COSMOS
Navigate the Compliance Universe

ethikos Volume 34, Number 4. April 01, 2020
A technology and data practice code of conduct: No longer optional but necessary

By Decanda Faulk, RN, Esq., CIPP/US

Decanda Faulk (df@faulk-associates.com) is Healthcare Consultant at Comprehensive Care Management Solutions Inc. and Senior Commercial & Compliance Counsel at Law Office of Decanda Faulk P.C. in Newark, NJ, where she serves as outside consulting general counsel for two companies.

We live in a digital, mobile world where advanced technology allows businesses to acquire, access, alter, and create an abundance of data—the majority of which are analyzed through data science.[1] Data science allows data to be analyzed in a manner a company finds beneficial in many ways. Personal/sensitive data are a big part of the data these technology- and data-driven resources touch and data scientists, who are currently in an unregulated profession, analyze. With technology and data becoming increasingly more used in our daily lives, having a governing set of principles is prudent to ensure they pose no harm.

Public support for smarter technology and applications exists, but sadly, as innovation in technology- and data-driven products continues to advance, the public's trust is eroding. People want reassurance that they can trust these resources. Therefore, it is wise for big data and big tech to adopt an ethical approach to technology deployment and data practice to strengthen public trust and maintain support for advanced technologies.

To maximize the benefits of these technologies and practices, creating a targeted technology and data practice code of conduct, endorsed by the C-suite and corporate board, signals to employees and the public that a company takes its commitment to create and maintain the responsible development, deployment, and use of technology seriously. This message also shows employees that their employers want them to uphold said commitment. The government also has a bigger role to play in promoting the responsible development and deployment of technologies, specifically data-driven technologies and artificial intelligence (AI). Moreover, the government has a duty to the public to ensure that technology is not developed and deployed in harmful ways.

Compliance remains essential to an organization's viability. When compliance fails, the public often perceives every aspect of the organization, including its workforce, as untrustworthy or, worse, corrupt. The compliance failures of a few can taint an entire organization and harm many innocent people. Undoubtedly, ethical lapses of giant tech companies, data breaches, and discriminatory AI, which are becoming all too common with the rise of technological innovations, are unacceptable and avoidable compliance failures. Therefore, the technology industry and businesses in general need to reassure end users that they are acting in the users' best interests. A written technology and data practice code of conduct that governs behavior relating to product design developments and deployments, as well as data practice, is one way to reassure the public.

A technology and data practice code of conduct is prudent

With the prevalence of technology, every business is now considered a technology company, which places a responsibility on them to be better in how they deploy technology and handle data. Like universities, which are starting to adopt a more medicine-like moral compass approach to computer science,[2] other businesses and the United States government can take a more ethical approach to technology innovations and data practice.

A medicine-like moral compass approach refers to the important step in becoming a doctor that requires medical students to take the Hippocratic Oath, which includes a promise to "do no harm." Moreover, living in a privacy-, technology-, data-, and algorithm-driven world, where great functionality can coexist with risible data practices, a company's use and overall oversight of technology should no longer begin and end with its chief information (or technology) officer. Rather, the responsibility should now extend up through the C-suite and to the corporate board,[3] and they should be supported by salient government guidance.

With the increasing importance of advancements in technology and data practice, more action is required. Like any advancements, it behooves society to ensure such progress does more good than harm. Consistent with other obligations to end users, employers likely want to promote an understanding to their employees—and earn the public's trust—of a commitment to develop and use technological data-driven tools and AI in an ethical, transparent, and accountable manner. A technology and data practice code of conduct can assist in this endeavor.

A technology and data practice code of conduct serves many purposes, the most significant being to signal a top-down approach to the ethical, transparent, and accountable development and deployment of engineered technology products and data practices. Basically, having such a code in place sets the moral compass for developing technology and data practice. If more companies (especially tech start-ups) consider a technology and data practice code of conduct approach, it can reassure the public that technology does not have to come with harmful consequences, and such code can serve as a guide to employees' decision-making. Incorporating privacy by design as supported by the International Association of Privacy Professionals and some tech companies is another promising initiative. However, an important first step and demonstrative commitment to effective compliance and ethics is a well-written and targeted code of conduct.

App designers, app developers, and employees deserve guidance in their decision-making to innovate (or procure) in a more thoughtful, transparent, and accountable fashion, with a top-down commitment to creating (or acquiring) technology in accordance with a company's values and principles. An effective technology and data practice code of conduct can represent a pathway to a safe and trusted environment where technology can continue to flourish in a thoughtful, accountable, ethical, and transparent manner.

