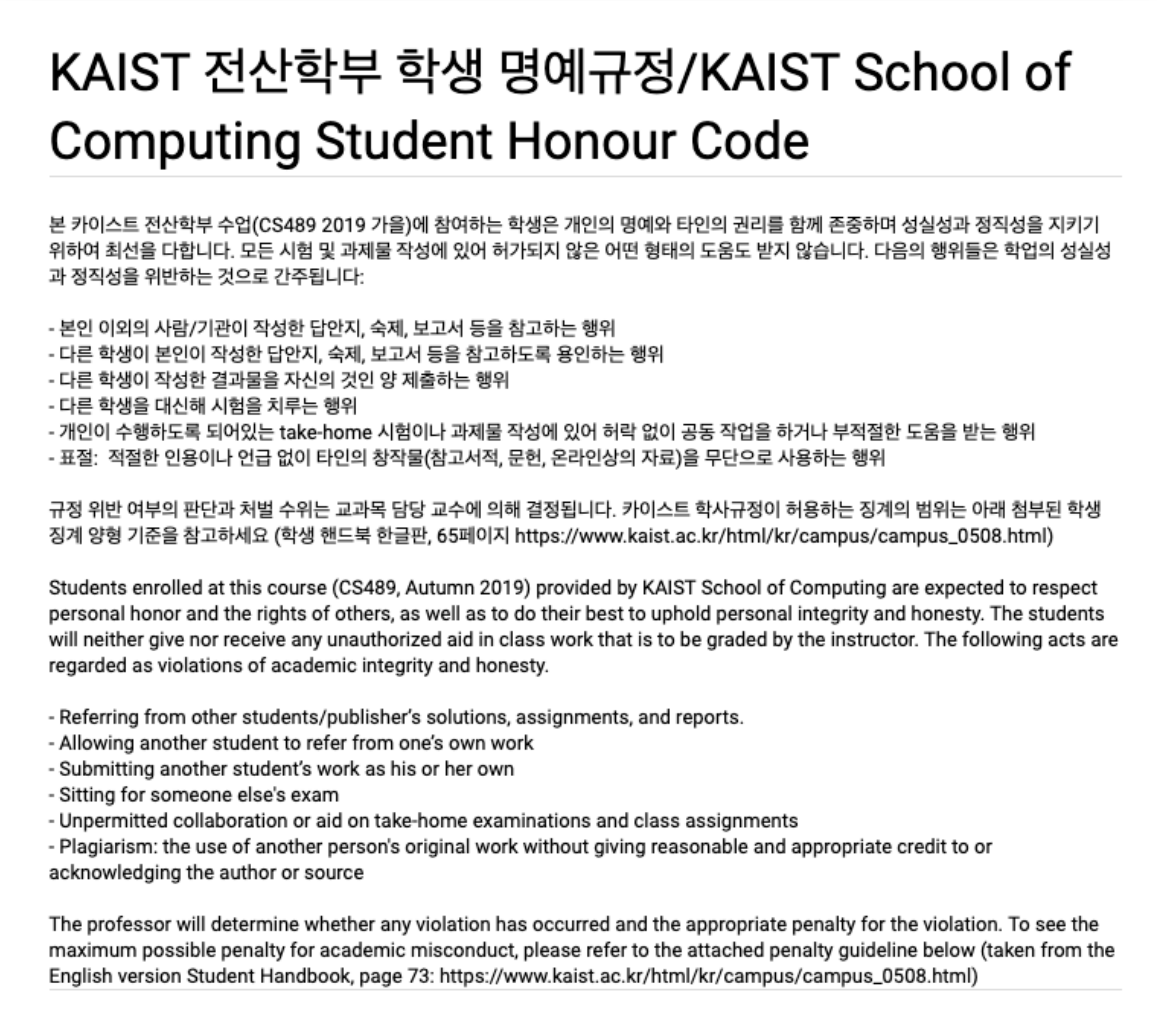
Professional Computer Ethics

CS489
Shin Yoo

Quick Advertisement

Sign up, or I am not grading your assignments (seriously).



KAIST 전산학부 학생 명예규정/KAIST School of Computing Student Honour Code

본 카이스트 전산학부 수업(CS489 2019 가을)에 참여하는 학생은 개인의 명예와 타인의 권리를 함께 존중하며 성실성과 정직성을 지키기 위하여 최선을 다합니다. 모든 시험 및 과제물 작성에 있어 허가되지 않은 어떤 형태의 도움도 받지 않습니다. 다음의 행위들은 학업의 성실성과 정직성을 위반하는 것으로 간주됩니다:

