Algorithms Ethics Paper

By Andrew Burbage

In our modern era of technology with its ease of access and ever expanding abilities there is a world of opportunity for people to do great things, but also for bad actors to do harm. The issues of privacy for those who need it for protection while also allowing for those who do evil to be identified and be held accountable is paramount but also not a simple task. On one hand privacy is extremely important and often regarded as a human right in the digital age yet at the same time those who use the same privacy and anonymity to commit various crimes and heinous acts make it imperative that privacy cannot be absolute. How can a balance be struck between privacy and accountability that allows for safety for the everyday person while also not being a safe harbor for crime and misuse?

To answer this question it will be helpful to build a solid background in the history and development of the ideas of privacy and the freedom it supports. The focus here will be on American history to allow for brevity and for relevance to the application to come that is intended for a largely American audience. From the founding of the United States there has been a large emphasis on personal freedom, this is clearly evident in the 1st, 4th, and 5th amendments in the Bill of Rights. These amendments guarantee citizens in the United States the right to freedom of speech, religion, assembly, and petition under the first amendment (this extends to the press as well), the protection from unreasonable searches under the fourth amendment, and a right to due process and a fair trial under the fifth amendment. These founding rights lay out a clear pattern of both privacy and the freedom that it makes possible. Citizens are free to express their opinions even if they are dissenting to the ruling party or the government itself. This

expression is protected from persecution by amendments like the 4th and 5th that allow for a level of privacy to express oneself freely. Jumping forward in time to the advent of technology and the more modern age the debate of privacy begins to grow as technology and society advances. Around 1960 as this debate was beginning to heat up some legal torts were asserted by a Mr. Prosser from cases collected by Warren and Brandeis. He asserted that privacy boiled down to 4 key points: “Prosser concluded that the cases recognized four distinct torts: (1) intrusion upon seclusion; (2) public disclosure of private facts; (3) false light or “publicity”; and (4) appropriation.” [1] Essentially he asserted that privacy boils down to the fact that people should be allowed to have privacy and that any exposure of personal details should be done with consent meaning that one's privacy is to be treated not only as a right but as a legally protected entity that requires consent for access and exposure.

Around the same time as these torts were made there were those in government abusing their power to violate the privacy of individuals based on suspicion and rumor. Two persons infamous for such abuses were Hoover, the director of the FBI at the time, and Senator McCarthy. The two worked together bugging meetings, tapping phones, and spying on citizens and political dissidents with no regard for privacy and with almost no oversight.[2] As time, technology, and society continued to progress so did reform and laws protecting citizens from such overreach. A key law that brought about this reform was the Privacy act of 1974 that ensured that at the Federal level that there was regulation and oversight when it came to monitoring and invasions of privacy made by the Federal government.[3] However, in the wake of the terrorist attacks on September 11th, 2001 the laws that protected citizens privacy were

---

[1] Daniel J. Solove, "A Brief History of Information Privacy Law" (George Washington University Law School, 2006), 14, https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications.
[2] Solove, "A Brief History of Information Privacy Law," 20-22.
[3] Solove, "A Brief History of Information Privacy Law," 26.

brought into question in the name of national security leading to the advent of the Patriot act in 2001 and its supplementary acts that came later. These acts asserted that the privacy of individuals was not untouchable when it came to the need to protect the whole of the country.[4] This brings the debate of privacy to the current question, how can individuals be afforded the freedom that comes with privacy and anonymity while also allowing for bad actors to be detected and identified so as to also protect others from crime and abuse that can come with privacy and anonymity?

This question by nature is ethical and requires a response that relies on guiding principles especially when it comes to the computer engineers , computer scientists, and cyber security specialists who are on the frontlines of this issue. Luckily, for such professions there are sets of guiding principles that allow for clear ways forward with problems like these. In the case of the computer science and technology fields the IEEE and ACM have published guidelines to help make morally and ethically correct determinations when they face this problem in their work. The IEEE's code of ethics asserts under section one that a key role of the professional is:

> "to hold paramount the safety, health, and welfare of the public, to strive to comply with ethical design and sustainable development practices, to protect the privacy of others, and to disclose promptly factors that might endanger the public or the environment;"[5]

Clearly the balance must be struck, individuals should be guaranteed privacy but also held accountable for what they do so as to protect them and others. However, this is just a high level view that does not really delve into the particular methods to meet this balance. The ACM code of Ethics expounds on this stating:

---

[4] Solove, "A Brief History of Information Privacy Law," 41-42.
[5] Institute of Electrical and Electronics Engineers, "IEEE Code of Ethics," accessed December 1, 2025, https://www.ieee.org/about/corporate/governance/p7-8.

> "Computing professionals should only use personal information for legitimate ends and without violating the rights of individuals and groups. This requires taking precautions to prevent re-identification of anonymized data or unauthorized data collection, ensuring the accuracy of data, understanding the provenance of the data, and protecting it from unauthorized access and accidental disclosure. Computing professionals should establish transparent policies and procedures that allow individuals to understand what data is being collected and how it is being used, to give informed consent for automatic data collection, and to review, obtain, correct inaccuracies in, and delete their personal data."[6]

Above are clear ways to allow for both a respect of privacy as well as a level of accountability. Notice that privacy is viewed as not only needing protection from the entity collecting data itself but also from outsiders who may attempt to retrieve that data. Furthermore, the data collected while private needs only to be enough to identify the individual and such information should be made available to that individual if they were to request it.

Ultimately, the question of how to protect the privacy of the individual while also allowing for accountability comes down to intentional actions when it comes to data collection and protection. Since the founding of the country there has been a struggle to find balance between privacy and security, between avoiding government overreach and unchecked privacy that leaves criminals and bad actors untraceable. The answer is to collect only what is necessary about users to identify them and to protect that data from others while also making it available to the individual for the entity to be held accountable as well as to those tasked with justice and

[6]Association for Computing Machinery, "ACM Code of Ethics and Professional Conduct," accessed December 1, 2025, https://www.acm.org/code-of-ethics.

defense, within reason, to hold those same individuals accountable. In real life this looks like audit logs to hold individuals accountable if they need to be identified, encryption to protect the private data of individuals, and data minimization policies to protect individuals from collecting entities.

Bibliography

Association for Computing Machinery. "ACM Code of Ethics and Professional Conduct." Accessed December 1, 2025. https://www.acm.org/code-of-ethics.

Institute of Electrical and Electronics Engineers. "IEEE Code of Ethics." Accessed December 1, 2025. https://www.ieee.org/about/corporate/governance/p7-8.

Solove, Daniel J. "A Brief History of Information Privacy Law." George Washington University Law School, 2006. https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications.