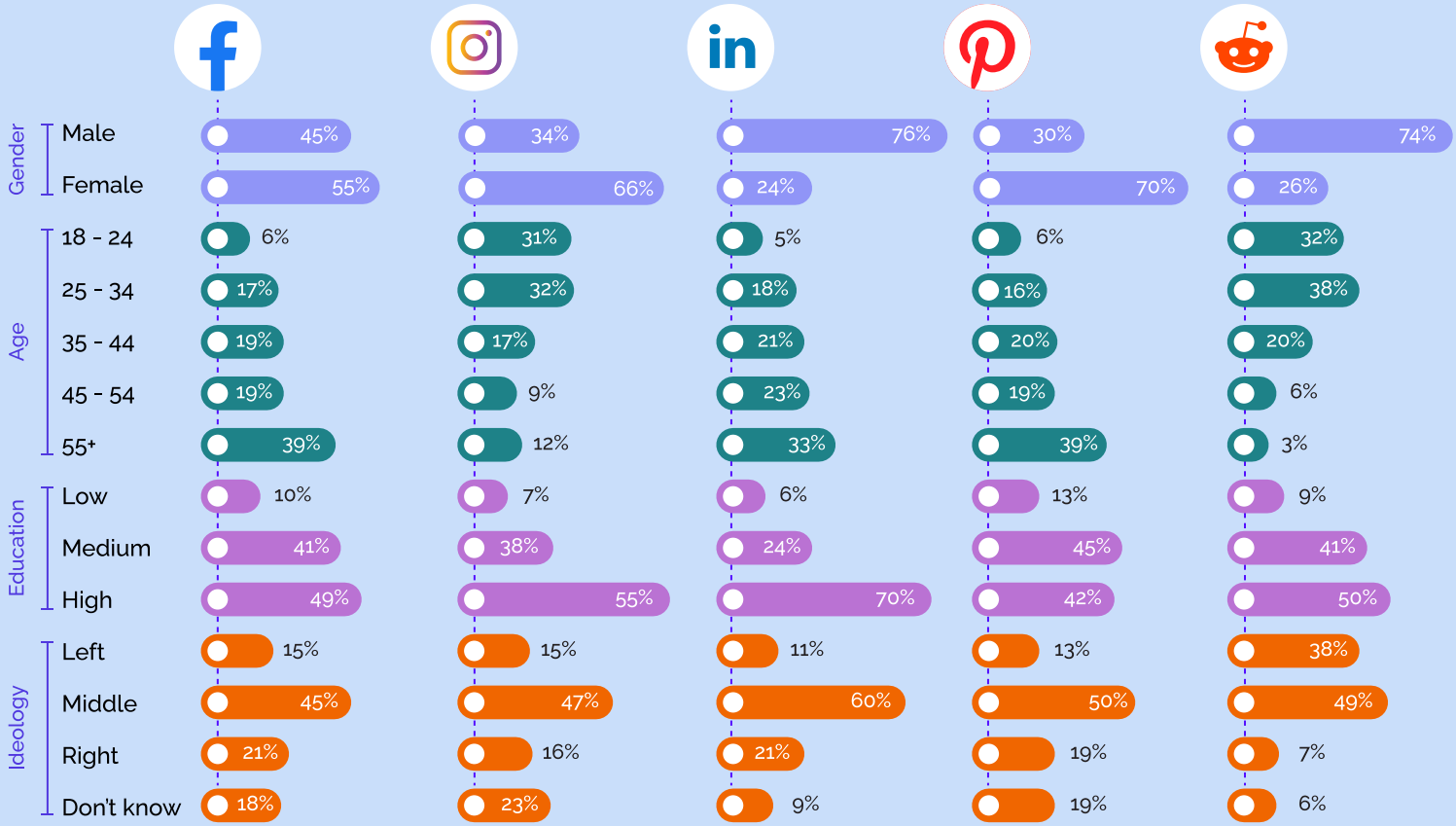
Participants also worried that social media companies were selling data about users. Phumzile, of South Africa, said she felt platforms were not "open and transparent about what they do with our information." "So here is the thing, Facebook is a free app, but you need to ask yourself, 'If I'm getting this app for free, what are they getting in return?'" she continued. "Chances are they're getting my information."

