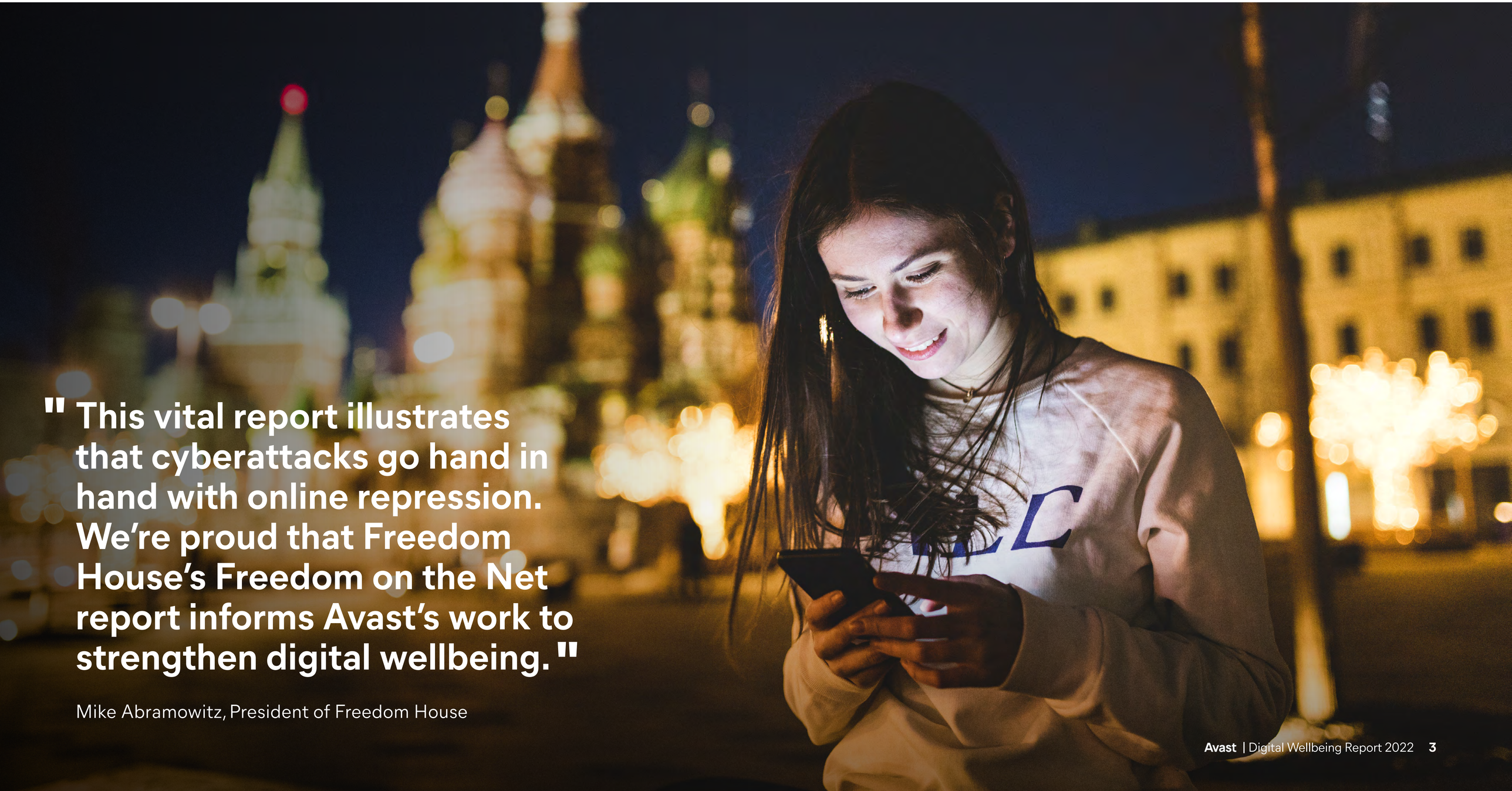
Avast Digital Wellbeing Report

Protecting our Digital Freedom:
The relationship between
Digital Wellbeing and
Freedom on the Internet

Table of contents



"This vital report illustrates that cyberattacks go hand in hand with online repression. We're proud that Freedom House's Freedom on the Net report informs Avast's work to strengthen digital wellbeing."

Mike Abramowitz, President of Freedom House

Introduction

Over the last two years, the Covid-19 pandemic has had an unprecedented impact on the wellbeing of internet users across the world.

As social distancing was adopted and most face-to-face economic activity came to a halt, many people found their lives changed from one day to the next as they started fully working, socializing, and living online.

This sharp increase in the use of the internet, however, also led to a rise in malicious online activity including large scale data breaches, online scams, and other cyber-attacks: At the same time, the world has seen an unparalleled spread of misinformation online since the start of the pandemic.

The FBI reported a 400% increase in reports of cybercrime[1] in the first month of the pandemic and a 7% increase in cybercrime reports in 2021 compared to 2020[2]. The World Economic Forum (WEF) also estimated that in the first six months of 2021 alone, the global volume of ransomware attacks against companies, or malicious software attacks, rose by 151% compared to 2020[3]. Avast further observed a 20% increase in ransomware attacks against its customers globally at the beginning of the pandemic, as well as a large increase in Covid-19 related scams such as websites selling coronavirus related medicines, fake pandemic guides, and malicious applications for mobile phones.

Other factors have contributed to the recent rise in malicious activity targeting internet users. The recent Russian invasion of Ukraine which began in February 2022, also generated an increase in scams related to the conflict like fake calls for donations generated on social media[4]. The success of criminals operating online is often improved by adapting their tactics to take advantage of world events; such tailoring allows them to reach more people just as marketers seek to do.

