Association for
Computing Machinery

Advancing Computing as a Science & Profession

The Code

ACM Code of Ethics and Professional Conduct

Affirming our obligation to use our skills to benefit society

- General Ethical Principles
- Professional Responsibilities
- Professional Leadership Principles
- Compliance with the Code
- Case Studies
- Using the Code

ACM Code of Ethics and Professional Conduct

Letter from the President

Computing professionals have a profound impact on both public and private life. Part of ACM's role is to guide computing's impact in order to better the world. As a professional organization, ACM identifies who we are by what we value. The ACM Code of Ethics and Professional Conduct clearly states what is essential to professional life. The Code is a contract among ourselves as professionals, as well as a public statement of our understanding of the responsibilities the profession has to the larger society that it serves.

With computing technology so interwoven into the fabric of daily life, the work that computing professionals do is essential to ensuring that technology is used to improve the lives of all people. Computing professionals also are the first line of defense against the misuse of technology. Our collective understanding of computing systems puts us in a position to protect sensitive information and ensure that systems integrate in ways that are appropriate, safe, and reliable. Society needs to be assured that we are committed to ethical conduct as the foundation of our work. That need has become the personal responsibility of every professional in our industry.

When the ACM Code of Ethics was last updated in 1992, many of us saw computing work as purely technical. The World Wide Web was in its infancy and people were just beginning to understand the value of being able to aggregate and distribute information widely. Today, we find ourselves in situations where our work can affect the lives and livelihoods of people in ways that may not be intended, or even be predictable. This brings a host of complex ethical considerations into play.

The ACM Code of Ethics is designed to help guide the aspirations of all computing professionals in doing our work. It acknowledges that ethical decisions are not always easily arrived at, and exhorts us, as professionals, to develop not only our technical abilities but our skills in ethical analysis as well.

This booklet, with both the Code and examples of applying the Code, is just the starting point, though. ACM's Committee on Professional Ethics has created a repository for case studies showing how ethical thinking and the Code can be applied in a variety of real-world situations. The "Ask an Ethicist" blog invites people to submit scenarios or quandaries as they arise in practice. Efforts are underway to develop ways to incorporate ethical considerations throughout the computer science curriculum, at levels from primary through graduate school.

The ACM Code of Ethics and Professional Conduct begins with the statement, "Computing professionals' actions change the world." The participation of professionals from around the world in developing the ACM Code of Ethics demonstrates that the global computing community understands the impact our work has—and that we take seriously our obligation to the public good.

Cherri M. Pancake
ACM President

A Guide for Positive Action

Computing advances in the 21st century have intensified the depth and breadth of the field's impact on society. Computing now shapes and defines the structures of society, interacting with and producing new socio-technical structures. Computing is no longer merely a support structure for doing complex calculations. It influences the essence of our being, running insulin pumps and pacemakers, managing our friendships, and identifying who should be punished, promoted, and hired. The roles and responsibilities of computing professionals have thus also undergone profound transformations that are reflected in this update to the ACM Code of Ethics and Professional Conduct.

As a rapidly changing and complex field, computing requires a high level of technical skill. High-speed and high-capacity communications facilitate local decisions that have a global impact on all aspects of society, including individual citizens. Fortunately, most of our ethical decisions are almost automatic, and consist of applying ethical decision skills we learned in our formative years. Yet, due to computing's role in changing society and the nature of human interaction, we need to revisit those ethical standards to clarify how they apply to the decisions of computing professionals. The complexity of computing systems often leads to a narrow focus on technical requirements, potentially missing the needs of some stakeholders. A book reading app may meet the requirement of enlarging font size for the visually challenged, but fail to consider the user when the instructions to achieve this effect are in a tiny font. In this example the system is an ethical failure, although it meets the technical requirement.

The change in the nature of computing's impact means that every decision requires us to identify a broader range of stakeholders and consider how to satisfy our obligations to them. A primary function of the Code is to help computing professionals identify potential impacts and promote positive outcomes in their systems. It also informs the public about important professional responsibilities and educates practitioners on the standards that society expects them to meet. Further, it makes clear to aspiring computing professionals what their peers strive for and expect of each other. As a reflection of the collective conscience of the computing profession, it encourages professionals to undertake positive actions and to resist pressure to act unethically.

The Code, like many modern codes, provides ethical principles that are to be taken as a whole. Considering a single principle often leads to incomplete responses to complex questions. Used holistically, the Code is an inspiring guide. But keep in mind that using it this way requires professionals to make ethical judgments about how various possible actions are consistent with (or conflict with) the Code's principles and, thus, expands the meaning of professionalism beyond mere technical competence.

Before you read the Code, call to mind a recent project. Use the Code to help you identify facts, stakeholders, and obligations that you might not have considered previously. Use the principles as springboards to different alternatives for decisions you made. Then ask yourself how that project could have made a more positive impact.

Don Gotterbarn and Marty J. Wolf
Co-Chairs, ACM Committee on Professional Ethics

The Code

ACM Code of Ethics and Professional Conduct

Preamble

Computing professionals' actions change the world. To act responsibly, they should reflect upon the wider impacts of their work, consistently supporting the public good. The ACM Code of Ethics and Professional Conduct ("the Code") expresses the conscience of the profession.

