The Ethical Vacuum in Cybersecurity: Why Professionals Are Still Navigating Alone

Carla Vieira | 2023

This Literature Review sought to analyse the scientific research done in the past 4 years on the Ethics of Cybersecurity with the purpose of the creation of a “Universal Code of Conduct” for the profession. 8 peer-reviewed articles form the backbone of this review; however other industry-relevant publications also ought to be mentioned as they illustrate the outcry for guidelines, if not the said “Universal Code of Conduct”. The discussion often gravitates around the most prominent conflicts: data privacy from governments and security professionals, whistleblowing, ethical hacking, Machine Learning and Artificial Intelligence possibly making biased ethical decisions and the weaponization of technology (Pawlicka et al, 2023). Despite the pressing need for guidance in the face of a rapid-paced evolution of emerging technologies, it seems to be the consensus that ethical challenges in cybersecurity cannot be resolved in a general way.

When it comes to data privacy, research conducted in 2020 found that general ethical review committees actually lack awareness of the core dilemmas in cybersecurity so it is not enough to call upon them for guidance (Maknish, K. et al). This same research concludes that a clear and enforceable code of conduct for the profession is much needed (Maknish, K. et al). Another group of researchers, for instance, argue that with ethical standards still being under development, it creates potential grey areas that facilitate privacy, ethics and data breaches (Dhirani et al, 2023). There is still another question regarding how much data should the security professional know to be able to protect that same data from cybercriminals (Pawlicka, 2023). This dilemma of data privacy goes at present beyond the typical maintenance of professional confidentiality by the cybersecurity professional (Maknish, K. et al). It also entails emerging technologies - namely Artificial Intelligence (AI) and Machine Learning (ML) - under the scope of the awareness that the cybersecurity professional (with or without an established Code of Conduct) will ultimately be the one dealing with the security of the huge amount of very sensitive data being collected. In that light, data privacy concerns include, among other emerging technologies, self-driving vehicles (Dhirani et al., 2023), state-of-the-art neurotechnologies (Pawlicka et al., 2023) and the use of AI to ensure the sovereignty of nations (Timmers, 2019).

Currently, each nation or region has its own set of guidelines and ethical standards (Dhirani, 2023), which leads to confusion and complexity for the cybersecurity professional to stay compliant. Lack of compliance could in turn lead to fines to the organisation one works for, which raises ethics and integrity issues. As an example of conflict, in the multitude of ways someone could become a certified cybersecurity professional, some issuing bodies have created their code of conduct as a condition for the certification to become and stay valid. It does not, however, seem to be broad enough to solve conflicting issues. For example, according to the ISC2 Code of Ethics, the ISC2 Certified Cybersecurity professional must *"Act honourably, honestly, justly, responsibly, and legally"* (ISC2 Code of Ethics, 1996-2023). If so, would an Australian cybersecurity professional breach these code values by complying with the Assistance and Access Act 2018 (Federal Register of Legislation, 2018), which technically undermines the power of cryptography to keep data private and safe for everyone (Bocetta, 2019)? It becomes even trickier knowing that organisations mostly work with a hybrid stack. This blend of third-party and organisation-owned technology may create a grey area even further, due to the lack of clear oversight in addition to the lack of clear and enforceable ethical guidelines for the conduct of the cybersecurity professional (Watters, A., 2023).

The second dilemma highlighted by this literature review is the lack of guidelines or perhaps a hierarchy of authority when conflicting interests clash in a whistleblowing scenario. Edward Snowden exposed abusive governments' oversight of regular citizens, not terrorists, and had to flee the country (Boussios, 2023). Another example is Chelsea Manning, who exposed the wrongdoings of the US government which she came to know while she was an Intelligence Analyst in the US Army. She exposed state crimes, political corruption, illegal use of wiretaps, murders and more. The result was a 35-year sentence (later commuted), while the criminals she exposed are yet to be brought to justice (Boussios, 2023). These notorious cases of cybersecurity professionals becoming whistleblowers have changed the public perception of privacy and the right to know when the public is being watched. This may normalise and open up room for ethical cybersecurity decisions from the regular citizen's perspective, rather than the Government's (Boussios, 2023).

The other side of the whistleblowing spectrum exemplifies corporate cybersecurity professionals who may have come across a zero-day vulnerability that could potentially expose the personally identifiable information of millions of people but be instructed to keep quiet based on a profit-focused decision. In each case, where should the cybersecurity professional stand? Should one follow their heart despite potentially facing lawsuits? Legal does not always equal ethical (Pawlicka, 2023). People being able to report all forms of cyber misconduct, such as data breaches or vulnerabilities in systems, and being protected by law would ultimately require proper systems in place so that it would be clear who the professional is responding to (Pawlicka, 2023).

When refering to the lack of an overarching Code of Conduct for cybersecurity professionals, the vast majority of scientific material published lately discusses ethical dilemmas like the ones mentioned above. Very few authors, however, have come up with a proposed solution. Formosa et al., in "*A Principlist Framework for cybersecurity ethics."* (2021) argue that general principles as guidelines in individual cases would be of great benefit. The 5 principles proposed are beneficence, non-maleficence, autonomy, justice, and explicability (Formosa et al., 2021). The authors acknowledge these principles can conflict with one another, therefore each context must be balanced. In their article, the 5 principles are tested on 4 common cybersecurity dilemmas: "penetration testing, distributed denial of service attacks (DDoS), ransomware and system administration" (Formosa et al., 2021). Ethical trade-offs do happen but overall the balancing of the 5 principles seems to satisfy the ethical guidance needed in each specific case study.

Another example of an author who tries to offer a solution is Paul Timmers in *Ethics of AI and Cybersecurity When Sovereignty is at Stake* (2019) and the Global Common Good

approach (Timmers, 2019). Since the United Nations has the tradition of contributing to the common global good in other areas, why not in cybersecurity? Could the United Nations be the mediator between the private sector, nations and the Internet community? Such collaboration would be intergovernmental in a private-public partnership setting, he argues. In his view, adopting cyberspace as a global common good will enable us to have the common ethics of global cyberspace. Therefore this would imply security-by-design and privacy-by-design in emerging technologies (Timmers, 2019). The author, thus, suggests some policy recommendations but this is still not the overarching Code of Conduct for Cybersecurity this literature review seeks to analyse.
This comprehensive research has not found any author claiming it is possible to create a Universal Code of Conduct or Universal Code of Ethics for Cybersecurity professionals. Instead, there is plenty of material explaining why this is a task full of challenges, justifying therefore the lack of such a Code. This is a widely accepted idea in the industry and it seems to be portrayed on a puzzled but not all negative note when only dealing with corporate issues the cyber professional may face as an individual (e.g. pen-testing dilemmas, who to sell to zero-day exploits, whistleblowing, etc).

The latent gap in the literature identified by this review would be to explore the scenario of the ethical conduct of the cybersecurity professional shaping the path ahead of the discussed emerging technologies. If at the most singular point of development, namely the individual professional, ethical behaviour is embedded and framed by clear guidelines, perhaps the final product would be ethical-by-design. In addition, overall the idea of an overarching Code of Conduct for the profession seems to have been long abandoned. When looking for articles on Google Scholar and USC Library, the search "ethical dilemmas in cybersecurity" returns mostly AI-related ethical issues. The search string "code of conduct cybersecurity" on the same databases does not return even one relevant peer-reviewed publication on the topic in the past decade.

In conclusion, it is worth mentioning plenty of Codes of Conduct have been created but overall the lack of sanctions if the codes are broken may undermine its relevance (Maknish, K. et al). The existence of a Code of Conduct to abide by would be a very strong argument for the professional trying to resist instructions to act unethically (Maknish, K. et al). They are also not comprehensive and overarching. As a prime example, the existing attempts for a Code do not offer guidance to the very relevant scenario of a professional needing to ethically deal with vulnerabilities. In the era of state-of-the-art neuro technologies being developed, how much would a zero-day exploit be worth in such a powerful scenario? Could the vulnerability researcher be tricked into selling to the wrong person if there are no clear guidelines instructing the path that should be followed Pawlicka, 2023)? The years ahead will hopefully show that these burning ethical questions and dilemmas in cybersecurity paved the way for a more transparent cyberspace, with or without a Universal Code of Conduct for Cybersecurity.