Over the years, many of the most meaningful compliance-driven initiatives have been required to have buy-in from the board and C-suite to be implemented, and they have been necessary to mitigate against harmful conduct. A technology and data practice code of conduct can guide employees in following a uniform company vision and mission to build trustworthy engineered products; deploy technology, including platforms, applications, and so on, responsibly; and handle personal and sensitive data ethically and accountably. Moreover, it places a greater emphasis on being proactive to mitigate discriminatory AI practices.

Data-driven technologies: First, do no harm; Second, be ethical

The pervasiveness of technology in our daily lives renders timely and paramount the maxim to be ethical in how technology is developed and used. Transparency is key to being ethical, and it should be part of the fabric of all technology companies and in the lexicon of every engineer and data scientist.

In practice, businesses must establish ethical guidelines for those developing technologies so they can work within those guidelines throughout a product's development, life cycle, and deployment. The frequent ethical lapses associated with how companies develop, deploy, and use data-consuming technologies—lapses that dominate media headlines—overwhelmingly support a technology and data practice code of conduct and drive home C-suite– and corporate board–level support for ethical conduct, transparency, privacy by design, and accountability in innovation when developing and deploying technology- and data-driven products and AI.

High-profile ethical lapses and high-risk in-home data harvesting technologies

It is often said in jest that Silicon Valley, unlike the medical profession with an ethic of "first, do no harm," has an ethos of "build first, ask forgiveness later." The belief today is that the Silicon Valley ethos is unsustainable. This ethos is partly responsible for the ethical lapses we have seen to date, examples of which include giant tech companies such as Google, Facebook, WhatsApp, and Instagram facing multibillion-dollar fines within hours of the General Data Protection Regulations taking effect on May 25, 2018. Privacy advocate Max Schrems filed the complaints against Google, Facebook, Instagram, and Whatsapp through a nonprofit he founded called NOYB – European Center for Digital Rights (from "none of your business").[4] Schrems argued that these tech companies "were acting illegally by forcing users to accept intrusive terms of service or lose access."[5] Such a "take-it-or-leave approach," Schrems said, "violates people's right under the General Data Protection Regulations (GDPR) to choose freely whether to allow companies to use their data,"[6] which, noyb.eu argued, is "'forced consent.'"[7] However, recent reports are encouraging; for example, Mozilla reports show that last year, only about a half of products in Mozilla's "privacy not included" buyer's guide met Mozilla's minimum-security standards. In 2019, about 75% of the products met Mozilla's minimum-security standards.[8] This indicates that companies are starting to take consumer privacy and security much more seriously.

In 2018, Facebook estimated that data from 87 million users were shared with Cambridge Analytica through a psychological survey application that collected users' personal data without their knowledge.[9] In July 2019, Facebook agreed to pay $5 billion to the United States Federal Trade Commission (FTC)—the largest privacy fine in the FTC's history—to resolve the Cambridge Analytica data scandal;[10] and in December 2019, Brazil imposed a $1.65 million fine on Facebook and its local unit for their role in said scandal.[11] Though Facebook has reported making changes to its platform and restricted the information accessible to app developers, more remains to be done.

Further, findings from a New York Times investigation into how smartphone-resident apps collect location data exposed "why it's important for the industry to admit that the ethics of individuals who code and commercialize technology is as important as the technology's code itself."[12] Additionally, homes have become a major frontier for data harvesting by big tech companies. Our personal data are being scooped up by smart speakers, app-activated thermostats, and other internet-connected devices. The data being collected through these devices may prove useful and fairly valuable to product designers, advertisers, governments, and law enforcement.[13] For example, Amazon's Echo, animated by the voice assistant Alexa, and Google's Home, with its Assistant, keep track of the questions people ask and store recordings of them. Manufacturers can develop a catalog of information about how people use smart home appliances and devices that communicate with a smartphone or a central hub (like Echo or Home) and take instructions by voice commands, remote controls, or a touchscreen. Such devices include ceiling fans made by Hunter Fan; thermostats made by Ecobee, Emerson, and Nest; Kwikset- and Schlage-branded door locks; and self-steering vacuums from iRobot. However, the ethical lapses we are experiencing today, together with data harvesting from in-home technologies, scream for technology and data practice to be governed by a code of conduct directed at technology- and data-driven resources and AI.