The Code is designed to inspire and guide the ethical conduct of all computing professionals, including current and aspiring practitioners, instructors, students, influencers, and anyone who uses computing technology in an impactful way. Additionally, the Code serves as a basis for remediation when violations occur. The Code includes principles formulated as statements of responsibility, based on the understanding that the public good is always the primary consideration. Each principle is supplemented by guidelines, which provide explanations to assist computing professionals in understanding and applying the principle.

Section 1 outlines fundamental ethical principles that form the basis for the remainder of the Code. Section 2 addresses additional, more specific considerations of professional responsibility. Section 3 guides individuals who have a leadership role, whether in the workplace or in a volunteer professional capacity. Commitment to ethical conduct is required of every ACM member, and principles involving compliance with the Code are given in Section 4.

The Code as a whole is concerned with how fundamental ethical principles apply to a computing professional's conduct. The Code is not an algorithm for solving ethical problems; rather it serves as a basis for ethical decision-making. When thinking through a particular issue, a computing professional may find that multiple principles should be taken into account, and that different principles will have different relevance to the issue. Questions related to these kinds of issues can best be answered by thoughtful consideration of the fundamental ethical principles, understanding that the public good is the paramount consideration. The entire computing profession benefits when the ethical decision-making process is accountable to and transparent to all stakeholders. Open discussions about ethical issues promote this accountability and transparency.

1 General Ethical Principles

A computing professional should...

1.1 Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.

This principle, which concerns the quality of life of all people, affirms an obligation of computing professionals, both individually and collectively, to use their skills for the benefit of society, its members, and the environment surrounding them. This obligation includes promoting fundamental human rights and protecting each individual's right to autonomy. An essential aim of computing professionals is to minimize negative consequences of computing, including threats to health, safety, personal security, and privacy. When the interests of multiple groups conflict, the needs of those less advantaged should be given increased attention and priority.

Computing professionals should consider whether the results of their efforts will respect diversity, will be used in socially responsible ways, will meet social needs, and will be broadly accessible. They are encouraged to actively contribute to society by engaging in pro bono or volunteer work that benefits the public good.

All people are stakeholders in computing.

In addition to a safe social environment, human well-being requires a safe natural environment. Therefore, computing professionals should promote environmental sustainability both locally and globally.

1.2 Avoid harm.

In this document, "harm" means negative consequences, especially when those consequences are significant and unjust. Examples of harm include unjustified physical or mental injury, unjustified destruction or disclosure of information, and unjustified damage to property, reputation, and the environment. This list is not exhaustive.

Well-intended actions, including those that accomplish assigned duties, may lead to harm. When that harm is unintended, those responsible are obliged to undo or mitigate the harm as much as possible. Avoiding harm begins with careful consideration of potential impacts on all those affected by decisions. When harm is an intentional part of the system, those responsible are obligated to ensure that the harm is ethically justified. In either case, ensure that all harm is minimized.

To minimize the possibility of indirectly or unintentionally harming others, computing professionals should follow generally accepted best practices unless there is a compelling ethical reason to do otherwise. Additionally, the consequences of data aggregation and emergent properties of systems should be carefully analyzed. Those involved with pervasive or infrastructure systems should also consider Principle 3.7.

A computing professional has an additional obligation to report any signs of system risks that might result in harm. If leaders do not act to curtail or mitigate such risks, it may be necessary to "blow the whistle" to reduce potential harm. However, capricious or misguided reporting of risks can itself be harmful. Before reporting risks, a computing professional should carefully assess relevant aspects of the situation.

1.3 Be honest and trustworthy.

Honesty is an essential component of trustworthiness. A computing professional should be transparent and provide full disclosure of all pertinent system capabilities, limitations, and potential problems to the appropriate parties. Making deliberately false or misleading claims, fabricating or falsifying data, offering or accepting bribes, and other dishonest conduct are violations of the Code.

Computing professionals should be honest about their qualifications, and about any limitations in their competence to complete a task. Computing professionals should be forthright about any circumstances that might lead to either real or perceived conflicts of interest or otherwise tend to undermine the independence of their judgment. Furthermore, commitments should be honored.

Honesty is an essential component of trust.

Computing professionals should not misrepresent an organization's policies or procedures, and should not speak on behalf of an organization unless authorized to do so.

1.4 Be fair and take action not to discriminate.

The values of equality, tolerance, respect for others, and justice govern this principle. Fairness requires that even careful decision processes provide some avenue for redress of grievances.

Computing professionals should foster fair participation of all people, including those of underrepresented groups. Prejudicial discrimination on the basis of age, color, disability, ethnicity, family status, gender identity, labor union membership, military status, nationality, race, religion or belief, sex, sexual orientation, or any other inappropriate factor is an explicit violation of the Code. Harassment, including sexual harassment, bullying, and other abuses of power and authority, is a form of discrimination that, amongst other harms, limits fair access to the virtual and physical spaces where such harassment takes place.

The use of information and technology may cause new, or enhance existing, inequities. Technologies and practices should be as inclusive and accessible as possible and computing professionals should take action to avoid creating systems or technologies that disenfranchise or oppress people. Failure to design for inclusiveness and accessibility may constitute unfair discrimination.

