Why You Should Care About Data Ethics

Ethical decision-making

Chaplain (Maj.) Glen Thompson,
Capt. Derrick Kozlowski
U.S. Army Signal School

In an era dominated by rapid technological advancement, the Army increasingly relies on data collection, analysis, and usage to achieve its mission objectives. Data-driven technologies enhance decision-making, situational awareness, and operational efficiency. However, the ethical implications of collecting, analyzing, and applying data must be critically considered. As the Army continues to collect more and more data and aggregate it together to tell data-informed stories to commanders, we must ensure we are protecting and sharing this information in an ethical manner.

As Soldiers and civilians in the United States Army, we adhere to Army Ethics. As defined in Army Doctrine Publication (ADP) 6-22, Army Ethics is "the set of enduring moral principles, values, beliefs, and laws that guide the Army profession and create the culture of trust essential to Army professionals in the conduct of missions, performance of duty, and all aspects of life."

The Army Ethic can be broken down into three parts. The first part represents the "what." This is comprised of a set of moral principles, values, beliefs, and laws that are constant across all members and organizations. It is divided into two categories: legal foundations that set the minimum standards for ethical conduct, and moral foundations.

The second part is the "why." Why do we have ADP 6-22? The ADP 6-22 guides the Army profession and creates a culture of trust essential to Army professionals. In our profession, trust is critical in that it allows Soldiers to strive toward positive outcomes with faith in their leaders and subordinates. The third part we have is the "when." We are expected to follow these moral principles, values, beliefs, and laws; not just on duty, but in all aspects of life.

The Army is in the business of training Soldiers, which implies that there is a standard to be trained to. The same is true in data ethics. According to the Federal Data Strategy, "Data ethics are the norms of behavior that promote appropriate judgments and accountability when collecting, managing, or using data, with the goals of protecting civil liberties, minimizing risks to individuals and society, and maximizing the public good." It is essential to follow the Privacy Act of 1974, the Federal Information Security Modernization Act, the General Data Protection Regulations, U.S. Constitution, and the Ethical Codes in Military Doctrine when managing and protecting data to ensure legal compliance and ethical conduct in military operations. Consistency, risk mitigation, increased transparency, consideration of wider perspectives, and most importantly, improved public trust are the benefits of data ethics.

The Federal Data Strategy Data Ethics Framework (2020) established seven tenets to help federal employees make ethical decisions and promote accountability when working with data. These tenants are:

1. Uphold applicable statues, regulations, professional practices, and ethical standards.
2. Respect the public, individuals, and communities.
3. Respect privacy and confidentiality.
4. Act with honesty, integrity, and humility.
5. Hold oneself and others accountable.
6. Promote transparency.
7. Stay informed of developments in data management and data science.

One of the key ethical concerns in Army data usage is the respect for individual privacy. The Army must carefully balance operational needs with the right to privacy for both Soldiers and civilians.

Data collection, particularly through surveillance technologies such as drones, facial recognition systems, and biometrics, poses significant ethical challenges. It is essential that the Army implements strict guidelines on what data can be collected, and how it is stored and accessed to ensure that privacy is not unnecessarily infringed upon. Transparency in data practices builds trust within the Army and with the public. Soldiers should be aware of how their data is being used, and there should be clear accountability mechanisms for data breaches or unethical use of information.

Ensuring that we are not adding bias into our data-informed decision-making process is going to be one of the most important things we do as we continue to collect and process more data. As new technologies emerge, such as quantum computing, autonomous systems, and more advanced artificial intelligence (AI), the Army must continuously adapt its ethical guidelines to address new risks. This requires ongoing collaboration between military leaders, ethicists, technologists, and legal experts.

The use of AI and machine learning in military decision-making can introduces concerns about bias if these models are not properly trained. This can be particularly concerning in situations where data-driven technologies are used to make decisions about targeting, surveillance, or risk assessment. Ensuring that data is representative and algorithms are tested for bias is critical to ensure we are empowering our leaders to make agile decisions with the best data available.

Chief Data Officer, Capt. Derrick Kozlowski, U.S. Army Signal School, teaches the first-ever Data for Leaders Course. A group of 16 leaders graduated from the course on June 28. (Photo by Laura Levering, U.S. Army Signal School)

In conclusion, data ethics in the Army is only going to get more and more complex as emerging technologies continue to be utilized. Data ethics has become another pillar that must be applied within professionalism and leadership. The responsible use of data is critical to maintaining trust, both within the Army and with the public it serves. Upholding ethical standards in data collection, analysis, and usage ensures that the Army can leverage the power of data while staying true to the Federal Data Strategy Data Ethics Framework and its seven tenants. As technologists, we must ensure that we are staying up to date with polices and emerging technology that can be used to add ethical concerns to our formations.

UPCOMING DATA OPPORTUNITIES …

Data for Leaders Course: Topics include data literacy, data governance, cloud fundamentals, understanding the power of data, telling a story with data, and zero trust.
***Course dates:* March 3-7, 2025; June 9-13, 2025; and Aug. 11-15, 2025.**

Data Engineer Foundations Course: Topics include an introduction to data modeling, database design, ETL (extract, transform, load) processes, API (application programming interface) processes, data warehousing fundamentals, practical application of cloud platforms, and more.
***Course dates:* Jan. 27—Feb. 7, 2025; April 28—May 9, 2025; and July 14—25, 2025.**

***For information* about either of these courses or to secure your spot on the Order of Merit List, contact Capt. Derrick Kozlowski at: derrick.r.kozlowski.mil@army.mil, or Chief Warrant Officer 5 Chris Westbrook at: chris.r.westbrook.mil@army.mil**