It is untenable for makers of smart technology devices to continue to place the onus solely on end users to trudge through voluminous privacy policies and terms of use so we can learn how the makers will use our information and how we can control such use. Potentially, a technology and data practice code of conduct, driven from the top down, can provide greater assurance of commitment and accountability concerning internet-, technology-, and data-driven products while offering helpful guidance to app designers, app developers, and employees on making informed and prudent decisions based on sound principles.

Privacy and technology

Privacy concerns are also on the rise as personal information is collected, processed, and transferred in new ways that challenge existing legal and social norms. According to a recent PricewaterhouseCoopers survey, 25% of consumers believe that businesses handle their sensitive personal data responsibly, while a mere 12% of consumers in 2019 trusted businesses more than they did in 2018.[14] The 2019 Ping Identity survey revealed that 81% of people "would stop engaging with a brand online following a data breach."[15] The percentage is up slightly from 78% in 2018, including 25% who would stop interacting with the brand in any capacity.[16] In 2018, cyberattacks exposed 2.8 billion consumer data records, costing more than $654 billion to US organizations.[17] With 60% of consumers reporting that they do not feel comfortable when businesses share their data,[18] it is incumbent upon information technology (IT) to know and understand when information is personal and/or sensitive and when it describes a person.

Today, IT professionals are expected to be knowledgeable about how privacy plays into their practices and the daily practices of others around them and with whom they should coordinate to improve privacy throughout information systems. Therefore, to reduce societal risks and threats to an organization's IT infrastructure, IT staff must combine a technical understanding of the available privacy-enabling and privacy-threatening technology with strategies for managing data through IT governance.

Then and now

Technology- and data-driven innovations now must contend with values produced for better usability, security, and privacy. Long gone are the days when IT was driven by value derived primarily from improved performance, better reliability, and stronger integrity—which remain important.

Big tech companies are best suited to take the lead on building trustworthy technology- and data-driven resources and nondiscriminatory AI, which includes improving privacy. Though it is established and common practice for developers and researchers to test usability, potential flaws, and security prior to a product going to market, until recently it was not established or common for technology developers to test for fairness, potential biases, and ethical implementation, or to take a privacy-by-design approach before a product hits the market or deploys into the enterprise.[19] However, today it is obligatory for companies building technologies and supporting applications to fundamentally incorporate principles of ethics, accountability, privacy, and transparency into their engineering.

Building trust

When Facebook, Google, YouTube, and Twitter are not careful and break the trust of their users, it has a ripple effect and results in consumers losing trust in advanced technology and the companies that leverage it. A technology and data practice code of conduct that frowns upon violating consumers' privacy rights and spreading lies (disinformation) and misinformation can certainly coexist with advanced technology.

According to Mitchell Baker, chairwoman of Mozilla Corporation, when the public expresses fear and anger over concerns of "misinformation making money for [big tech and big data] companies…hatred infecting the internet…and algorithms discriminating against the most vulnerable,"[20] leaders should ask themselves one question, "How can they make the internet, technology- and data-driven products, and AI not only better but also trustworthy?" She went on to say that with the work necessary to address the problems with the internet, protect our privacy, build trustworthy AI, and plug the holes allowing so much hate and misinformation to seep through the internet into our daily lives, perhaps the simple gesture of introducing a technology and data

practice code of conduct (with teeth) can go a long way in building end users' confidence and trust in new technologies and data practice.

To regain (or, in some instances, gain) public trust and do justice to maintaining effective and comprehensive compliance with the internet of things and technology, including AI and data practice, a technology and data practice code of conduct is prudent.

Compliance and technology tomorrow

It is no longer enough to have a broad-based corporate code of conduct that may reference IT and privacy or an IT policy on operating and safeguarding IT assets, including networks, computers, telephones, access controls, information, and databases, to mitigate risk and avoid reputational harm. Nor can the buck stop with the chief information security or technology officer to ensure technology is acquired and deployed in line with transparency and accountability.

A top-down technology and data practice code of conduct signals, at the highest levels of an organization (C-suite and board level), a commitment to ethical and responsible conduct in its business operations. Shareholders and investors share a similar responsibility to ensure companies are operating at a foundational level to avoid conduct harmful to both the company and the public it serves.

Once a technology and data practice code of conduct is in place, education and reinforcement must follow. Historically, a compliance program incorporates implementation, developing policies and procedures, conducting risk assessments, educating employees, and reinforcement. Today, compliance is widespread in most companies, so adding a component targeted at technology, including AI and data practice (as is already done with privacy), is not as cumbersome or costly as implementing an overall compliance program. It will, however, require a degree of time commitment in the initial rollout. Most companies already have many of the essential elements to create the technology and data practice code of conduct in place and effectively roll it out.