1.5 Respect the work required to produce new ideas, inventions, creative works, and computing artifacts.

Developing new ideas, inventions, creative works, and computing artifacts creates value for society, and those who expend this effort should expect to gain value from their work. Computing professionals should therefore credit the creators of ideas, inventions, work, and artifacts, and respect copyrights, patents, trade secrets, license agreements, and other methods of protecting authors' works.

Both custom and the law recognize that some exceptions to a creator's control of a work are necessary for the public good. Computing professionals should not unduly oppose reasonable uses of their intellectual works. Efforts to help others by contributing time and energy to projects that help society illustrate a positive aspect of this principle. Such efforts include free and open source software and work put into the public domain. Computing professionals should not claim private ownership of work that they or others have shared as public resources.

1.6 Respect privacy.

The responsibility of respecting privacy applies to computing professionals in a particularly profound way. Technology enables the collection, monitoring, and exchange of personal information quickly, inexpensively, and often without the knowledge of the people affected. Therefore, a computing professional should become conversant in the various definitions and forms of privacy and should understand the rights and responsibilities associated with the collection and use of personal information.

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.

Only the minimum amount of personal information necessary should be collected in a system. The retention and disposal periods for that information should be clearly defined, enforced, and communicated to data subjects. Personal information gathered for a specific purpose should not be used for other purposes without the person's consent. Merged data collections can compromise privacy features present in the original collections. Therefore, computing professionals should take special care for privacy when merging data collections.

1.7 Honor confidentiality.

Computing professionals are often entrusted with confidential information such as trade secrets, client data, nonpublic business strategies, financial information, research data, pre-publication scholarly articles, and patent applications. Computing professionals should protect confidentiality except in cases where it is evidence of the violation of law, of organizational regulations, or of the Code.

In these cases, the nature or contents of that information should not be disclosed except to appropriate authorities. A computing professional should consider thoughtfully whether such disclosures are consistent with the Code.

2 | Professional Responsibilities

A computing professional should...

2.1 Strive to achieve high quality in both the processes and products of professional work.

Computing professionals should insist on and support high-quality work from themselves and from colleagues. The dignity of employers, employees, colleagues, clients, users, and anyone else affected either directly or indirectly by the work should be respected throughout the process. Computing professionals should respect the right of those involved to transparent communication about the project. Professionals should be cognizant of any serious negative consequences affecting any stakeholder that may result from poor quality work and should resist inducements to neglect this responsibility.

Make a positive impact.

2.2 Maintain high standards of professional competence, conduct, and ethical practice.

High-quality computing depends on individuals and teams who take personal and group responsibility for acquiring and maintaining professional competence. Professional competence starts with technical knowledge and with awareness of the social context in which their work may be deployed. Professional competence also requires skill in communication, in reflective analysis, and in recognizing and navigating ethical challenges. Upgrading skills should be an ongoing process and might include independent study, attending conferences or seminars, and other informal or formal education. Professional organizations and employers should encourage and facilitate these activities.

2.3 Know and respect existing rules pertaining to professional work.

"Rules" here include local, regional, national, and international laws and regulations, as well as any policies and procedures of the organizations to which the professional belongs. Computing professionals must abide by these rules unless there is a compelling ethical justification to do otherwise. Rules that are judged unethical should be challenged. A rule may be unethical when it has an inadequate moral basis or causes recognizable harm. A computing professional should consider challenging the rule through existing channels before violating the rule. A computing professional who decides to violate a rule because it is unethical, or for any other reason, must consider potential consequences and accept responsibility for that action.

2.4 Accept and provide appropriate professional review.

High-quality professional work in computing depends on professional review at all stages. Whenever appropriate, computing professionals should seek and utilize peer and stakeholder review. Computing professionals should also provide constructive, critical reviews of others' work.

2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.

Computing professionals are in a position of trust, and therefore have a special responsibility to provide objective, credible evaluations and testimony to employers, employees, clients, users, and the public. Computing professionals should strive to be perceptive, thorough, and objective when evaluating, recommending, and presenting system descriptions and alternatives. Extraordinary care should be taken to identify and mitigate potential risks in machine learning systems. A system for which future risks cannot be reliably predicted requires frequent reassessment of risk as the system evolves in use, or it should not be deployed. Any issues that might result in major risk must be reported to appropriate parties.

Computing is a service to society.

2.6 Perform work only in areas of competence.

A computing professional is responsible for evaluating potential work assignments. This includes evaluating the work's feasibility and advisability, and making a judgment about whether the work assignment is within the professional's areas of competence. If at any time before or during the work assignment the professional identifies a lack of a necessary expertise, they must disclose this to the employer or client. The client or employer may decide to pursue the assignment with the professional after additional time to acquire the necessary competencies, to pursue the assignment with someone else who has the required expertise, or to forgo the assignment. A computing professional's ethical judgment should be the final guide in deciding whether to work on the assignment.