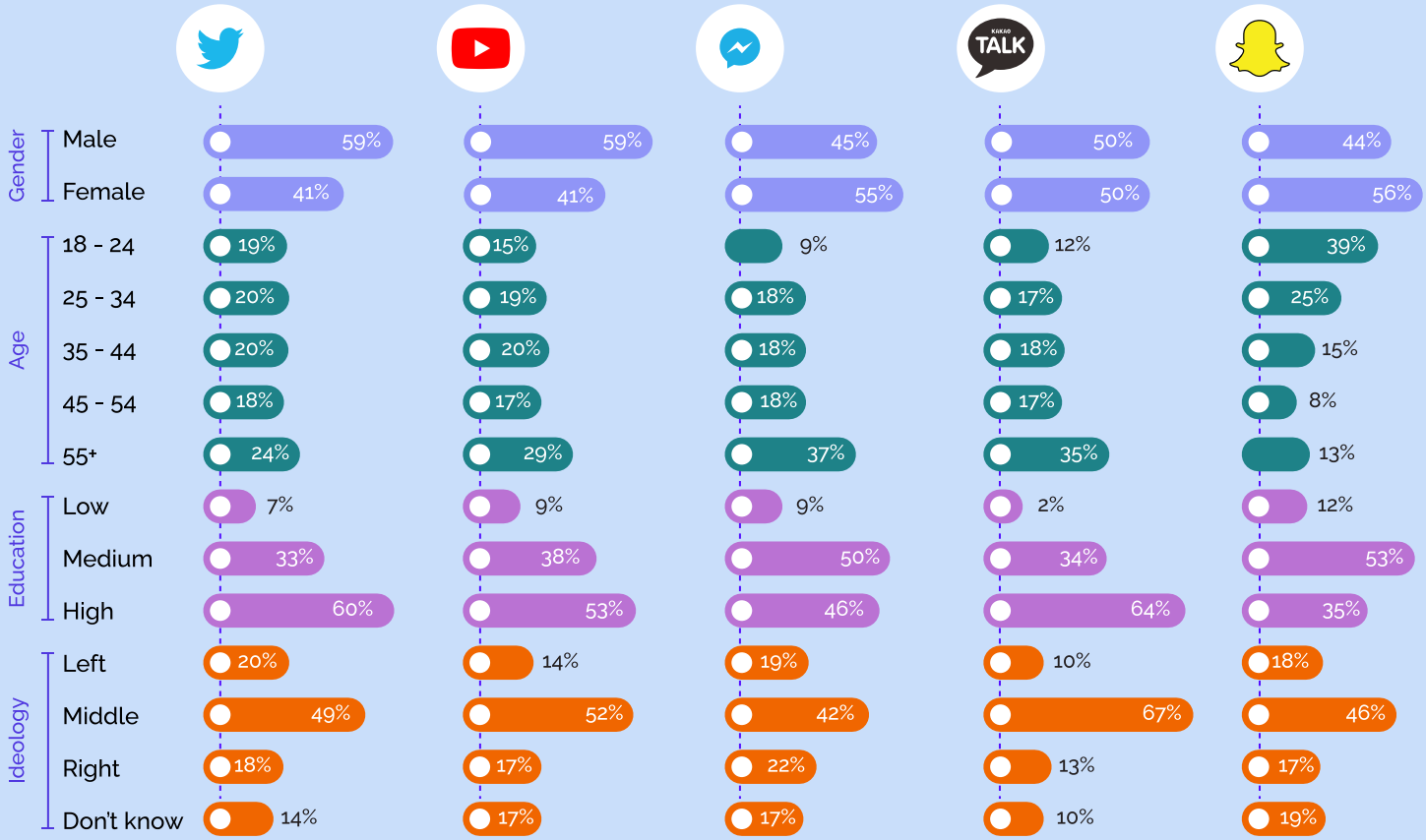
Concerns about data safety made some users careful about which platforms they use. Dennis, of the U.S., for example, said he feels safer on Twitter than Facebook. "Facebook, I mean time and time again their information is being used for this, they're selling information for that, so I don't trust Facebook; I don't use it," he said.