Decline in Digital Freedom

Several governments across the world responded to the pandemic by implementing widespread authoritarian tactics. Authoritarianism deepened across the world both in hybrid and authoritarian regimes, and 2020 was the worst year on record in terms of the number of countries affected by deepening autocratization[5]. The year 2021 also saw global internet freedom decline for the eleventh consecutive year and, due to the pandemic, free expression online was put under unprecedented strain[6]. Covid-19 related misinformation campaigns have surged since the beginning of the pandemic, moving from anti-vaxxer messaging to pro-Kremlin propaganda in February 2022. Misinformation is spread on Twitter, Facebook, and other social networks, driven

[1] Maggie Miller, "FBI Sees Spike in Cyber Crime Reports during Coronavirus Pandemic" (The Hill - April 16, 2020)
[2] Federal Bureau of Investigations, "FBI Internet Crime Report 2021" (FBI - Internet Crime Complaint Centre, 2022)
[3] World Economic Forum, "Global Cybersecurity Outlook 2022" (2022)
[4] Avast is actively monitoring the situation with regards to the 2022 Russian invasion of Ukraine and is exploring the impact the conflict on cyberattacks and access to the internet: "Avast warns users of crypto scams taking advantage of Ukraine conflict". An additional consideration about the conflict has been included in this study's Conclusions.
[5] International Institute for Democracy and Electoral Assistance, "The Global State of Democracy 2021 - Building Resilience in a Pandemic Era" (2021)
[6] Freedom House, "Freedom on the Net 2021 - the Global Drive to Control Big Tech" (2021)

by bad actors using automated bots, and AI to generate and amplify content. This activity is facilitated by social network algorithms that prioritize boosted and viral content, leading to malinformed digital citizens.

In 2022, the rapid deterioration of digital freedom in Russia began a day before Russia's invasion of Ukraine on February 24, with widespread reports at that time indicating that the Kremlin was slowing down the access to social media websites like Facebook and Twitter[7]. Supposedly in an effort to block the Russian population's access to information from the Western world, Facebook, Twitter, and several news pages including BBC Russia, Deutsche Welle and Radio Free Europe were subsequently fully blocked one week after the start of the invasion. Later in March, Russia also blocked Google News, after Google announced it would not allow advertising that condone the war[8].

The relationship between digital freedom and digital wellbeing

In an effort to continue advocating for the wellbeing of internet users, Avast set out to explore the relationship between digital wellbeing and online freedom, and the interplay of factors affecting the two. Digital wellbeing is a broad, complex term that has different meanings, however, for the purpose of this study it has been defined as: 'the ability of an internet user to utilize the internet in an open, regulated, private, secure, and informed way'[9].

The aim of this study is to analyze the relationship between a country's freedom of the internet, measured by its Freedom on the Net Index, and the digital wellbeing of its citizens, highlighting the correlation between one's online freedom and wellbeing. This study further builds on Avast's Digital Citizenship Report, which explored post-pandemic online behaviors, and is part of Avast's efforts in understanding how our life online can be improved[10].

Avast firmly believes that privacy online is fundamental to digital wellbeing and is a strong advocate for privacy at the core of all internet use. Other factors that impact the digital wellbeing of a nation include its population's wealth, its level of education including digital skills, the openness of its society and government, and the extent of its internet regulation. To analyze this interplay, this study takes into consideration Freedom House's 'Freedom on the Net' (FotN) report, an annual report that surveys internet freedom around the world through analysis, fact-based advocacy, and on-the-ground capacity building. Avast chose the FotN report as it is aligned with our understanding of digital freedom. The FotN report aligns with Avast's view of digital freedom in assessing aspects outlined in the methodology section of this report.

The study sets out a methodology used to assess the relationship, the way the data was collected, and the parameters used to explore it. A section on findings sets out three key insights about this relationship. Finally, conclusions are drawn that include potential issues to be explored by further studies, and policy recommendations are made for regulators and policy makers to take into consideration when trying to address the overall digital wellbeing of their citizens. The efforts that Avast has made in trying to improve the digital wellbeing of its customers and of internet users across the globe are also explored.

[7] James Purtill, "From Instagram to Paypal, Russia's internet is being dismantled as a digital iron curtain descends"

[8] Hern, Alex, "Russia blocks Google News after ad ban on content condoning Ukraine invasion". (The Guardian - 24 March 2022).

[9] More context on Digital Wellbeing: Open – allowing internet users to access all areas of the open internet, without restrictions based on geographic location and nationally established firewalls; Regulated – allowing internet users to be protected by legislations ensuring ability to use the internet use without infringing their privacy and human rights; Private – allowing internet users to carry out private activity online without being monitored or targeted by their government; Secure – allowing internet users to access the internet securely without having to fear potential cyber-attacks from public or private entities; Informed – allowing users to use the internet in an informed way, having access to information that empowers and enables their lives and businesses.

[10] Avast, "Avast Digital Citizenship Report: Post-Pandemic Online Behavior" (Avast - November 2021)

Methodology

To assess the relationship between Digital Wellbeing and online freedom, Avast took into consideration one primary metric: Freedom House's Freedom on the Net Index which is widely regarded as the most reliable index that seeks to measure the levels of internet freedom in many countries.

By using the data provided by Freedom House, Avast was able to compare this data with its own internal data to better understand digital wellbeing.