2.7 Foster public awareness and understanding of computing, related technologies, and their consequences.

As appropriate to the context and one's abilities, computing professionals should share technical knowledge with the public, foster awareness of computing, and encourage understanding of computing. These communications with the public should be clear, respectful, and welcoming. Important issues include the impacts of computer systems, their limitations, their vulnerabilities, and the opportunities that they present. Additionally, a computing professional should respectfully address inaccurate or misleading information related to computing.

2.8 Access computing and communication resources only when authorized or when compelled by the public good.

Individuals and organizations have the right to restrict access to their systems and data so long as the restrictions are consistent with other principles in the Code. Consequently, computing professionals should not access another's computer system, software, or data without a reasonable belief that such an action would be authorized or a compelling belief that it is consistent with the public good. A system being publicly accessible is not sufficient grounds on its own to imply authorization. Under exceptional circumstances a computing professional may use unauthorized access to disrupt or inhibit the functioning of malicious systems; extraordinary precautions must be taken in these instances to avoid harm to others.

2.9 Design and implement systems that are robustly and usably secure.

Breaches of computer security cause harm. Robust security should be a primary consideration when designing and implementing systems. Computing professionals should perform due diligence to ensure the system functions as intended, and take appropriate action to secure resources against accidental and intentional misuse, modification, and denial of service. As threats can arise and change after a system is deployed, computing professionals should integrate mitigation techniques and policies, such as monitoring, patching, and vulnerability reporting. Computing professionals should also take steps to ensure parties affected by data breaches are notified in a timely and clear manner, providing appropriate guidance and remediation.

Consistently support the public good.

To ensure the system achieves its intended purpose, security features should be designed to be as intuitive and easy to use as possible. Computing professionals should discourage security precautions that are too confusing, are situationally inappropriate, or otherwise inhibit legitimate use.

In cases where misuse or harm are predictable or unavoidable, the best option may be to not implement the system.

3 Professional Leadership Principles

Leadership may either be a formal designation or arise informally from influence over others. In this section, "leader" means any member of an organization or group who has influence, educational responsibilities, or managerial responsibilities. While these principles apply to all computing professionals, leaders bear a heightened responsibility to uphold and promote them, both within and through their organizations.

A computing professional, especially one acting as a leader, should...

3.1 Ensure that the public good is the central concern during all professional computing work.

People—including users, customers, colleagues, and others affected directly or indirectly—should always be the central concern in computing. The public good should always be an explicit consideration when evaluating tasks associated with research, requirements analysis, design, implementation, testing, validation, deployment, maintenance, retirement, and disposal. Computing professionals should keep this focus no matter which methodologies or techniques they use in their practice.

3.2 Articulate, encourage acceptance of, and evaluate fulfillment of social responsibilities by members of the organization or group.

Technical organizations and groups affect broader society, and their leaders should accept the associated responsibilities. Organizations—through procedures and attitudes oriented toward quality, transparency, and the welfare of society—reduce harm to the public and raise awareness of the influence of technology in our lives. Therefore, leaders should encourage full participation of computing professionals in meeting relevant social responsibilities and discourage tendencies to do otherwise.

3.3 Manage personnel and resources to enhance the quality of working life.

Leaders should ensure that they enhance, not degrade, the quality of working life. Leaders should consider the personal and professional development, accessibility requirements, physical safety, psychological well-being, and human dignity of all workers. Appropriate human-computer ergonomic standards should be used in the workplace.

3.4 Articulate, apply, and support policies and processes that reflect the principles of the Code.

Leaders should pursue clearly defined organizational policies that are consistent with the Code and effectively communicate them to relevant stakeholders. In addition, leaders should encourage and reward compliance with those policies, and take appropriate action when policies are violated. Designing or implementing processes that deliberately or negligently violate, or tend to enable the violation of, the Code's principles is ethically unacceptable.

3.5 Create opportunities for members of the organization or group to grow as professionals.

Educational opportunities are essential for all organization and group members. Leaders should ensure that opportunities are available to computing professionals to help them improve their knowledge and skills in professionalism, in the practice of ethics, and in their technical specialties. These opportunities should include experiences that familiarize computing professionals with the consequences and limitations of particular types of systems. Computing professionals should be fully aware of the dangers of oversimplified approaches, the improbability of anticipating every possible operating condition, the inevitability of software errors, the interactions of systems and their contexts, and other issues related to the complexity of their profession—and thus be confident in taking on responsibilities for the work that they do.

3.6 Use care when modifying or retiring systems.

Interface changes, the removal of features, and even software updates have an impact on the productivity of users and the quality of their work. Leaders should take care when changing or discontinuing support for system features on which people still depend. Leaders should thoroughly investigate viable alternatives to removing support for a legacy system. If these alternatives are unacceptably risky or impractical, the developer should assist stakeholders' graceful migration from the system to an alternative. Users should be notified of the risks of continued use of the unsupported system long before support ends. Computing professionals should assist system users in monitoring the operational viability of their computing systems, and help them understand that timely replacement of inappropriate or outdated features or entire systems may be needed.

