Cyber Citizenship: Navigating the Digital Landscape Coaching

Ashley G. Yousufzai, PhD¹ & Jeffrey T. Hancock², PhD,

Presented at Ethics the Heart of Coaching: Expanding the Boundaries of Ethical Thinking & Practice
Virtual Conference: www.coachingethicsforum.com
Hosted by the Coaching Ethics Forum,
8 & 9 December, 2023

ABSTRACT: The coaching industry is evolving towards unprecedented access, scale, and globalization. The rise of digital coaching greatly enables this transformation but also requires adaptation of traditional coaching models. This panel discussion explored the construct of “cyber citizenship” in coaching, defined by three pillars: digital literacy, global civics, and cybersecurity. Within digital literacy, we explore the importance of knowing how to digest information, sort fiction from fact, learn about the development of new technologies (e.g. artificial intelligence and machine learning) and adapt one’s skills to the digital landscape. Within global civics, the discussion focused on the importance of establishing and nurturing trust in a culturally competent way with clients in the digital realm. The session ended with a discussion of cybersecurity best practices to safeguard sensitive client information and protect both the coach and the client from potential online threats. This session aimed to empower coaches to navigate the digital landscape with integrity, gain awareness of the threats and opportunities, and ultimately, foster a safe and effective digital coaching environment for all.

Keywords: Cyber Citizenship, Global Civics, Cybersecurity, Digital Literacy, Digital Coaching

Session Type: Interactive Panel Discussion

Cyber Citizenship: Navigating the Digital Landscape in Coaching

Advancements in technology have greatly influenced the field of coaching, facilitating easier connections with clients across different time zones and cultures. However, with these advancements comes the added responsibility of balancing the efficiency offered by technology with maintaining trust and safety within the coaching relationship. Cyber citizenship, a concept made popular by Singer and McConnell

1. Ashley G. Yousufzai, PhD. BetterUp, Ann Arbor, MI, USA. Email: amguidroz@gmail.com
2. Jeffrey T. Hancock. Department of Communication, Stanford University, Stanford, CA, USA. Email: Hancockj@stanford.edu
(2021), presents a collection of behaviors needed to thrive in an online digital environment. With digital coaching, this includes revisiting assumptions and best practices inherent to traditional coaching and considering them within the context of the digital landscape. By building digital literacy, being aware of global civics and minding best practices in cybersecurity, coaches will be equipped to maintain trust and safety while navigating the evolving digital landscape (Singer et al., 2021).

**Digital Literacy**

The first pillar of cyber citizenship, digital literacy, refers to a coach’s ability to effectively use and evaluate information and technologies. Developing digital literacy skills enables coaches to incorporate digital tools into their practice, discern fact from fiction, navigate online platforms, and adapt to the ever-changing digital world. Several examples discussed in the presentation included how one can discern the truthfulness of information shared via social media posts and what to look for to ensure that we are not contributing to the dissemination of “fake news”. Without digital literacy, coaches run the risk of using digital tools ineffectively or unintentionally compromising the quality and safety of the coaching process.

Additionally, digital literacy involves staying aware of how technology is evolving within the coaching space. For example, the use of Artificial Intelligence (AI) has the potential to increase efficiency, reduce cognitive load, and improve the overall coaching experience for both coaches and clients. However, AI is still in its infancy and bias is known to exist in the initial training data and algorithms that AI tools are built upon (IBM, 2023). The responsible use of AI therefore requires awareness that bias may exist and enacting AI governance practices to minimize the impact of bias in development of AI tools. This will not only benefit coaches, but also their clients, organizations and society as a whole by ensuring that AI tools do not move past what makes coaching so special - the nuance of a moment that provides the catalyst for personal change.

**Global Civics**

The second pillar, global civics, addresses the importance of cross-cultural competence in a global digital environment. With the widespread use of digital coaching platforms, coaching has become more accessible to a diverse, global audience. However, it is crucial for coaches to approach their work from a perspective that considers each client’s unique context and experiences, including their relationship
with technology. For example, researchers have observed differences between generations (Culp-Roche, et al. 2020) and country or origin (Huang, et al. 2019) in one’s comfort with and intentions to use technology. The global nature of digital coaching heightens the need for cultural competence and humility particularly by not making assumptions that all coachee’s will enter a digital coaching relationship with the same experience or comfort level. Failure to do so can result in missed growth opportunities and potential harm to the coaching relationship (Roche & Passmore, 2021).