It is advisable to tailor your technology and data practice code of conduct to your specific company needs and avoid the cookie-cutter approach. Again, most companies already have the key aspects needed to implement a proper technology and data practice code of conduct in place. They simply need to assemble the diverse components into a suitable format and then educate employees on its use. Reinforcement should occur annually and as needed.

Develop and implement a technology and data practice code of conduct

First, take an inventory of your business. The type of business you are in and how you develop or acquire, deploy, and use technology will determine what a technology and data practice code of conduct should look like for your business. What is it you want to communicate to your product designers, product developers, technologists, employees, customers, and consumers about your business?

The Association for Computing Machinery (ACM), a worldwide professional association for the computing industry, starts its code of ethics with the understanding that public good is the primary consideration in ethical decision-making. The ACM offers five important recommendations that serve as a starting point for companies and boards of directors (trustees) concerned with keeping those in their organizations on the path of practicing good computing ethics. The first step is to ensure you have a specific computing/technology code of ethics, in addition to the overall code of conduct, at your organization. This article intentionally omits discussion of the other four steps, but readers may go to http://bit.ly/3aKdYyI to read the ACM's updated code of ethics.

The ACM believes that the power of computing and technology is so great that it requires its own set of guardrails

to ensure the impacts of both its proper and improper use are well understood. An effective technology and data practice code of conduct should embrace this important attribute.

The SysAdmin, Audit, Network, Security (SANS) Institute has an IT code of ethics for security professionals, and Information Systems Audit and Control Association (ISACA) has a code of professional ethics, which are resources the C-suite and boards of directors/trustees may find useful in supporting a compliance initiative to develop and implement an effective technology and data practice code of conduct.

ACM, ISACA, SANS, and similar organizations cannot facilitate or achieve the greatest technological good if C-suites and corporate directors are not working in tandem to promote a culture of ethical, transparent, and accountable technology and data practice in their companies. A technology and data practice code of conduct indicates a commitment to standards and principles that support these attributes.

A technology and data practice code of conduct can follow common code standards

A code of conduct sets forth a company's pledge to ensure that its business conduct, operations, leadership, and workforce are governed by standards and principles that indicate it will function in an ethical manner and within the company's identity (e.g., its mission and values). When well written, a code of conduct clarifies an organization's mission, values, and principles, linking them to standards of professional conduct. Additionally, a code of conduct serves as a central guide and reference for employees in supporting their day-to-day decision-making, especially when the code focuses on specific steps employees should take when faced with difficult decisions.

Because most employees want to follow the rules and do the right thing but may not know or understand how to comply with the rules, a good technology and data practice code of conduct can help them do their jobs better. For example, when considering ethics in technology and data harvesting, it is recommended to include, among others, the following:

- A principle of fair, transparent, and accountable use of technology and data guidelines for procurement of technology by procurers, enabling procurement decisions to be made in an informed manner;
- A review of contracting and procurement arrangements that balance adoption of innovation with maintaining integrity and security of data; and
- A guide to the deployment and use of new technology that complies with ethical conduct.

By no means should the goal of a technology and data practice code of conduct be to seek to stifle access to and use of innovation. In contrast, such a code should promote and support responsible technology developments and data practices (especially when such innovation has the ability to improve healthcare diagnoses, treatment, care coordination, management, experience, and overall outcomes while enhancing efficiencies and economies of scale in healthcare delivery systems). Therefore, before embarking on developing and implementing a technology and data practice code of conduct, companies should first identify the technology data-driven innovations it pursues, including the tools it uses, and evaluate them based on risk levels.

Risk level evaluations do not mean just risk posed to the company as it relates to reputational harm. It also includes risks to end users and other third parties who could sustain irreparable personal and/or professional harm if technology developers, implementers, and procurers of technology- and data-driven resources fail to develop and deploy or acquire and use platforms and applications in a responsible and ethical manner.

Big tech and big data companies, as well as procurers of technology- and data-driven resources, can also take a

cue from the United Kingdom's National Health Service's (Department of Health & Social Care) guidance code of conduct for data-driven health and care technology,[21] which was updated July 18, 2019. Its code of conduct is supportive of data-driven innovation, but like the European Union's General Data Protection Regulation, the United Kingdom seeks to balance the use of technology and data with transparent, accountable, and ethical behavior.