3.7 Recognize and take special care of systems that become integrated into the infrastructure of society.

Even the simplest computer systems have the potential to impact all aspects of society when integrated with everyday activities such as commerce, travel, government, healthcare, and education. When organizations and groups develop systems that become an important part of the infrastructure of society, their leaders have an added responsibility to be good stewards of these systems. Part of that stewardship requires establishing policies for fair system access, including for those who may have been excluded. That stewardship also requires that computing professionals monitor the level of integration of their systems into the infrastructure of society. As the level of adoption changes, the ethical responsibilities of the organization or group are likely to change as well. Continual monitoring of how society is using a system will allow the organization or group to remain consistent with their ethical obligations outlined in the Code. When appropriate standards of care do not exist, computing professionals have a duty to ensure they are developed.

Support ethical conduct of all computing professionals.

4 | Compliance with the Code

A computing professional should...

4.1 Uphold, promote, and respect the principles of the Code.

The future of computing depends on both technical and ethical excellence. Computing professionals should adhere to the principles of the Code and contribute to improving them. Computing professionals who recognize breaches of the Code should take actions to resolve the ethical issues they recognize, including, when reasonable, expressing their concern to the person or persons thought to be violating the Code.

4.2 Treat violations of the Code as inconsistent with membership in the ACM.

Each ACM member should encourage and support adherence by all computing professionals regardless of ACM membership. ACM members who recognize a breach of the Code should consider reporting the violation to the ACM, which may result in remedial action as specified in the ACM's Code of Ethics and Professional Conduct Enforcement Policy.

THE CODE AND GUIDELINES WERE DEVELOPED BY THE ACM CODE 2018 TASK FORCE:

Executive Committee:

Don Gotterbarn (Chair), Bo Brinkman, Catherine Flick, Michael S. Kirkpatrick, Keith Miller, Kate Varansky, and Marty J. Wolf.

Members:

Eve Anderson, Ron Anderson, Amy Bruckman, Karla Carter, Michael Davis, Penny Duquenoy, Jeremy Epstein, Kai Kimppa, Lorraine Kisselburgh, Shrawan Kumar, Andrew McGettrick, Natasa Milic-Frayling, Denise Oram, Simon Rogerson, David Shama, Janice Sipior, Eugene Spafford, and Les Waguespack.

The Task Force was organized by the ACM Committee on Professional Ethics. Significant contributions to the Code were also made by the broader international ACM membership. This Code and its guidelines were adopted by the ACM Council on June 22, 2018.

Case Studies

The cases presented in this section are fictionalized scenarios intended to illustrate how computing professionals can apply the Code as a framework for analyzing ethical dilemmas. These cases studies are designed for educational purposes to illustrate applying the Code to complex situations, and all names, businesses, places, events, and incidents are fictitious and are not intended to refer to actual entities.

In these analyses, we applied a four-step process denoted by the acronym **CARE: Consider** (stakeholders and consequences), **Analyze** (how the Code applies to the context), **Review** (possible actions), and **Evaluate** (decisions and future impact). The CARE framework provides an outline for judging whether possible actions in each case would be consistent with both the letter and the spirit of the Code. These questions establish a general approach to assist computing professionals in ethical decision-making.

- **Consider:** Who are the relevant actors and stakeholders? What were the anticipated and/or observable effects of the actions or decisions for those stakeholders? What additional details would provide a greater understanding of the situational context?
- **Analyze:** What stakeholder rights (legal, natural, or social) were impacted and to what extent? What technical facts are most relevant to the actors' decision? What principles of the Code were most relevant? What personal, institutional, or legal values should be considered?
- **Review:** What responsibilities, authority, practices, or policies shaped the actors' choices? What potential actions could have changed the outcomes?
- **Evaluate:** How might the decision in this case be used as a foundation for similar future cases? What actions (or lack of action) supported or violated the Code? Are the actions taken in this case justified, particularly when considering the rights of and impact on all stakeholders?

Michael S. Kirkpatrick
Education Coordinator, ACM Committee on Professional Ethics

Malware Disruption

Rogue Services advertised its web hosting services as "cheap, guaranteed uptime, no matter what." While some of Rogue's clients were independent web-based retailers, the majority were focused on malware and spam. Several botnets used Rogue's reliability guarantees to protect their command-and-control servers from take-down attempts. Spam and other fraudulent services leveraged Rogue for continuous delivery. Corrupted advertisements often linked to code hosted on Rogue exploiting browser vulnerabilities to infect machines with ransomware.

Case Study

1

Despite repeated requests from other ISPs and security organizations, Rogue refused to intervene with these services, citing their "no matter what" pledge to their customers. International pressure from other governments failed to induce national-level intervention, as Rogue was based in a country whose laws did not adequately proscribe such hosting activities. Given Rogue's non-compliance with these requests, a response team consisting of security vendors and government organizations created a prototype worm designed specifically to target Rogue's network and destroy the malicious services.

Consider: In deciding whether to proceed with the attack, the security response team needs to consider the impact on stakeholders that include Rogue's clients, those affected by the malware hosted on Rogue's systems, and others who rely on the services of Rogue's non-malicious clients. While the worm is intended to disrupt the malware hosting, it could disrupt the operation of non-malicious clients or escape Rogue's network, spreading to other ISPs. The worm could also prove to be ineffective and fail to achieve its aim, though alerting Rogue's malicious clients in the process. More information about Rogue's non-malicious clients would be beneficial, particularly whether they understood the nature of and risks caused by Rogue's malicious clients.