One aspect of cultural competence is recognizing and examining implicit biases, which are unconscious beliefs that can influence judgments, decisions, and behaviors, even if they are not intended (Grant & O’Connor, 2019). Everyone holds implicit biases based on their own experiences and culture. When these biases are not addressed, they can negatively impact the coaching relationship. In the global digital coaching landscape, coaches are exposed to a wide range of cultural contexts, which can challenge the coaching process and relationship. For example, coaching practices that draw from the field of positive psychology should be used with caution in non-western populations, as much of the research and interventions are tested on Western populations which may not be representative of the global population as a whole (van Zyl & Rothmann, 2020; 2022). How mental health and well-being are discussed and viewed varies widely across cultures and a lot of that variability can be explained by where a culture falls on the individualism-collectivism scale. In collectivistic cultures, mental health and wellbeing are viewed as a function of societal factors, compared to individualistic cultures (Papadopoulos, et al. 2013). Simply put, what works in one culture may not be effective in another, leading to misunderstandings or harm. Coaches must be aware of these cultural differences and constantly reflect on how their biases may be influencing their work.

Global civics in the context of digital coaching emphasizes the importance of cross-cultural competence. Coaches must recognize and address their implicit biases, adapt their coaching approach to different cultural perspectives, and continually reflect on their own context and cultural identity. Cultural humility and curiosity are essential in engaging with diverse clients, and coaches must actively educate themselves and advocate for cultural inclusivity (Masters, et al., 2019; Yeager & Bauer-Wu, 2013). This shared responsibility extends to coaching platforms, which must provide training and support for cross-cultural competence while ensuring their products meet the needs of diverse populations. By collectively promoting cultural competence and global citizenship, the coaching industry can foster meaningful and inclusive coaching relationships that empower clients from all cultural backgrounds.
Cybersecurity

The third pillar of cyber citizenship, cybersecurity, involves recognizing threats to client privacy, protecting sensitive coaching information, and implementing preventative measures to avoid data breaches and maintain trust (IBM, 2021). Coaches can be the target of cybersecurity attacks performed by individuals or groups with harmful intent to steal data or disrupt computing systems (Singer et al., 2021). Understanding the environment of online threats is crucial for coaches as they are the frontline defense to client data. Practices such as using strong passwords, secure file drives, and keeping software up to date, are essential for supporting software health and data management.

Other important aspects of cybersecurity to consider are data security and data transparency. Technology has significantly expanded the amount of coaching data available, making it necessary for coaches to protect sensitive information in accordance with global regulatory standards. Coaches can prioritize client confidentiality by omitting personal identifying information in their notes and storing information securely. Using integrated platform capabilities for messaging and note-taking is also recommended as these platforms provide robust security measures. While these types of tools can aid in productivity, a human review of any AI-supported notetaking or message creation is recommended to ensure accuracy and minimize bias.

Data transparency involves creating a culture where policies are transparent, and open discussions and disagreements are encouraged (Gino, 2017). Transparency is crucial for building trust among all stakeholders. Privacy policies and agreements, internal data ethics boards, and ethical data management practices are a few examples of how coaches and technology providers can create a culture of shared responsibility around data transparency. For example, the use of assessments is common in coaching engagements and the provider, coach and coachee share responsibility for how that is ethically incorporated into the coaching engagement. The provider is responsible for ensuring the validity of the assessment and security of the data collected. The provider and coach share responsibility in training coaches on how to debrief the assessment, and the coach and coachee share responsibility for how that information is used to support the coachee’s journey. At its core, cybersecurity is a shared responsibility, between coach, client, and technology provider, that requires continuous learning to keep pace with technological advancements.

Developing Cyber Citizenship Skills

There are several ways coaches can develop their cyber citizenship. First, stay informed of the latest
technological advancements and digital tools, including advancements in AI and machine learning within coaching. Coaches should engage in regular training, education and reflective practice to learn new digital skills, cultivate a culturally competent coaching approach, and stay current with data privacy and security best practices. Coaches can also promote cyber citizenship within the coaching industry, as well as with their clients, by discussing the impact of technology on coaching processes. Lastly, advocating for the ethical use of AI, emphasizing the need for transparency, bias reduction and client-centered value in the creation of AI-powered tools will ensure that client-centricity is at the heart of coaching innovation.

References


