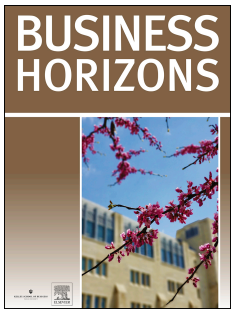

A $10 million question and other cybersecurity-related ethical dilemmas amid the COVID-19 pandemic

Aleksandra Pawlicka, Michał Choraś, Marek Pawlicki, Rafał Kozik

PII: S0007-6813(21)00133-6

DOI: https://doi.org/10.1016/j.bushor.2021.07.010

Reference: BUSHOR 1796

To appear in: *Business Horizons*

Please cite this article as: Pawlicka A., Choraś M., Pawlicki M. & Kozik R., A $10 million question and other cybersecurity-related ethical dilemmas amid the COVID-19 pandemic, *Business Horizons*, https://doi.org/10.1016/j.bushor.2021.07.010.

A $10 million question and other cybersecurity-related ethical dilemmas amid the COVID-19 pandemic

Aleksandra Pawlicka [a, *]
apawlicka@itti.com.pl

Michał Choraś [a, b]
mchoras@itti.com.pl

Marek Pawlicki [a, b]
mpawlicki@itti.com.pl

Rafał Kozik [a, b]
rkozik@itti.com.pl

[a] ITTI, Rubież 46, 61-612 Poznań, Poland

[b] UTP University of Science & Technology, Al. prof. S. Kaliskiego 7, 85-796 Bydgoszcz, Poland

***Corresponding author**

A $10 million question and other cybersecurity-related ethical dilemmas amid the COVID-19 pandemic

Abstract

Cybercrime and cybersecurity are like two sides of the same coin: They are opposites but cannot exist without each other. Their mutual relation generates a myriad of ethical issues, ranging from minor to vital. The rapid development of technology will surely involve even more ethical concerns, like the infamous example of a fitness tracking company allegedly paying $10 million worth of ransom. Every cybersecurity solution, tool, or practice has to be ethical by design if it is to protect people and their rights. To identify the ethical issues that cybersecurity/cybercrime might bring about in the future, we conducted the first broad and comprehensive horizon-scanning study since the COVID-19 pandemic arose. As we began this project, nobody had the slightest idea that the coming months would bring the COVID-19 pandemic, and that the reality we had known was about to change dramatically. As it soon became apparent, the deadly coronavirus brought completely new cybersecurity/cybercrime ethical dilemmas to light, and some of the ones known before were transformed or shifted. This article presents the results of our horizon-scanning study concerning the ethical dilemmas that emerged amid the COVID-19 pandemic.

KEYWORDS: Cybersecurity; Cybercrime; Data privacy; Human rights; COVID-19

1. Scanning the cybersecurity horizon in times of crisis

One may understand cybercrime as a wide array of illegal actions that are made possible by access to an information technology structure. They include electronic fraud, unauthorized access, ID theft, systems interference, and many more actions and new types of crime that came into existence with the creation of the original internet (Frank & Odunayo, 2013; Timmers, 2019). This led to increasing unease concerning the state of one's security in cyberspace, and thus the concept of cybersecurity was conceived. Its main goal is to secure cyberspace by eliminating vulnerabilities in systems and networks, thereby protecting the confidentiality and privacy of data. It comprises all kinds of best practices and technologies, tools and techniques, policies and concepts, as well as diverse assets like systems, devices, infrastructure, applications, data and software, and personnel; all of the above are aimed at preventing cybercrime and mitigating its effects (Frank & Odunayo, 2013). Thus, although cybersecurity is the contrary of cybercrime, they cannot exist without each other.

Ethics studies morality: it strives for determining what is right and what is wrong in an objective manner. It is supposed to come up with standard or proper behavior that would be widely approved by the public. This is not a simple task, since ethics is not the same as law; even if one disagrees with the law, one must obey it. Yet ethics are personal; every human defines their own set of ethical principles, the so-called personal ethical system. Thus, there are situations when one person considers their own actions entirely justifiable, even though others would not (BrainKart, n.d.; Faily et al., n.d.).