Analyze: Allowing Rogue's malicious clients' service to continue impacts the rights of individuals they harm, whereas Rogue's retailer clients have rights relating to the integrity and preservation of their data and business. Furthermore, Rogue's clients should have had transparent information of the risks associated with their business model. The most relevant portions of the Code are Principles 1.2 and 2.8, as the worm authors must consider whether the intentional harm to Rogue's systems is justified to support the public good.

Review: Rogue's policy of non-interference with their clients, coupled with their refusal to cooperate with takedown requests, shaped the choices of the security response team. Cooperation by Rogue or a more robust legal framework by their host country would have provided more options for a resolution that did not risk such harm.

Evaluate: This case highlights a key nuance of Principle 1.2. Given that the worm was designed with the specific intent of causing harm to Rogue's systems, the authors are obligated to ensure the harm is ethically justified. As the worm aims to shut down web services that are clearly harmful and malicious, the intent of the worm is consistent with the moral obligations identified in Principle 1.1. Additionally, the Code obligates the authors to minimize unintended harm by limiting the worm's effects solely to Rogue's systems. Rogue's other (non-malicious)

clients could rightfully object if their data is harmed, so the worm should include additional precautions to avoid this unintentional harm.

The worm also highlights the guidance in Principle 2.8. The worm will clearly access Rogue's systems in ways that are not authorized—destroying data in the process—but targeting known malicious software demonstrates a compelling belief that the service disruption was consistent with the public good. While there is a legitimate concern that such a worm could be manipulated as a precedent for someone seeking vigilante action, this case suggests how a computing professional should approach this work, by resorting to malicious actions only when other approaches are unsuccessful.

Historical context and additional discussion

This scenario is like a real incident that occurred in November 2008. McColo, a web hosting provider, had been responsible for a significant source of spam and malware. In contrast to the destructive worm described above, McColo's upstream provider severed their connection to the Internet. This action disrupted the operation of several of the world's largest botnets, as they had hosted their master servers on McColo.

The McColo takedown raises the question of what role ISPs and content providers should play in handling malicious content. Public repositories such as Github host the source code of many potentially malicious projects, including keyloggers and penetration testing tools. Social networking sites like Twitter and Reddit have been criticized in their handling of harassment, abuse, and objectionable content. On the other hand, Cloudflare, a content delivery network, terminated the account for the neo-Nazi Daily Stormer website. Given these disparate responses, the role of computing professionals in disrupting such services is not settled. Computing professionals in organizations that host third-party content should carefully reflect on how their services align with the principles of the Code, striving to ensure that their work supports the public good as the paramount consideration.

Linking Public Data Sets

Quinn is a member of a medical research team studying the role of genetic factors in psychological disorders, particularly focusing on how different variants influence social behavior. To facilitate this work, Quinn built a tool that linked three anonymized data sets: an anonymized set of genetic test results accessible only by medical researchers, a publicly available anonymized database of clinical diagnoses, and a custom database of public social networking posts. To preserve anonymity, the tool replaced all personally identifiable information in the social networking posts with quasi-identifiers. Quinn's team was granted approval for a study by their ethics review board (ERB), on the grounds that all data was anonymous and/or public, and all users had opted in to the data collection.

Case Study 2

While testing the tool, Quinn discovered a bug that incorrectly linked some records of multiple individuals as a single person. Given that the data sets were all anonymized, the team had accepted that such erroneous matches were likely to occur. The bug increased the expected number of such matches, but only slightly;

as such, the bug was classified as low priority. Quinn raised concerns that there may be other such bugs and suggested that the source code be released under an open source license to facilitate peer review of both the tool and the overall research.

Consider: Before releasing the code, Quinn and the team need to consider the impact on relevant stakeholders, particularly individuals whose records are contained in the data sets. When data sets are linked, re-identification of individuals is a common risk, which could lead to harm. Quinn would need to evaluate the merged data according to established anonymization metrics. Even more problematic, Quinn would need to consider how the merged data sets could be linked with other unknown data collections to break the existing anonymity.

Analyze: Quinn's team had a moral (and almost certainly a legal) responsibility to protect the human subjects of their research. Although they worked with their ERB as part of this process, making the tool publicly available—even while keeping the existing data private—introduces unpredictable risks of data re-identification. Individuals who opt into such data sets could not be expected to anticipate the risk of using their data in this way. The most relevant portions of the Code are Principles 1.2 and 1.6, though several other principles apply.

Review: Prior to releasing the source code in any way, Quinn's team should consult with their ERB regarding the risks. It is possible that the ERB members lack the technical expertise to determine that releasing the code is tantamount to releasing the merged data. Additionally, Quinn should consider alternative ways to do such peer review, such as making the code available only on request and under restricted terms.