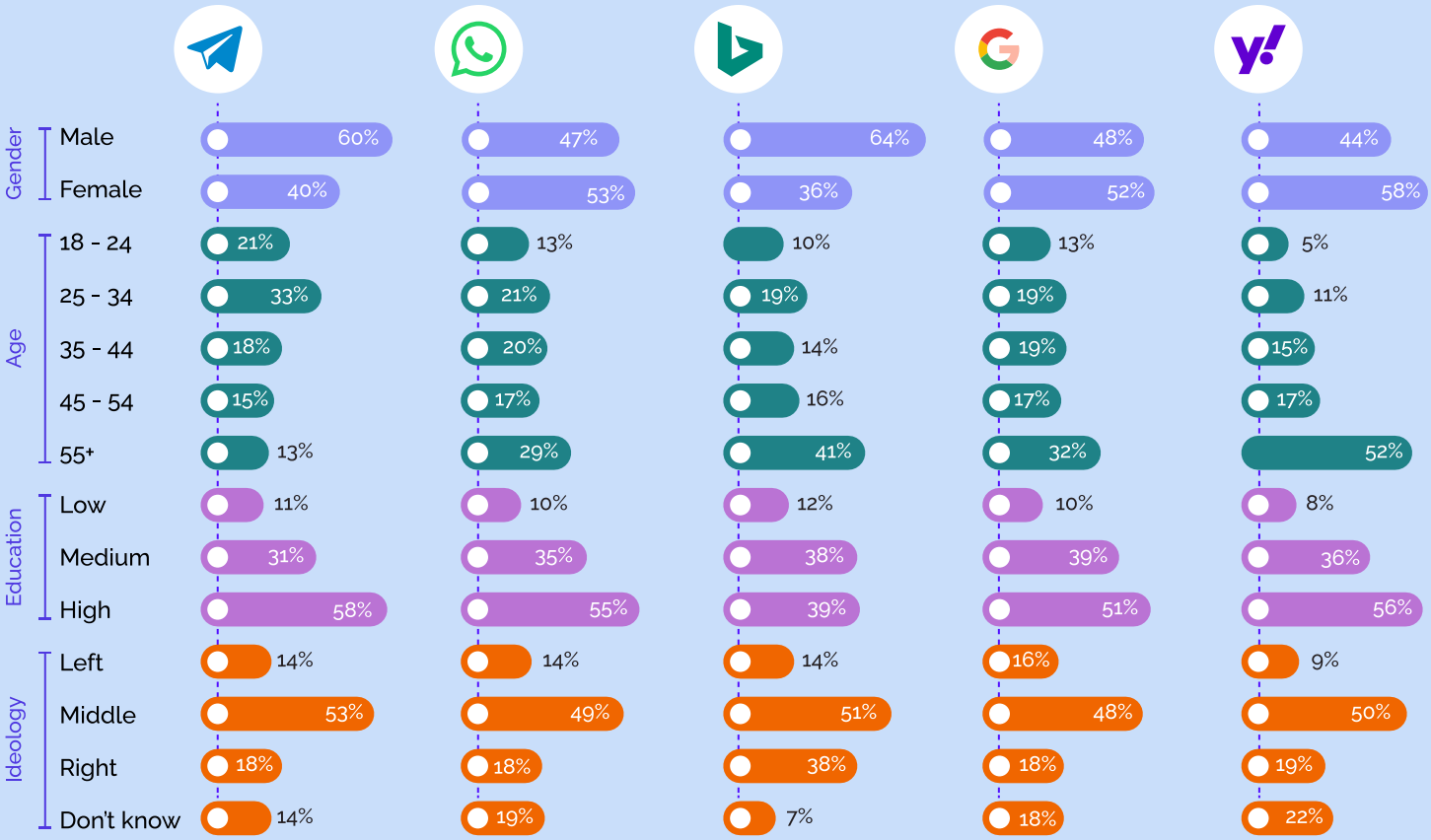
Others encouraged people to become informed about how to adjust privacy settlings on platforms to keep their content safer. "You need to know how to block private information. Your setting has to be the highest security setting for any social media," advised Kumanan, of Malaysia.

User demographics from survey

Based on the survey respondents across all 20 countries, we looked at the demographics of superusers. For example, of those naming Facebook as their most used social media platform, 45% are male and 55% are female.






Gender
Male
Female
Age
18 - 24
25 - 34
35 - 44
45 - 54
55+
Education
Low
Medium
High
Ideology
Left
Middle
Right
Don't know
60%
40%
21%
33%
18%
15%
13%
11%
31%
58%
14%
53%
18%
14%
47%
53%
13%
21%
20%
17%
29%
10%
35%
55%
14%
49%
18%
19%
64%
36%
10%
19%
14%
16%
41%
12%
38%
39%
14%
51%
38%
7%
48%
52%
13%
19%
19%
17%
32%
10%
39%
51%
16%
48%
18%
18%
44%
58%
5%
11%
15%
17%
52%
8%
36%
56%
9%
50%
19%
22%

Logo glossary

Social media

- Facebook
- Instagram
- LinkedIn
- Pinterest
- Reddit
- Twitter
- YouTube

Messaging

- Facebook Messenger
- KakaoTalk
- Snapchat
- Telegram
- WhatsApp

Search engines

- Bing
- Google
- Yahoo

Civic Signals