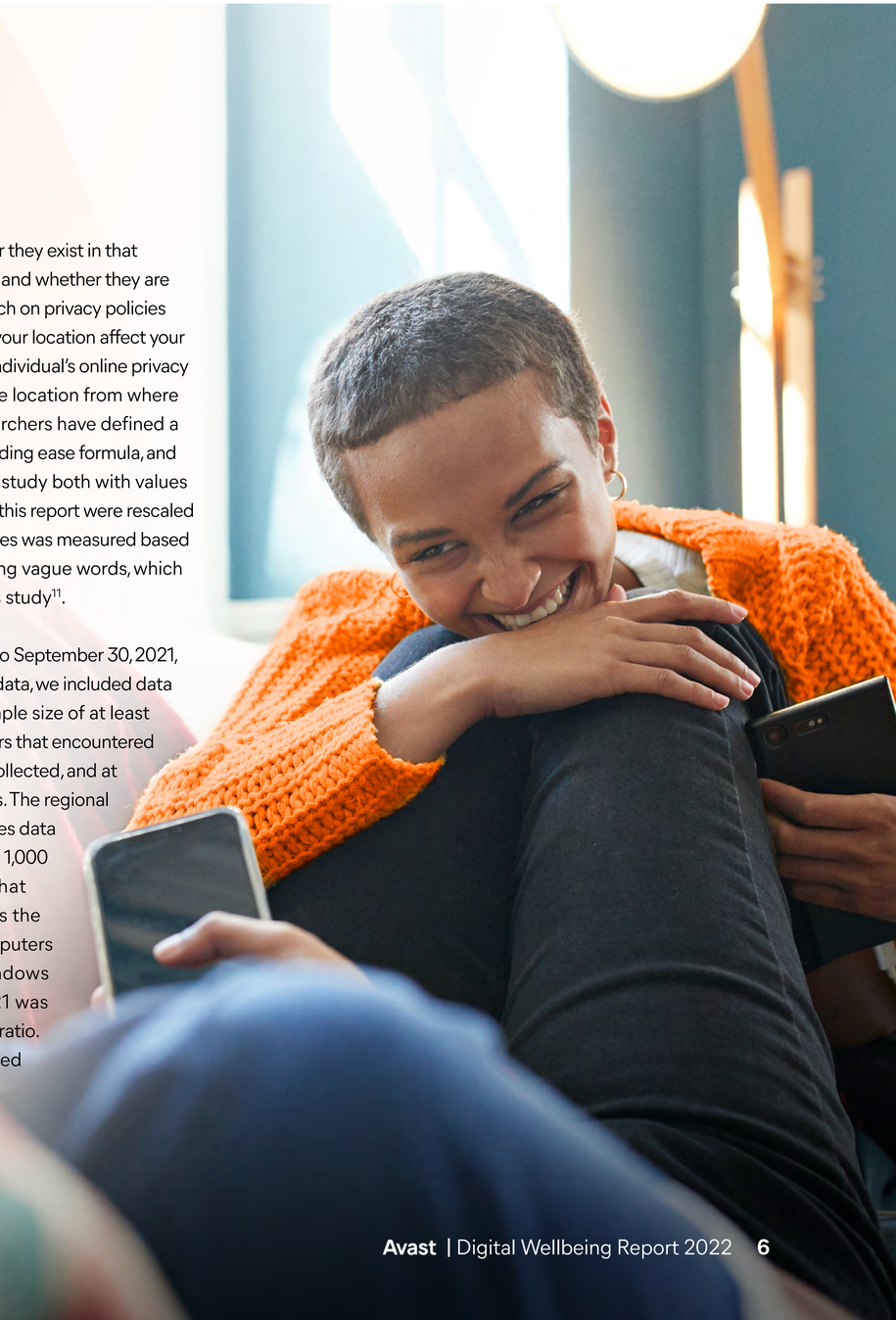
Freedom House's Index measures a state's level of internet freedom based on a set of methodological questions. The Index takes into consideration indicators such as: the free flow of information; the protection of free expression, access to information, and privacy rights; and freedom from both legal and extra-legal repercussions arising from online activities:

- Blocked social media or communications platforms
- Blocked political, social, or religious content
- Deliberately disrupted ICT networks
- Manipulated online discussions via progovernment commentators
- Passing of new law or directive increasing censorship
- Passing of new law or directive increasing surveillance or restricting anonymity
- Arrest, imprisonment or prolonged detention of blogger or ICT user for political or social content
- Physically attacked or killed (including in custody) blogger or ICT user
- Technical attacks against government critics or human rights organizations

The methodology includes 21 questions divided into three categories: obstacles to access, limits on content, and violation of user rights. Each question is scored on a varying range of points. Under each question, a higher number of points is allocated for a freer situation, while a lower number of points is allotted for a less free one. Points add up to produce a score for each of the subcategories, and a country's total points for all three represent its final score (0-100). Depending on the score, countries are classified as: Free, Partly Free and Not Free. Free countries score between 100-70, Partly Free countries between 69-40, while Not Free countries score between 39-0. The countries investigated by Freedom House presented an appropriate range of countries for our studies and were used as a basis for this research.

Avast used its own in-house data which it collects by providing services to its customers, including: risk ratio data, collected from Avast's threat detection network, which represents the average ratio of Avast users protected monthly from at least one threat divided by the total number of active Avast users protected; information about the age of operating systems used by Avast customers; and the presence of online privacy policies per state looking at three aspects, including whether they exist in that surveyed state, whether they are readable, and whether they are vague. More information on Avast's research on privacy policies can be found in a study titled: "How does your location affect your online privacy?", which looks into how an individual's online privacy varies throughout the world based on the location from where they connect to the internet. Avast researchers have defined a readability metric based on the Flesch reading ease formula, and a vagueness metric based on a previous study both with values ranging from 0-1, which for the purpose of this report were rescaled to 0-100%. The vagueness of privacy policies was measured based on segments in privacy policies containing vague words, which were labeled by annotators in a previous study[11].

For the risk ratio, data from July 1 through to September 30, 2021, was used. To provide statistically relevant data, we included data from countries and territories with a sample size of at least 10,000 computers belonging to home users that encountered threats during the months the data was collected, and at least 1,000 computers used by businesses. The regional breakdowns included in this report includes data from regions with a sample size of at least 1,000 computers belonging to home users that encountered threats during the months the data was collected and at least 100 computers used by businesses. To assess the Windows products used, data of September 2021 was used, as this data varies less than the risk ratio. For the privacy policies study, we included markets covered by the Press Freedom Ranking, and assessed privacy policies with the status of November 16, 2021.



[11] Logan Lebanoff and Fei Liu Automatic Detection of Vague Words and Sentences in Privacy Policies (University of Central Florida, August 28, 2018)

Key Findings

People in Free countries are less at risk from cyberattacks

As part of this study, our team of researchers found that people who live in Free countries are at a lower risk of encountering a cyberattack (30%) than people in countries that are Partly (36%), or Not Free (36%). By comparing the Freedom on the Net Index provided by Freedom House to the risk ratio provided by Avast's internal data, a relationship can be observed. As can be seen on Chart 1, countries that scored higher on the Freedom on the Net Index like Iceland, Estonia, Canada, and Costa Rica and which are by the standards set out by Freedom House considered Free countries, show a lower risk ratio score, especially when compared to the end of the spectrum. In fact, countries with lower Freedom on the Net Index like Saudi Arabia, Vietnam, Myanmar and China, or Not Free countries, showed a higher risk ratio and therefore a higher incidence of malware attacks against people and businesses.