Owing to the remarkably diverse nature of cyberspace, ethical conduct there is all the more idiosyncratic. This does not mean that ethical considerations should be excluded from questions of cyberspace. On the contrary, considering ethics when performing any kind of cybersecurity planning ensures not only protection of the technical layer and but also the various freedoms of the individual and their basic human rights (Puddephatt & Kaspar, 2015; Shoemaker et al., 2019).

This is why we devised a broad, horizon-scanning study of the ethical issues that may arise in relation to cybercrime and cybersecurity. We conducted our study as part of the H2020 project PREVISION, and it was the first broad and systematic horizon-scanning study to detect societal and ethical dilemmas and emerging issues spanning over cybersecurity solutions.

This study involved systematic scanning of almost 4,000 diverse sources of knowledge, including scientific journals, media outlets, websites, magazines, books and book chapters, and conference proceedings, as well as several hundred social media entries. Then, 269 items were marked as relevant and analyzed in depth. Additionally, a survey was distributed among a group of experts during the project's plenary meeting; the results of the survey provided invaluable insights for the overall study. The study was designed in the second half of 2019 and conducted between January and June 2020.

After all the data had been gathered and analyzed, the so-called signals were identified and divided into strong and weak ones. Strong signals are the ones that are reported by the media or that exist in the public consciousness; the weak ones, when correctly interpreted, become important early signals, even though they might seem slight or insignificant at first (Rowe et al., 2017). The study went as planned and yielded some very significant results, which can be found in another of our articles (Pawlicka et al., 2021).

When the initial research for this article had just begun and the materials were being gathered, no one had the slightest idea what the coming months would bring. Even before the World Health Organization (WHO) declared the COVID-19 pandemic on March 11, 2020, the life we knew had started to change in unpredictable directions. As of September 2020, the disease is still spreading, and there seems to be no end to this situation; neither can we predict the course it is going to take.

Nevertheless, it is already clear that this new reality has brought about plenty of ethical dilemmas that were unheard of at the launch of this study. This article presents some of the identified cybercrime- and cybersecurity-related ethical issues that the deadly coronavirus has raised.

2. Cybersecurity- and cybercrime-related ethical issues that arose with the COVID-19 pandemic

As the everyday has become violently disrupted, social distancing has forced people to be more dependent on the internet (Fidler, 2020). Because the pandemic has forced millions of workers to work remotely, there has been a sharp increase in videoconferences, the usage of cloud-based storage, and online shopping (Rementeria, 2020). Most of the ethical questions related to this trend result from the fact that ill-willed cyberspace actors have been exploiting weaknesses and vulnerabilities to their own advantage (Council of Europe, 2020). As Gerg (2020) noted, "this unique environment is truly too good to pass up for many threat actors, no matter the ethical implications."

2.1. Malware, ransomware, phishing, and other cyberattacks

As ECHO (2020) concluded, "hackers are now exploiting the fact that the human factor is an even bigger weakness than before." Various types of planted malware have been reported in websites that inform the public on the course the pandemic is taking, or in websites that contain specific, pandemic-related keywords. Targeting vulnerable, confused, or scared people seeking information in uncertain times is profoundly unethical. Naturally, cyberattacks had been socially engineered before the pandemic—that is, they were always designed to prey on the fears and habits of people—but exploiting fear amid a pandemic takes sinister to a new level. This is "social engineering at its worst" (Gerg, 2020).

Coronavirus-specific topics have also been used as part of phishing email campaigns, that is, malicious emails used to steal users' personal data, credit card information, or other credentials. Some of the malicious messages have included asking for donations to the Centers for Disease Control (CDC), providing malicious links to "COVID-19 Tax Relief Documents", giving "drug advice" from a "World Health Organization doctor," and so on (Gerg, 2020; Pawlicka et al., 2020). Similarly, law enforcement agencies have warned that criminals have been disseminating emails offering COVID-19 drugs (of course, fake and nonexistent ones) while pretending to be governmental health organizations like the CDC. In fact, according to a United Nations report, "the current volume of coronavirus-related email lures, by far, represents the highest number of attacks the Cyberspace has witnessed" (UNODC, 2020).