Conclusion

Big tech companies like Google, Apple, and Microsoft are taking proactive measures and rethinking their virtual assistant programs after a steady drip of news reports spurred a backlash. Google suspended human transcriptions of Assistant audio, later resuming them;[22] Apple now lets users delete their Siri history and opt out of sharing recordings,[23] and it hired many former contractors to increase its control over human listening; and Amazon started letting Alexa users opt out of manual reviews of their recordings.[24]

These are all promising signs that things are changing favorably and heading in the right direction. Again, most of what could be captured in a technology and data practice code of conduct likely exists in a company's reservoir of policies and procedures and simply needs to be consolidated into a workable document and rolled out with training and education.

1 Ioannis Zempekakis, "Regulation and Ethics in Data Science and Machine Learning," Towards Data Science, September 12, 2019, http://bit.ly/2TT4D0X.
2 Natasha Singer, "Tech's Ethical 'Dark Side': Harvard, Stanford and Others Want to Address It," TheNew York Times, February 12, 2018, https://nyti.ms/2W5eovx.
3 Marty J. Wolf, "Computing Ethics are a Board Concern," Directors & Boards, October 30, 2019, http://bit.ly/2vbz2zd.
4 Derek Scally, "Max Schrems files first cases under GDPR against Facebook and Google,"The Irish Times, May 25, 2018, http://bit.ly/33m133B.
5 Douglas Busvine and Lucy Fielder, "GDPR Day 1: Privacy Activist Files Complaints Against Tech Giants Over 'Forced Consent,'" Insurance Journal, May 25, 2018, http://bit.ly/2TYDhGG.
6 Douglas Busvine, "GDPR Day 1."
7 Michael Grothaus, "Google and Facebook are already accused of breaking GDPR laws," FastCompany, May 25, 2018, http://bit.ly/3aRC9vb.
8 "Mozilla's Latest 'Privacy Not Included' Buyer's Guide," National Public Radio, December 2, 2019, https://n.pr/2IH6FvL.
9 Issie Lapowsky, "Facebook Exposed 87 Million Users to Cambridge Analytica," *Wired*, April 4, 2018, http://bit.ly/38ZD6QR.
10 Federal Trade Commission, "FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook," news release, July 24, 2019, http://bit.ly/2lXjt99.
11 Ricardo Brito, "Brazil fines Facebook $1.6 million for improper sharing of user data," *Reuters*, December 30, 2019, https://reut.rs/2UhyX5x.
12 Klaus-Michael Vogelberg, "Industries must adopt ethics along with technology," TechCrunch, December 20, 2018, https://tcrn.ch/337gE6Y.
13 Matt Day, "You're Home Alone with Alexa. Are Your Secrets Safe?" Bloomberg Businessweek, July 18, 2019, https://bloom.bg/39Dw8Ck.
14 PricewaterhouseCoopers, Consumer Intelligence Series: Protect.me, 2017, https://pwc.to/2VX24NY.
15 Ping Identity, "81% of Consumers Would Stop Engaging with a Brand Online After a Data Breach, Reports Ping Identity," news release, October 22, 2019, http://bit.ly/2Q5Wq8x.

16 Ping Identity, 2019 Consumer Survey: Trust and Accountability in the Era of Data Misuse, last accessed March 12, 2020, http://bit.ly/2IJ4N5U.
17 Conor Cawley, "Cyber Attacks Cost US Businesses $654 Billion in 2018," tech.no, June 12, 2019, http://bit.ly/38yz6Xm.
18 Help Net Security, "Most Consumers Don't Trust Companies to Keep Personal Information Secure," October 10, 2018, http://bit.ly/3aKW13e.
19 Klaus Michael Vogelberg, "Industries must adopt ethics along with technology," N-Tic Infotech, December 20, 2018, http://bit.ly/2xsX8pR.
20 Mitchell Baker to Mozilla mailing list, December 31, 2019, https://mozilla.org.
21 U.K. Dep't of Health and Social Services, Code of conduct for data-driven health and care technology, updated July 18, 2019, http://bit.ly/3aPFDyx.
22 The Associated Press, "Google will start transcribing audio recordings again," *ABC News*, September 23, 2019, https://abcn.ws/2Qr6hWG.
23 Alex Hern, "Apple lets users opt out of having Siri conversations graded," *The Guardian*, October 30, 2019, http://bit.ly/3b9Cb1T.
24 Ben Fox Rubin, "Amazon now lets you stop human review of your Alexa recordings," CNET, August 2, 2019, https://cnet.co/339M5xp.