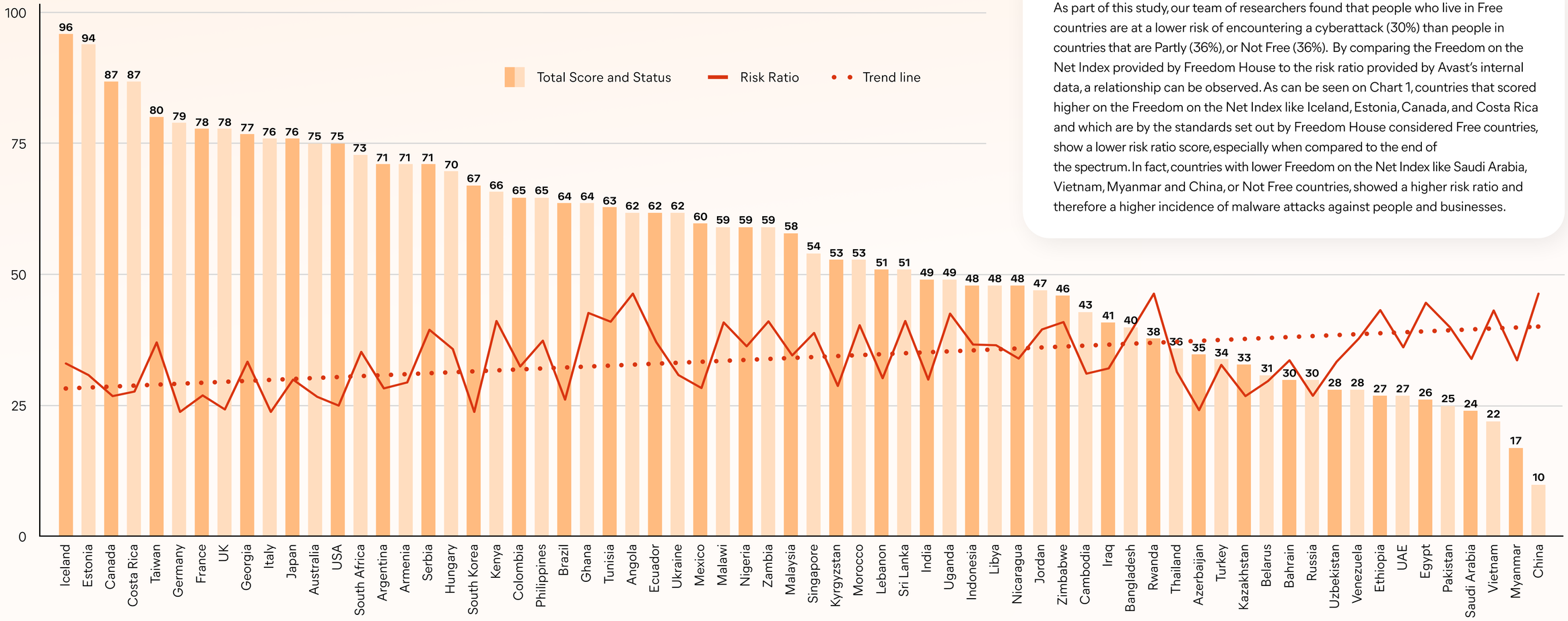


Chart 1: Total score and status of freedom according to the Freedom on the Net report (higher is better) vs. risk of encountering a cyberattack based on Avast data (lower is better)

Key Findings

People in Free countries are less at risk from cyberattacks

The increased risk ratio could be related to a number of potential factors, which were also identified in the Freedom on the Net Report. These could include violation of user rights, prohibition of encryption services, large scale state surveillance, data collection, and the presence of backdoors used for state surveillance. These findings show there exists an indirect correlation between the Freedom on the Net Index of a state and the risk incident, but not a direct causation. In Free states, citizens are less likely to be at risk of being targeted by malicious cyber activity.

Chart 2 also shows this indirect correlation. By grouping all identified Free countries, the number of attacks Avast had to block per month per state - the risk ratio - is at 30%, a lower figure than in countries considered Partly Free (36%) and Not Free (36%).

30% Free

36% Partly Free

36% Not Free

Chart 2: On average, people in Free countries have a lower risk of encountering a cyber attack than people in countries that are Partly, or Not Free. The above figure has a margin of error of <1%.

This suggests a correlation between a higher threat risk and the wealth of the countries, as measured in GDP per capita. As can be seen on Chart 1, lower wealth countries are at a higher risk of malware attacks: countries like Venezuela, Ethiopia, Pakistan, and Myanmar feature a higher risk ratio than wealthier countries. On the contrary, countries with a higher GDP per capita like France, Germany, and the United Kingdom, have a lower risk ratio and their citizens are less at risk. One interpretation could be that lower GDP per capita could lead to lower level of cyber education and therefore poor user security practices; such risky practices could include a greater use of torrent sites to access free content, games, movies, and a higher rate of consumption of illegal, more insecure content[12], which in turn can expose users to increased online risks.

[12] John F. Gantz, Joe Howard et al., "The Dangerous World of Counterfeit and Pirated Software. How Pirated Software Can Compromise the Cybersecurity of Consumers, Enterprises and Nations and the Resultant Costs in Time and Money." (IDC, March 2013)

Key Findings

People living in Not Free countries where older software is prevalent are more at risk from cyberattacks

To explore the correlation between wealth and the risk of encountering a cyberattack further, Avast looked at the age of operating systems as one possible reason. Avast's researchers found that users in Free countries on average use more up-to-date Windows products that are still supported by Microsoft with software and security updates, making them less prone to attacks, than users in Partly and Not Free countries.