The most popular phishing attempts that criminals have used are "open redirects" and "business email compromise." The former consists of a website automatically directing to another, malicious website, while the latter simply means that the email is designed to appear to come from a trusted, benign organization (Gerg, 2020).

Another key ethical issue concerns ransomware, i.e., malicious software that infects a computer, encrypts the user's data, and demands that the user pay a fee in order for the system to work again (Kaspersky, 2021). Although the attack itself has been known before, it is the shift in cybercriminals' behavior that is the most disgraceful, considering what kinds of people they target and how often they do it. In addition to this, large "organizations" (aka gangs) known for deploying and facilitating the payments of ransomware made official statements assuring users that special pandemic "discounts" on ransom amounts will be given to their "partners" (i.e., victims). They have also declared they will stop attacking healthcare facilities "until the stabilization of the situation with virus" (Gerg, 2020). Considering the fact that sensitive data leaks occurred just a few days after that pledge, it is hard to believe the criminals are being sincere, no matter what they might say.

Apart from targeting personal computers of individuals, criminals have been mercilessly exploiting cybersecurity weaknesses in healthcare. Hospitals and other healthcare facilities have been repeated victims of attacks, including ransomware (Abed, 2020). Healthcare-related websites have been repeatedly flooded with traffic in order to overcrowd them, to make them unstable, or to disable them completely. The WHO has been mercilessly targeted as well; the number of reported attacks have increased fivefold since the start of the pandemic (WHO, 2020). As Gerg (2020) puts it, "while it is certainly never okay to threaten the infrastructure of a healthcare organization, to deploy these attacks during a pandemic is egregious." Surely, the actions of cybercriminals have never put so many lives at risk before.

Another ethical problem concerns paying ransom. It would be easy to tell administrators to pay the money and to thus resume saving lives. In fact, ransomware has been causing so much damage that it has recently made the FBI soften their previous stance against paying ransom (Cytelligence, 2021). But this would mean that both individuals and organizations—often using taxpayers' money—financially support organized crime. And paying ransoms surely encourages more attacks. The fitness tracking company Garmin may not be a healthcare facility, but when their services went offline in June 2020 following a ransomware attack, they allegedly paid $10 million to be able to function again, sparking a fierce media debate on the ethics of the situation (Humphries, 2020). Another set of ethical dilemmas revolves around cybersecurity measures, or the lack thereof, and the inevitable trade-off between protecting one's privacy and helping governments to tackle the coronavirus.

2.2. Contact-tracing apps and big data

Several countries have integrated smartphones with big data in the fight against COVID-19, and some other governments have been encouraged to explore this strategy. This raises many concerns, including ethical ones, as so much personal data used to monitor behavior may be a significant threat to users' privacy. Additionally, there is a concern that cybersecurity and privacy issues may simply be overlooked in favor of technological possibilities that promise to get the pandemic under control.

More specifically, in several countries, contact-tracing apps have been deployed to help trace the spread of the virus. Tech giants and public health authorities have teamed up to create solutions as quickly as possible; even competing companies like Google and Apple have formed partnerships to help the cause. The technology was meant to inform people whether they had come in contact with someone infected with COVID-19. But many reports have raised concerns about the cybersecurity and privacy risks the

application programming interfaces (APIs) and related policies could bring about (Davis, 2020).

Despite contact-tracing apps' potential to become an extremely useful tool to help flatten the pandemic's curve, there are serious concerns. Experts argue that the system needs more data to be effective, but the question arises whether these apps could later be turned into tools for mass surveillance, and the resulting databases may even be used to expose the identities of the app's users. In other words, the data hoard may support "mission creep"—that is, the data could be later used, for example by the government, for purposes far beyond the original intent (Hamilton, 2020). Other risks include possible overreach, discrimination, and difficulty ensuring that participation is voluntary (Davis, 2020).