Reference List

Bocetta, S. (2019 Feb 14) *Australia's New Anti-Encryption Law is Unprecedented and Undermines Global Privacy*. FEE Stories Website. Available: https://fee.org/articles/australia-s-unprecedented-encryption-law-is-a-threat-to-global-privacy/

Boussios, E. G. (2023), *Snowden, Manning & the new knowledge cyberclass*. In Emerald Insight Digital policy, regulation and governance 25(4). Available https://www-emerald-com.ezproxy.usc.edu.au/insight/content/doi/10.1108/DPRG-12-2022-0147/full/html

Dhirani, L.L.; Mukhtiar, N.; Chowdhry, B.S.; Newe, T. Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review. Sensors 2023, 23, 1151. https://doi.org/10.3390/s23031151

Federal Register of Legislation (2018) *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018.* Federal Register of Legislation Website. Available: https://www.legislation.gov.au/Details/C2018A00148

Formosa, P., Wilson, M., Richards, D. (2021) 'A Principlist Framework for Cybersecurity Ethics' 109 *Computers & Security* 102382. Elsevier. Available: https://usc.primo.exlibrisgroup.com/permalink/61USC_INST/3ct1hk/cdi_crossref_primary_10_1016_j_cose_2021_102382

ISC2 (1996-2023). *ISC2 Code of Ethics*. Available: https://www.isc2.org/Ethics

Kozhuharova, D., Kirov, A., & Al-Shargabi, Z. (2022). Ethics in cybersecurity. *What are the challenges we need to be aware of and how to handle them?* In J. Kolodziej, M. Repetto, & A. Duzha (Eds.), *Cybersecurity of digital service chains. Lecture notes in computer science* (Vol. 13300). Springer.

Macnish, K., Ham, J., (2020) *'Ethics in Cybersecurity Research and Practice'* 63 *Technology in society* 101382. Available: https://usc.primo.exlibrisgroup.com/permalink/61USC_INST/3ct1hk/cdi_proquest_journals_2478256946

Martinho, A., Herber, N., Kroesen, M., Chorus, C. (2021) *Ethical issues in focus by the autonomous vehicles industry*, Transport Reviews, 41:5, 556-577, DOI: 10.1080/01441647.2020.1862355

Pawlicka, A., Pawlicki, M., Kozik, R., Choraš, R. S. (2023), *"What will the future of cybersecurity bring us, and will it be ethical? The hunt for the black swans in cybersecurity ethics".* IEEE Access. Available: https://usc.primo.exlibrisgroup.com/permalink/61USC_INST/3ct1hk/cdi_doaj_primary_oai_doaj_org_article_7979811730ce4bb08d68f98dd9dfe03

Popa, E.O., van Hilten, M., Oosterkamp, Bogaardt, M. (2021) The use of digital twins in healthcare: socio-ethical benefits and socio-ethical risks. *Life Sci Soc Policy* 17, 6. Available: https://rdcu.be/djYWo

Sanders, L. (2021 Feb 11), *Can privacy coexist with technology that reads and changes brain activity?* Science News Website. Available:

https://www.sciencenews.org/article/technology-brain-activity-read-change-thoughts-privacy-ethics

Timmers, P. (2019), *Ethics of AI and Cybersecurity When Sovereignty is at Stake*, In Minds and Machines (2019) 29:635–645 in https://doi.org/10.1007/s11023-019-09508-4

Watters, A. (2023 Feb 03) *5 Ethical Issues in Technology to Watch for in 2023* CompTia Website. Available:
https://connect.comptia.org/blog/ethical-issues-in-technology