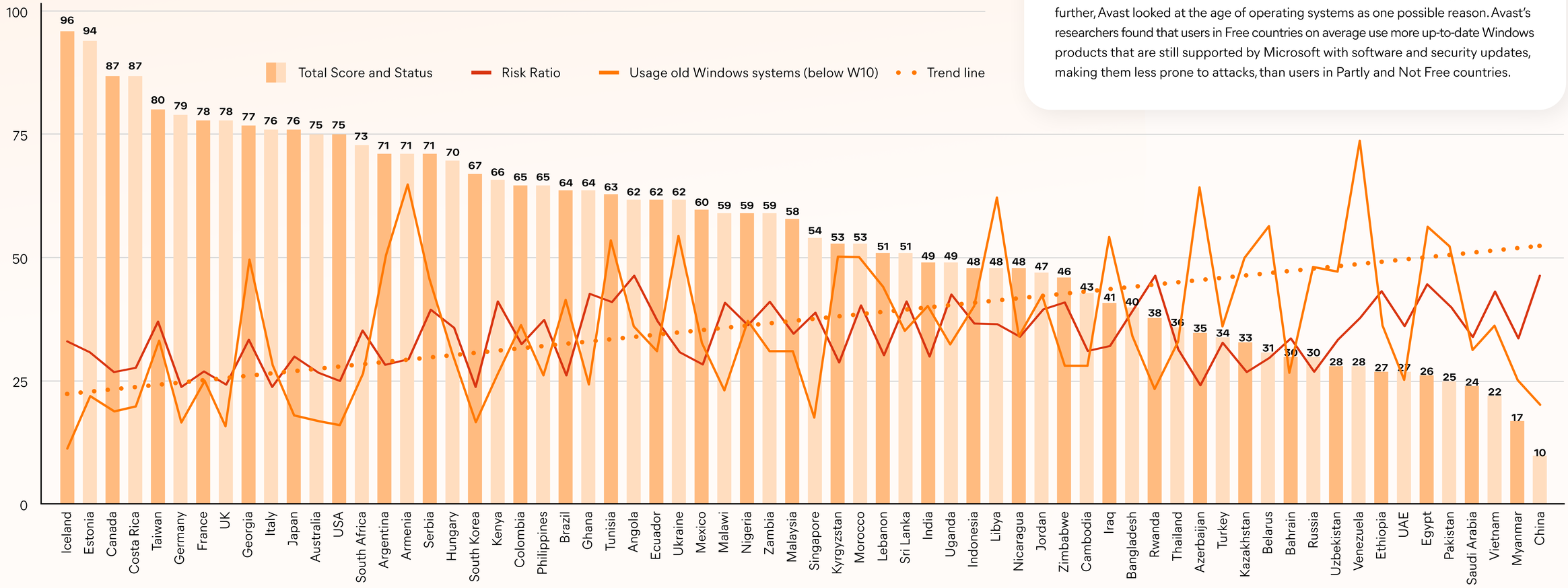


Chart 3: Users in Free countries on average use more up-to-date operating systems (that are still supported by Microsoft with software and security updates), making them less prone to attack

Key Findings

People living in Not Free countries where older software is prevalent are more at risk from cyberattacks

By comparing the ranking in the Freedom House Freedom on the Net Index to Avast's internal data (Chart 3), it can be inferred that in wealthier countries, such as those found higher up in the Index including Germany, France and the UK, users tend to have up-to-date operating systems, which can better guard them against cyberattacks.

Conversely, users in countries that scored lower on the Freedom on the Net Index, like Indonesia, Turkey, and Belarus, have on average a lower GDP per capita and tend to use more outdated operating systems, which increases the risk of a cyberattack.

Our researchers found that only 28% of users in Free countries are still using outdated desktop operating systems. By contrast, 38% percent of users in Partly Free countries are using outdated systems, and this figure is even higher in Not Free countries as ranked by the Freedom on the Net Index (41%). This is visualized in Chart 4.

Chart 4: Share of outdated operating systems people use in Free, Partly Free, and Not Free countries.

28% Free

38% Partly Free

41% Not Free

This could be explained by the relationship that exists between levels of freedom in a state and those of wealth, with Partly and Not Free countries also tending to experience lower levels of wealth and vice-versa. While this cannot be observed in all countries sampled, there is little doubt that if further explored, a correlation could be found between the two. Higher levels of overall wealth might facilitate the quick adoption of newer and more up-to-date technology, while lower levels of wealth could mean users need to keep using outdated operating systems despite the vulnerability and higher risks that they pose. This in turn leads to a higher risk ratio when it comes to cyberattacks.

Key Findings

Robust privacy policies have an impact on digital wellbeing

Building on the previous work carried out by Avast as set out in a research published in January 2022 which analyzed the impact of location and region in shaping a state's own notion of online privacy[13], Avast also found a relationship between a country's Freedom on the Net Index score and its stance on privacy laws.

As can be seen in Chart 5, presence of privacy policies can prevalently be observed at a higher rate in countries considered Free (70%) than in countries considered Partly and Not Free (52% and 47%). Free countries are more likely to have regulations in place set out to protect consumers in their jurisdictions, leading to more uptake on the adoption of privacy policies. It could also be suggested that regulations that set out the need to ensure that websites and platforms draft privacy policies, could indeed improve the digital wellbeing of people online.

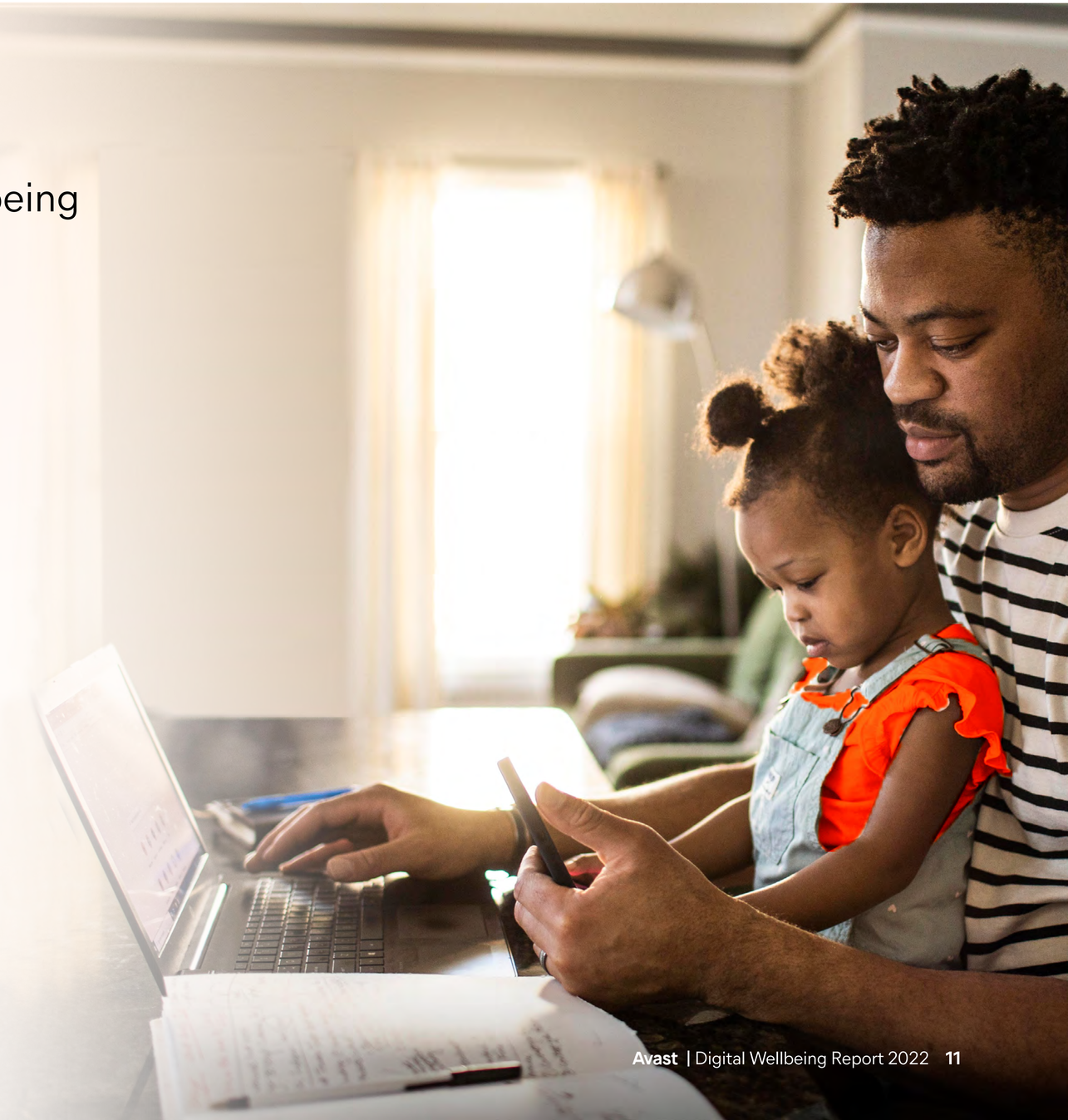
[13] Joe Bosso, "How Does Your Location Affect Your Online Privacy?" (blog.avast.com - January 5, 2022)