Yet another ethical issue concerns how the application will be phased out after the pandemic subsides, and whether the exit strategy has been properly designed (Hamilton, 2020). Moreover, vast amounts of sensitive data gathered in one place would attract hackers wanting to steal it, and any such data breach would have devastating effects, even to the point that "if the information ends up in the wrong hands or used in an inappropriate way, people could be stripped of their rights" (Davis, 2020).

Another point to consider is that threat actors often try to launch malicious clones of popular apps (Davis, 2020). This is also true for contact-tracing apps; hackers will again try to exploit vulnerable, innocent people and lure them into downloading fake, malicious apps (Davis, 2020).

The ethical issues may be the reason for the fact that, according to a study by the *Washington Post* and the University of Maryland, three in five Americans would either be unable to use contact-tracing systems or would not want to, which in fact makes the apps useless, as they rely on user participation (Davis, 2020). It has been argued that this is caused by the fact that "with privacy, an ounce of prevention is better than a pound of cure (Davis, 2020)." It is possible that people are just being apprehensive, or that citizens are simply not actually aware of what they exchange for the benefits that participation brings. Complete transparency, clear consent mechanisms, and simple opt-out procedures must be enacted for users' consent to be fully informed (Davis, 2020).

Finally, the pandemic also raises the question of governments' preparedness for such a situation. In case of an outbreak, can citizens trust their governments that the apps will be as secure as possible? Despite repeated warnings over the last 20 years, governments have miserably failed the trust of their citizens, and now people may simply be too hesitant to download and install any application, even if told to do so by the government (Fidler, 2020).

2.3. The Zoom issue

The COVID-19 outbreak led to an immense rise in the popularity of Zoom and other videoconferencing platforms, as they are used to hold meetings, classes, lectures, and even funerals. But it turned out that the Zoom platform came with some weaknesses that put the privacy and well-being of millions of people at risk (Fidler, 2020). Shockingly, the vulnerabilities had been known for years but were not addressed properly. The company explained that such programs are very complex, so some issues might not be found ahead of time. This leads to an ethical dilemma: Companies are well aware that their applications contain flaws, some of them potentially dangerous. Despite this, they

assume that the problems can be patched later, without minimal costs to the company, instead of striving for security proactively. This drive to save company money and resources leads to jeopardizing customers' data and privacy (Fidler, 2020). Companies find it easy to adopt such practices, as they do not seem to break any laws. One should therefore question whether these company policies, which do not prioritize citizens' security and thus indirectly let their security be undermined, can still be called ethical. Other, less mentioned but still significant cybersecurity/cybercrime-related ethical issues include cyberespionage, deepening social inequalities and exclusiveness, and fake news about COVID-19.

2.4. Cyberespionage

Researchers have noticed that the COVID-19 situation has led to a sharp increase in cyberespionage as companies compete to develop a cure or vaccine for the deadly virus. The involved parties have been targets of infiltration by governments and everyone who would like to gain access to this technology as soon as possible (Fidler, 2020). One of the most recent examples of such attacks was the hack of the European Medicines Agency in December 2020, when hackers stole documents related to the Pfizer and BioNTech COVID-19 vaccine and promptly released them online (Porter, 2021).

2.5. Deepening social inequalities and exclusiveness

The social inequalities in education and work become deeper for people with poor internet access or without access at all. Actually, although schools in most pandemic-affected areas closed and resorted to teaching exclusively online, some reports show that during the lockdown, as much as 40% of students were unable to continue their education (World Council of Churches, 2020). Having access to the internet is more and more often thought to be an emerging human right because it contributes to and complements one's freedom of expression, speech, and information exchange (Shackelford, 2017). If this is true, then depriving people of internet access becomes a burning issue of ethics (Barry, 2020).