Evaluate: Principle 1.2 warns against the harms that can be caused by data aggregation; Principle 1.6 re-emphasizes this point by stressing that merging data can strip privacy guarantees in the original sets. Principle 1.6 also suggests that the inaccuracies introduced by the bug must be fixed, and subjects must be adequately informed of the risks. In addition, the tool may facilitate the collection of data (such as metadata associated with the social networking activity) beyond the minimum amount necessary. Principle 2.5 also declares that the team must consider possible future risks associated with this tool and data use. In addition, Principles 2.1 and 2.4 obligate transparent communication with stakeholders, which would obligate informing both the ERB and all subjects of these risks. As such, publicly releasing the source code for this tool could cause harm and would be inadvisable.

The use of social networking posts also raises concerns in regard to Principle 2.8. Although these posts were publicly accessible, Quinn's team had no reasonable belief that using the data in this way was authorized. Some individuals' posts may have been made public because they did not understand the system's privacy controls. Even those who knowingly made their posts public would not have considered that these posts would be linked to genetic records.

Quinn's attempt to seek peer review is consistent with the intent of Principles 2.2 and 2.4. In recognizing the potential for bugs in the tool, Quinn sought input from other computing professionals; however, given the risks involved, a more discreet form that did not involve a completely public release would have been recommended. It is not clear whether Quinn had sufficient training in data anonymization techniques; if not, the guidance of Principle 2.2 suggests that Quinn should not have developed the tool without acquiring these technical competencies.

Historical context and additional discussion

There have been many examples of anonymized public data sets leading to leakage of private information. In the late 1990s, Latanya Sweeney demonstrated that combining an anonymized hospital discharge data set with public voting registration records could allow for the re-identification of individual patients. A 2001 study by Salvador Ochoa and others re-identified Chicago homicide victims by combining records with the Social Security Death Index. Arvind Narayanan and Vitaly Shmatikov used the 2010 Netflix Prize machine learning competition data to re-identify individuals by combining it with information from the Internet Movie Database (IMDb). The Australian Department of Health published a data set in 2016 that leaked private health records when linked to a date of birth or medical procedures. In 2017, Malte Möser et al. demonstrated how to use web trackers and other techniques to break the anonymity of blockchain cryptocurrencies, such as Bitcoin and Monero.

As these cases show, linking anonymized data sets with other records—some of which are publicly accessible—can lead to re-identifying individuals. Computing professionals should be especially cognizant of these risks and raise awareness of these issues with their respective teams. In particular, computing professionals who build tools that facilitate this linkage are compelled to evaluate these possible outcomes and take precautions to minimize potential harm.

Medical Implant Risk Analysis

Corazón is a medical technology startup that builds an implantable heart health monitoring device. The device comes with a smart phone app that monitors and controls the device wirelessly, as well as stores a persistent record that can be shared with medical providers. After being approved by multiple countries' medical device regulation agencies, Corazón quickly gained market share based on the ease of use of the app and the company's vocal commitment to securing patients' information. To further expand their impact, Corazón worked with several charities to provide the device at a reduced price to patients living below the poverty line.

Case Study 3

As a basic security mechanism, Corazón's implant could only be accessible through short-range wireless connections, requiring the phone and implant to be in close proximity. Data transferred between the app and the device employed standard cryptographic algorithms, and all data stored on the phone was encrypted. To support on-going improvement, Corazón had an open bug bounty program inviting disclosure of potential vulnerabilities in their app.

At a recent security conference, an independent researcher claimed to have found a vulnerability in the wireless connectivity. The researcher presented a proof-of-concept demonstration where a second device in close proximity could modify commands sent to the implant to force a device reset. The attack relied on the use of a hard-coded initialization value stored in the implant device that created a predictable pattern in the data exchanges that could be manipulated. In

consultation with Corazón's technical leaders, the researcher concluded that the risk of harm with this attack is negligible, given the limited capabilities of the device.

ANALYSIS SUMMARY:
Corazón's practices embody the goals of several principles in the Code. Corazón's products and their charity work contribute to society and to human well-being, consistent with the aims of Principle 1.1. In addition, their rigorous approach to design, validation, and maintenance exemplifies Principle 3.1, holding the public good as the central concern within their processes. By working within governmental regulation agencies, Corazón demonstrated a commitment to Principle 2.3. Corazón's use of cryptography and vulnerability disclosure practices adheres to the robust security goals of Principle 2.9. Furthermore, Corazón's reliance on standard cryptographic algorithms—rather than attempting to devise an unproven proprietary technique—shows commitment to Principle 2.6, restricting their developers' work to areas of competence.

Corazón's consultation with the researcher also highlights a key aspect of Principle 2.5. The design and implementation of Corazón's products exhibit a commitment to comprehensive and thorough risk analysis. Furthermore, Corazón welcomed independent security evaluation to identify additional issues that their designers overlooked. Once a potential vulnerability was discovered, Corazón acted responsibly and quickly to determine the scope of the flaw with the aim of mitigating the harm.

One area of concern regarding Corazón's design is the use of a hard-coded value in the implant. Given the nature of the device, fixing this design choice would be difficult if it proved necessary. However, there is insufficient evidence at this point to determine the scope of the risk induced by this design.

Corazón's on-going commitment to security and improvement also exemplifies an important aspect of Principle 3.7. Corazón's rapid success in this specialized healthcare field is an instance of the integration of technology into the infrastructure of society. Recognizing the increased stewardship required by this Principle, Corazón began working with charities to serve individuals whose poverty may have excluded them from access.