70%
Free

52%
Partly Free

47%
Not Free

Chart 5: The presence of privacy pages in Free countries is higher than in countries Partly or Not Free.



Avast also surveyed (Chart 6) data showing the "average vagueness" and "average readability" of privacy policies in English of different countries. Policies like the EU's General Data Protection Regulation (GDPR) or California's Consumer Privacy Act (CCPA) are designed to create more transparency and more understanding from consumers of their rights with regards to personal data and its collection by private and public entities. If these data protection policies are however unclear, the goal of these policies is missed.

The data Avast collected shows that even though privacy pages are more prevalent in Free countries, there does not appear to be a direct correlation between the readability and the vagueness of those privacy policies and the freedom index of that country.

For example, privacy policies in Free countries like the United States and Australia are rather vague and come with a lower readability, but in many European countries as well as in Japan, Taiwan and South Africa, privacy policies are easier to read and less vague.

Readability score also doesn't seem to be consistent across Europe despite the European Level top-down approach of the General Data Protection Regulation (GDPR). A country like Italy is on the lower end of the spectrum, making its privacy policies harder to read and vague, while Germany displays a higher level of readability and a low level of vagueness, meaning its privacy policies are on average easier to read and less vague.

What can be therefore argued is that while Free countries can ensure a higher level of digital wellbeing due to a higher presence of privacy policies protecting its citizens and consumers in their online activity, this does not ensure that these countries will have easily readable and clear privacy policies.

Key Findings

Even though privacy policies are more prevalent in Free countries, they are similarly vague and hard to read as in countries Partly or Not Free.

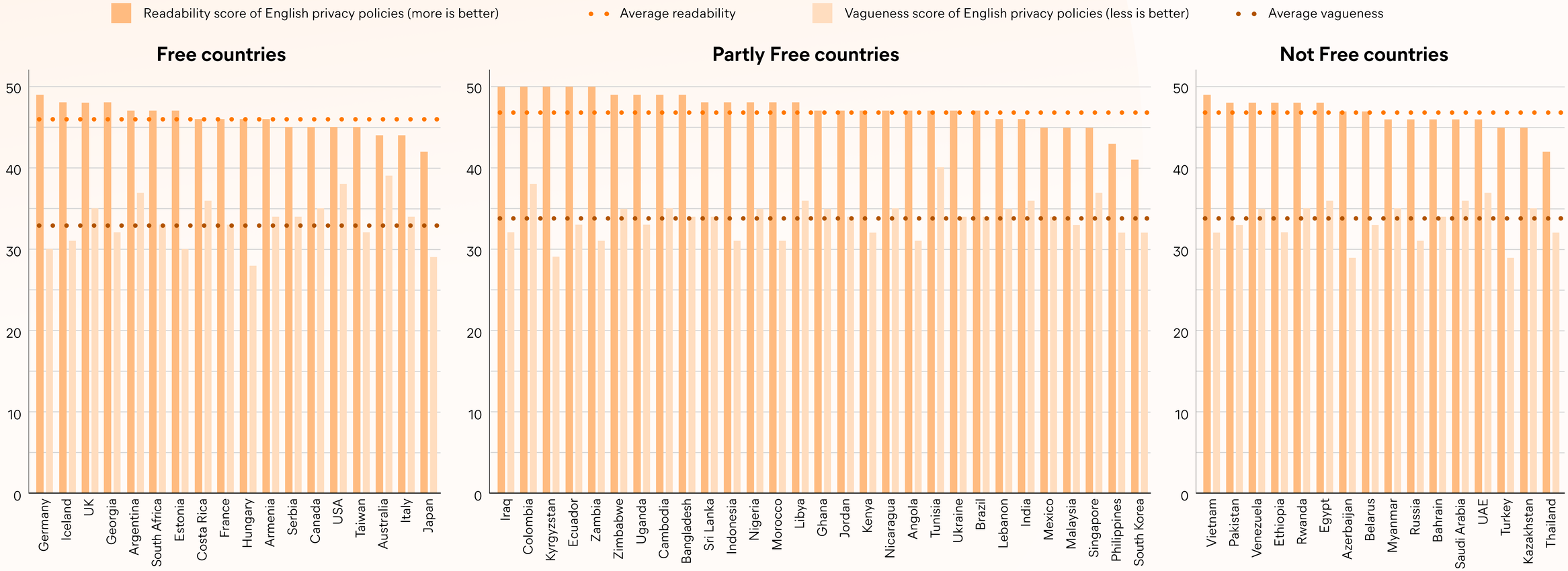


Chart 6: In many Free countries privacy policies are vague, or hard to read; Readability: <46% very difficult to read; 46%-58% difficult to read; Vagueness: "0% - no segments containing a vague word"; 100% - all of the segments containing vague words

The 2022 Russian invasion of Ukraine

On 24 February, in an escalation of the Russo-Ukrainian War started by Russia in 2014, Russian troops began military operations into Ukrainian territory and began to carry out a full-scale invasion in order to eliminate the country's democratically elected government.