2.6. Fake news concerning COVID-19

Another ethical concern relates to the flood of fake news. Fake news may be ridiculous and useless, but it cannot simply be dismissed, as it may also be misleading and thus bear extremely serious consequences. For example, hundreds of people allegedly died because they believed the fake news about the curative effects of ingesting hydroxychloroquine, soap, or large amounts of alcohol (Spring, 2020). As with phishing campaigns, some people will disseminate false information just for the sake of clicks, no matter how unethical their behavior may be or what horrific results it may bring in the long run (World Council of Churches, 2020).

3. The new world order post-COVID-19

The COVID-19 pandemic has changed the world we knew, and the future is still uncertain. As Mauro (2020) said, "we must be ready to have a conversation about the … dimensions of the cybersecurity threats we will face during the COVID-19 pandemic." How governments, policy makers, cybersecurity specialists, and citizens address these new, emerging ethical dilemmas will directly influence the future world. Although the ultimate influence of the pandemic over cyberspace and its ethical dilemmas is yet unknown, it is already apparent that "COVID-19 is a game changer … there will be a new world order post COVID-19 that will have an impact on digital liberties" (World Council of Churches, 2020). In addition, it is unlikely that ill-willed cyberspace actors will refrain from exploiting vulnerabilities; instead,

people must be educated so they can protect their property and privacy themselves, by avoiding risky behaviors, being vigilant, and maintaining proper cyber hygiene.

Our horizon-scanning study of the possible ethical dilemmas has shown yet again that cybersecurity, although seemingly a strictly technical issue, is in fact a matter of ethics. No matter how harsh the global situation may be, cybersecurity must always be about people, and it must aim to protect their rights and freedoms.

[Insert Acknowledgment Here]

References

Abed, S. (2020, May 5). Coronavirus, cybersecurity, and contact tracing conflicts. *Healthcare IT News*. Available at https://www.healthcareitnews.com/blog/europe/coronavirus-cybersecurity-and-contact-tracing-conflicts

Barry, J. J. (2020, May 26). COVID-19 exposes why access to the internet is a human right. *OpenGlobalRights*. Available at https://www.openglobalrights.org/covid-19-exposes-why-access-to-internet-is-human-right/

Council of Europe. (2020). *Cybercrime and COVID-19*. Available at https://www.coe.int/en/web/cybercrime/cybercrime-and-covid-19

Cytelligence. (2021). *Cybersecurity in 2020*. Available at https://cytelligence.com/cybersecurity-in-2020/

Davis, J. (2020, May 20). COVID-19 contact tracing apps spotlight privacy, security rights. *Health IT Security*. Available at https://healthitsecurity.com/news/covid-19-contact-tracing-apps-spotlight-privacy-security-rights

ECHO. (2020, April 8). *The COVID-19 hackers mind-set*. Available at https://echonetwork.eu/wp-content/uploads/2020/04/20200408-ECHO-WhitePaper-Hackers-Mindset-FINAL.pdf

BrainKart. (n.d.). *Ethical issues in computer security*. Available at http://www.brainkart.com/article/Ethical-Issues-in-Computer-Security_9739/

Faily, S., McAlaney, J., & Claudia, I. (n.d.). *Ethical dilemmas and dimensions in penetration testing*. Available at https://cybersecurity.bournemouth.ac.uk/wp-content/papercite-data/pdf/fami15.pdf

Fidler, D. P. (2020, March 30). Cybersecurity in the time of COVID-19. *Council on Foreign Relations*. Available at https://www.cfr.org/blog/cybersecurity-time-covid-19

Frank, I., & Odunayo, E. (2013). Approach to cyber security issues in Nigeria: Challenges and solution. *(IJCRSEE) International Journal of Cognitive Research in Science, Engineering, and Education, 1*(1). Available at https://www.ijcrsee.com/index.php/ijcrsee

Gerg, C. (2020, May 18). How hackers are exploiting COVID-19. *Security Magazine*. Available at https://www.securitymagazine.com/articles/92411-how-hackers-are-exploiting-covid-19