Abusive Workplace Behavior

Diane recently started a new industry research job, joining the company's interactive technologies team. In graduate school, her advisor had collaborated with several members of the team on a few research projects, involving and highlighting Diane's contributions whenever possible. The team had been impressed by Diane's work and recruited her as she was approaching graduation.

Case Study
4

Max, the team's technical leader, had built a reputation as a brilliant yet mercurial expert in augmented reality. His team's contributions were highly cited within the field, with Max typically claiming primary authorship as the team leader. Their work was also highlighted frequently in the popular press, always with quotes only from Max. Despite the team's repeated successes, Max would erupt with verbal and personal attacks for even minor mistakes. He would yell at the person and berate

them in internal chat forums. On multiple occasions, team members—only the women—have found their names removed from journal manuscript submissions as punishment.

Diane soon found herself the target of one of Max's tirades when she committed a code update that introduced a timing glitch in the prototype shortly before a live demo. Infuriated, Max refused to allow Diane to join the team onstage. Feeling Max's reaction was unprofessional and abusive, Diane approached the team's manager, Jean, who must consider how to respond.

ANALYSIS SUMMARY:
Max's abusive behavior clearly violates several principles in the Code. His verbal abuse violated both Principles 1.1 and 1.2, by failing to maintain a safe social environment and failing to adhere to high standards of professional communication. By removing names from journal submissions and blocking Diane from appearing onstage, Max violated these team members' rights to credit for their work, violating Principle 1.5. Max's retaliation also demonstrates a violation of Principle 1.4. His punitive actions of removing names and blocking participation show a history of targeting only women team members. This behavior is a clear abuse of power that limits these team members' fair access to the work environment.

Section 3 of the Code provides Jean with guidance on how to respond in this case. Principle 3.3 obligates leaders to provide for the psychological well-being and human dignity of the team. In addition, Principle 3.4 has leaders articulate, apply, and support policies that reflect the principles of the Code. Allowing Max's behavior to continue unchallenged would fail to achieve this standard. Consequently, Jean must address Max's behavior and support Diane's objection.

Malicious Input to Content Filters

The U.S. Children's Internet Protection Act (CIPA) mandates that public schools and libraries employ mechanisms to block inappropriate material that is deemed harmful to minors. Blocker Plus is an automated Internet content filter designed to help these institutions comply with CIPA's requirements. To accomplish this task, Blocker Plus has a centrally controlled blacklist maintained by the software maker. In addition, Blocker Plus provides a user-friendly interface that makes it a popular product for home use by parents.

Case Study
5

Due to the challenge of continually updating the blacklist, the makers of Blocker Plus began to explore machine learning techniques to automate the identification of inappropriate content. During the development of these changes, Blocker Plus combined input from both home and library users to aid in the classification of content. Pleased with their initial results, Blocker Plus deployed these techniques in their production system. Furthermore, Blocker Plus continued to collect input from users to refine their learned models.

During a recent review session, the development team reviewed several recent complaints about content being blocked inappropriately. An increasing amount of content regarding gay and lesbian marriage, vaccination, climate change,

and other topics not covered by CIPA, had been added to the blacklist. Initial investigations into these incidents suggested that some activist groups had exploited Blocker Plus's feedback mechanism to provide input that corrupted the classification model.

ANALYSIS SUMMARY:
Blocker Plus is a system designed to block content legally designated as harmful to children. While this filtering constitutes a form of censorship, children are considered a protected vulnerable class. To reduce the impact on adults, CIPA also mandates that these filters must be disabled on request. Given that Blocker Plus is complying with U.S. federal regulations to facilitate socially responsible uses of computers, the system is consistent with Principles 1.1 and 2.3.

Given the complexity and risk involved in Blocker Plus's use of machine learning techniques, Principle 2.5 calls for extraordinary care. Principle 2.9 suggests that Blocker Plus should have included better protections against the intentional misuse by the activist groups. Blocker Plus's deployment of machine learning causes harm by suppressing information of legitimate public interest and safety, as well as by discriminating based on sexual orientation, raising concerns for both Principles 1.2 and 1.4. In addition, Blocker Plus provides an example of a system becoming integrated into the educational infrastructure of society. Principle 3.7 emphasizes that the developers of such systems have an added responsibility to provide good stewardship and Blocker Plus must correct these issues.

Additional Resources

ACM Code of Ethics and Professional Conduct
https://www.acm.org/code-of-ethics

Código de Ética y Conducta Profesional de ACM
https://www.acm.org/código-de-ética

计算机协会道德与职业行为准则
https://www.acm.org/code-of-ethics/the-code-in-chinese

ACM Committee on Professional Ethics (COPE)
https://ethics.acm.org/

Resources for using the Code
https://ethics.acm.org/using-the-code/

Case Studies on how the Code can be applied
https://ethics.acm.org/case-studies/

Ask an Ethicist advice column
https://ethics.acm.org/integrity-project/ask-an-ethicist/

ACM Code of Ethics Enforcement Procedures
https://www.acm.org/code-of-ethics/enforcement-procedures