The invasion has had a large impact on Ukrainian civilians as physical and digital attacks on Ukraine's infrastructure coupled with the loss of life from the extensive and bloody military operations have forced millions of Ukrainians to flee their homes in search of safety. In an attempt to mask the true reality of the conflict in Ukraine, Russia took unprecedented steps to limit access to the internet within its borders, significantly limiting its citizen's digital freedom.

At the national and international level, Russia started a large-scale state-sponsored disinformation campaign using state-sponsored news outlets, such as Russia Today, Sputnik, and alternative media sources which fall short of minimal journalistic standards and practices, as well as agents of influence willing to advance storylines into the media and social media stream. These outlets and accounts deployed various tactics with the overall aim of eroding trust in society and making it difficult for ordinary citizens to distinguish facts from lies, a common tool used by the Russian state propaganda machine[14]. These actions were further worsened by the impact of international sanctions, which forced most social networking sites, media outlets and private entities to pull out from the Russian market, effectively leaving Russians to consume carefully curated online content controlled by their government.

Illicit activity online has also increased due to the conflict. Cybercriminals are taking advantage of the vulnerabilities created by this unprecedented humanitarian crisis, attempting to set up online scams aimed at stealing personal and banking information from Ukrainians, as well as at people seeking to help Ukrainians from abroad. Avast has observed invitations from Ukrainian groups trying to gather international online consensus to voice their opposition against Russia by driving Distributed Denial of Service (DDoS) attacks. These tactics are criminal offenses and the tools used to carry them out are not secure, especially with regard to the collection of personal data. While they are being used to gather consensus at the moment, these tools could also be used to carry out attacks on targets outside of the Russian conflict. Lastly, large-scale DDoS attacks on Russian media sites, banks and energy companies have already been carried out, and uncoordinated attacks and threats of attacks from hacking groups, such as Anonymous, could have wider impact on more countries than those directly involved in this conflict.

Avast and its employees across the world strongly oppose war in all its forms and call on all parties in this conflict to lay down their physical and digital arms. Our mission is and will continue to be to protect digital freedom for a better, safer online world.

Photo by Alice Kotlyarenko on Unsplash

[14] Popken, Ben, "Russia's Age-Old Playbook for Attacking Democracy Exposed" (NBC, 6 November 2018)

Conclusions

This study has made several observations as to the correlation that can be found when examining the relationship between the digital wellbeing of a country and the freedom of its citizens online.

Despite its limitations, including the reduced scope and focus on three elements that affect digital wellbeing online (risk of cyberattacks, wealth and privacy), the following conclusions can be drawn from its findings.

Less Free countries face greater cyber risks

Firstly, our research found that there is a relationship between a country's Freedom on the Net Index and the risk of its citizens being exposed to cyberattacks. Lower risk levels can be observed in freer countries and higher risk levels can be found in countries with a lower index of Freedom on the Net. As a second finding, the study explored the age of software as a factor affecting the Freedom on the Net of citizens of a country. The study found that in countries where older operating systems are more prevalent for internet use, citizens are more at risk of cyberattacks. On the contrary, countries where newer software is more prevalent, can be considered less at risk of cyberattacks.

Existence of privacy policies does not mean sufficient privacy protection

Finally, this study looked at the prevalence of privacy policies in the countries surveyed and found that, on average, freer countries are more likely to have privacy policies in place. This, however, does not translate with regard to the readability or the vagueness of these policies, as no relationship between the countries' Freedom on the Net Index and the clarity of their privacy policies can be found.

These findings and the data processed by Avast altogether show that there exists a large gap between Free and Not Free countries when it comes to the digital wellbeing of their citizens. Citizens in less Free countries are more at risk of abuse by cybercriminals and are additionally not protected by their governments with regards to policies aimed at safeguarding their privacy, their right to freedom of speech, and the ability to access unbiased information online. The digital wellbeing of citizens of Free countries can therefore be considered to be higher, as policies are in place to protect their security and their privacy online.

Further Studies

While this study has only considered one core aspect of digital wellbeing, these results show that many disadvantages can combine to exacerbate challenging situations in different regions around the world. Further studies could explore in more detail the correlation between affluence and the presence of up-to-date software in different geographies, among other things. Investigating the correlation between a country's GDP and the presence of up-to-date software could amplify Avast's initial findings, and a study of a commonly used software and the presence of its latest updates on computers across different geographical regions could be relevant. This in turn could be compared to the GDP of different countries, to discern if a relationship can be found. Further studies could also dive into misinformation campaigns driven by governments, and their impact on citizens, as well as their impact on internet users around the world.

In the final sections of this study, Avast proposes five ways in which digital wellbeing could be improved for online users by recommending five actions for governments and private sector actors to undertake.

Policy Recommendations

Promoting digital wellbeing online requires attention and action from a range of stakeholders - government, industry, civil society, and consumers - to ensure policies across cybersecurity, privacy and education keep pace with the rapid evolution of technology and tactics of bad actors.

It is important that a holistic policy approach puts ethics and consumer focus at the forefront in order to promote trust and drive uptake of protective measures and adoption of best practice. Additionally, because of technology's propensity to quickly outpace regulation and the need for policymakers to ensure laws are flexible and future-proof, industry must take a leading role in reacting to emerging threats and voluntarily protect and promote digital wellbeing online.

One focus of this report has been on countries' wealth and that relationship to digital wellbeing. Cybersecurity, privacy, and identity protection products are products like any other which come at a cost to consumers, part of which is reinvested into maintenance as well as research and development to ensure bad actors' evolving threats are protected against. Less wealthy countries' governments and citizens may of course be less able to access the products and services to protect and promote digital wellbeing, but can profit from free options available on the market. As we live more of our lives online, just as the international community continues to promote development in the Global South, governments, international organizations, and private industry should collaborate to increase access to secure systems to ensure all internet users across the globe are protected against malicious activity.

As the internet and trends are evolving, innovation is needed to keep up with new risks consumers are facing, including cybersecurity, privacy, identity, and misinformation challenges, which is something policy makers should fight.