Hamilton, I. A. (2020, April 29). 170 cybersecurity experts warn that British government's contact tracing app could be used to surveil people even after coronavirus has gone. *Business Insider*. Available at https://www.businessinsider.com/cybersecurity-experts-uk-government-contact-tracing-surveillance-2020-4?r=US&IR=T

Humphries, M. (2020, August 4). Report: Garmin paid the ransomware demand. *PC Magazine*. Available at https://www.pcmag.com/news/report-garmin-paid-the-ransomware-demand-wastedlocker

Kaspersky. (2021). *What is ransomware?* Available at https://www.kaspersky.com/resource-center/definitions/what-is-ransomware

Mauro, A. (2020, April 9). Working from home during the coronavirus pandemic creates new cybersecurity threats. *The Conversation*. Available at https://theconversation.com/working-from-home-during-the-coronavirus-pandemic-creates-new-cybersecurity-threats-134954

Pawlicka, A., Jaroszewska-Choras, D., Choras, M., & Pawlicki, M. (2020). Guidelines for stego/malware detection tools: Achieving GDPR compliance. *IEEE Technology and Society Magazine, 39*(4), 60–70.

Pawlicka, A., Choraś, M., Kozik, R., & Pawlicki, M. (2021). First broad and systematic horizon scanning campaign and study to detect societal and ethical dilemmas and emerging issues spanning over cybersecurity solutions. *Personal and Ubiquitous Computing*. Available at https://doi.org/10.1007/s00779-020-01510-3

Porter, S. (2021, January 14). Pfizer COVID-19 vaccine data leaked by hackers. *Healthcare IT News*. Available at https://www.healthcareitnews.com/news/emea/pfizer-covid-19-vaccine-data-leaked-hackers

Puddephatt, A., & Kaspar, L. (2015, November 18). Cybersecurity is the new battleground for human rights. *Open Democracy*. Available at https://www.opendemocracy.net/en/cybersecurity-is-new-battleground-for-human-rights/

Rementeria, A. (2020). Pandemic increases cybersecurity risks. *Legal Ethics in Motion*. Available at https://www.legalethicsinmotion.com/2020/05/pandemic-increases-cybersecurity-risks/

Rowe, E., Wright, G., & Derbyshire, J. (2017). Enhancing horizon scanning by utilizing pre-developed scenarios: Analysis of current practice and specification of a process improvement to aid the identification of important 'weak signals.' *Technological Forecasting and Social Change*, *125*, 224–235.

Shackelford, S. (2017, February 13). Should cybersecurity be a human right? *The Conversation*. Available at https://theconversation.com/should-cybersecurity-be-a-human-right-72342

Shoemaker, D., Kohnke, A., & Laidlaw, G. (2019). Ethics and cybersecurity are not mutually exclusive. *EDPACS*, *60*(1), 1–10.

Spring, M. (2020, May 27). Coronavirus: The human cost of virus misinformation. *BBC News*. Available at https://www.bbc.com/news/stories-52731624

Timmers, P. (2019). Ethics of AI and cybersecurity: When sovereignty is at stake. *Minds and Machines, 29*(4), 635–645.

UNODC. (2020, May 10). *COVID-19: Cyber threat analysis*. Available at https://www.unodc.org/documents/middleeastandnorthafrica//2020/COVID19/COVID19_MENA_Cyber_Report_EN.pdf

WHO. (2020, April 23). *WHO reports fivefold increase in cyber attacks, urges vigilance*. Available at https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance

World Council of Churches. (2020, May 15). Web meeting focuses on cyber ethical challenges of COVID-19. *World Council of Churches*. Available at https://www.oikoumene.org/en/press-centre/news/web-meeting-focuses-on-cyber-ethical-challenges-of-covid-19

Acknowledgment

This work has been performed under the H2020 833115 project PREVISION, which has received funding from the European Union Horizon 2020 Programme. This article reflects only the authors' views; the European Commission is not liable for any use that may be made of the information contained herein.