Policy Recommendations

Avast proposes below five areas of focus to enhance digital wellbeing online is improved across the globe, as well as five recommendations on how to achieve it:

Privacy Policies

Incentivize clear and understandable privacy policies with robust protections:

Online companies should commit to voluntary privacy policy codes of conduct setting out requirements for transparency and readability, as well as in relation to privacy principles such as data retention and purpose limitation. The end goal would be for anyone with a certain level of education to be able to read and understand these policies. For example, Flesch–Kincaid readability tests could be a good scale to measure this.

Product Cybersecurity

Futureproof cybersecurity regulation to account for technological advancements:

Policymakers and regulators should update current cybersecurity rules to reflect the proliferation and increased use of digital products, including interconnected devices, and services, ensuring products are secure by design with secure deployment settings. This should include a discussion around how long vendors are mandated to support products and operating systems with patches and security updates, so they can be used safely for a longer period of time.

Digital Education

Strengthen consumers' digital resilience and encourage digital hygiene:

Policymakers and regulators, in partnership with private industry, should conduct consumer-focused campaigns to promote education about the online security risks and cyber hygiene best practices, set against wider digital skills targets.

Digital Trust

Open standardisation of identity and trust regulations across online platforms and services:

The European Commission is intending an update to eIDAS, the electronic identification, authentic and trust services, with the intention to provide European citizens with digital wallets that store their ID and digital credentials safely, allowing for them to be used privately and securely across goverment and non-government services. If implemented effectively, eIDAS 2.0 can solve many problems including credential theft, as the ID is tied to the use by one individual only, and the problem of misinformation spread via bots which social networks could easily identify and block. It is an excellent opportunity for Europe to lead as an example for policymakers around the world, but care must be taken to avoid unintended consequences[14].

Multi Stakeholder Dimension

Share best practice on the evolving international threat environment:

International forums already consult and keep in close dialogue with industry, civil society, and academia however, to ensure government, businesses and consumers are best equipped to anticipate and protect against evolving cyber threats, greater sustained public private partnership is required[15].

[14] Avast Blog, "eIDAS 2.0: How Europe can define the digital identity blueprint for the world"

[15] Cybersecurity Tech Accord, "Multistakeholder Participation at the UN: The Need for Greater Inclusivity in the UN Dialogues on Cybersecurity," (2021)

Avast's Efforts to Improve Digital Wellbeing Worldwide

Avast has been providing cybersecurity solutions for over 30 years and today keeps over 435 million users around the world safe and private.

Avast has been providing cybersecurity solutions for over 30 years and today keeps over 435 million users around the world safe and private. Today's security goes beyond antivirus protection by providing support for personal privacy and identity, which is why Avast provides security, privacy protection and performance optimization for free.

Avast also developed a tool which is currently being tested in the United States, called News Companion, which uses information from fact checking sources to indicate whether a news site being visited is trustworthy, or known to spread misinformation. The goal is to provide people with context to understand the content, its origins, to empower people to better detect fake news on their own.

Beyond offering products which help improve people's digital safety, Avast believes that to improve people's online experiences we need to be hands-on and in contact with digital users to understand their concerns.

Through the Avast Foundation, Avast created the Spark Fund which is supporting projects to improve young people's digital lives. The Fund is supported via a Youth Leadership Board, working with young people across the world to listen to and understand the obstacles they face to being fully included, safe and free in the digital world. The Youth Board takes decisions on issues where Avast's funding should go, and which projects should be supported. Avast also established and continues to run the Be Safe Online Project which brings education about digital literacy and safety to school students in our native Czech Republic.

Avast also regularly engages with several organizations to achieve our mission to improve people's digital lives. Avast is a partner of Refuge UK, supporting its push against tech abuse, and a member of the Coalition Against Stalkerware, which actively fights against cyber stalking. As part of this Coalition, Avast is committed to fighting stalkerware on Android phones, and putting efforts into educating people about the existence of stalkerware and other means of stalking through tech. In Germany, Avast is a member of Deutschland sicher im Netz, an organization engaged in promoting digital safety in Germany. Avast has also participated in the organization's Digital Kompass, a roundtable for elderly citizens with the aim of educating them on online safety. In 2020, Avast has also joined the Internet Watch Foundation, a global charity dedicated to identifying and purging online child sexual abuse content. Avast has been helping IWF crack down on the creation and sharing of child abuse imagery by filtering out webpages that host this type of content.

Sources

Avast Digital Citizenship Report
Post-Pandemic Online Behavior
Avast (Avast September 2021) Link

How Does Your Location Affect Your Online Privacy?
Bosso, Joe (blog.avast.com January 5, 2022) Link

Multistakeholder Participation at the UN
Cybersecurity Tech Accord (2021) Link

FBI Internet Crime Report 2021
Federal Bureau of Investigations (FBI - Internet Crime Complaint Centre, 2022) Link

Freedom on the Net 2021
The Global Drive to Control Big Tech
Freedom House, 2021 Link

The Dangerous World of Counterfeit and Pirated Software.
How Pirated Software Can Compromise the Cybersecurity of Consumers, Enterprises and Nations and the Resultant Costs in Time and Money.
Gantz, John F., Joe Howard et al., (IDC, March 2013) Link

Russia blocks Google News after ad ban on content condoning Ukraine invasion
Hern, Alex (The Guardian - 24 March 2022) Link

The Global State of Democracy 2021
Building Resilience in a Pandemic Era
International Institute for Democracy and Electoral Assistance, 2021 Link

Automatic Detection of Vague Words and Sentences in Privacy Policies
Lebanoff, Logan and Liu, Fei (University of Central Florida, August 28, 2018) Link

FBI Sees Spike in Cyber Crime Reports during Coronavirus Pandemic
Miller, Maggie (The Hill – 16 April 2020) Link

From Instagram to PayPal
Russia's internet is being dismantled as a digital iron curtain descends
Purtill, James (ABC News – 22 March 2022) Link

Russia's Age-Old Playbook for Attacking Democracy Exposed Coronavirus Pandemic
Popken, Ben (NBC, 6 November 2018) Link

Avast warns users of crypto scams taking advantage of Ukraine conflict
Salat, Michal (Avast Blog, February 25, 2022) Link

eIDAS 2.0: How Europe can define the digital identity blueprint for the world
Tobin, Andy (Avast Blog, 2022) Link

Global Cybersecurity Outlook 2022
World Economic Forum, 2022 Link