- 본인 이외의 사람/기관이 작성한 답안지, 숙제, 보고서 등을 참고하는 행위
- 다른 학생이 본인이 작성한 답안지, 숙제, 보고서 등을 참고하도록 용인하는 행위
- 다른 학생이 작성한 결과물을 자신의 것인 양 제출하는 행위
- 다른 학생을 대신해 시험을 치루는 행위
- 개인이 수행하도록 되어있는 take-home 시험이나 과제물 작성에 있어 허락 없이 공동 작업을 하거나 부적절한 도움을 받는 행위
- 표절: 적절한 인용이나 언급 없이 타인의 창작물(참고서적, 문헌, 온라인상의 자료)을 무단으로 사용하는 행위

규정 위반 여부의 판단과 처벌 수위는 교과목 담당 교수에 의해 결정됩니다. 카이스트 학사규정이 허용하는 징계의 범위는 아래 첨부된 학생 징계 양형 기준을 참고하세요 (학생 핸드북 한글판, 65페이지 https://www.kaist.ac.kr/html/kr/campus/campus_0508.html)

Students enrolled at this course (CS489, Autumn 2019) provided by KAIST School of Computing are expected to respect personal honor and the rights of others, as well as to do their best to uphold personal integrity and honesty. The students will neither give nor receive any unauthorized aid in class work that is to be graded by the instructor. The following acts are regarded as violations of academic integrity and honesty.

- Referring from other students/publisher's solutions, assignments, and reports.
- Allowing another student to refer from one's own work
- Submitting another student's work as his or her own
- Sitting for someone else's exam
- Unpermitted collaboration or aid on take-home examinations and class assignments
- Plagiarism: the use of another person's original work without giving reasonable and appropriate credit to or acknowledging the author or source

The professor will determine whether any violation has occurred and the appropriate penalty for the violation. To see the maximum possible penalty for academic misconduct, please refer to the attached penalty guideline below (taken from the English version Student Handbook, page 73: https://www.kaist.ac.kr/html/kr/campus/campus_0508.html)

Profession

- Originally referred to the commitment to a religious order - early universities drew most of their faculty from religious orders, hence teachers are called “professors”, i.e., those who profess (religious beliefs)

- Then it evolved to mean “gentlemen’s occupation” built around guilds

- Nowadays: *“a paid occupation, especially one that involves prolonged training and a formal qualification”*

Formal Qualification?

- Chartered Engineer (UK): an accredited Master of Engineering degree and 4+ years of field experience after graduation qualifies you to be peer-reviewed
    - British Computer Society is in charge of software engineers
- Professional Engineer/Engineer (Korea): government-led hierarchy of professional license
    - Engineer Information Processing
    - Professional Engineer Computer System Application

Requirements of a Professional

- Highly developed skills and deep domain knowledge
- Autonomy: you are supposed to know better (than the client) and make the right decision
- Observance of a code of conduct
  - Professional / personal / institutional / community

ACM Code of Ethics and Professional Conduct

- Association for Computing Machinery: established in 1947, the largest scientific and educational computing society (currently over 100,000 student/professional members)

- Executive Council voted to adopt a Code of Ethics in 1992: 24 imperatives that define the personal responsibilities of computing professionals.

- The latest version was created in 2018: https://www.acm.org/code-of-ethics

Are 24 sufficient?

“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.”

1. General Ethical Principles: A computing professional should…

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

2. Avoid harm.

3. Be honest and trustworthy.

4. Be fair and take action not to discriminate.

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

6. Respect privacy.

7. Honor confidentiality.

2. Professional Responsibilities: A computing professional should…

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

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

3. Know and respect existing rules pertaining to professional work.

4. Accept and provide appropriate professional review.

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

2. Professional Responsibilities: A computing professional should…

6. Perform work only in areas of competence.

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

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

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

3. Professional Leadership: A computing professional, especially one acting as a leader, should…

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

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

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

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

3. Professional Leadership: A computing professional, especially one acting as a leader, should…

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

6. Use care when modifying or retiring systems.

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

4. Compliance with the Code: A computing professional should…

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

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

Case Studies

Read each of the following scenarios, and point out the relevant parts of ACM Code of Ethics and Professional Conduct

(all taken from https://ethics.acm.org/code-of-ethics/using-the-code/)

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 to exploit browser vulnerabilities to infect machines with ransomware.

Despite repeated requests from major ISPs and international organizations, Rogue refused to intervene with these services, citing their “no matter what” pledge to their customers. Furthermore, 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.

Ultimately, Rogue was forcibly taken offline through a coordinated effort from multiple security vendors working with several government organizations. This effort consisted of a targeted worm that spread through Rogue’s network. This denial-of-service attack successfully took Rogue’s machines offline, destroying much of the data stored with the ISP in the process. All of Rogue’s clients were affected. No other ISPs reported any impact from the worm, as it included mechanisms to limit its spread. As a result of this action, spam and botnet traffic immediately dropped significantly. In addition, new infections of several forms of ransomware ceased.

Analysis

- Rogue violated 1.1 (contribute to society and human well being) and 1.2 (avoid harm).

- Rogue was complicit in violating 2.8 (access computing and communication resources only when authorised or when compelled by the public good)

- Rogue violated 3.1 (ensure that the public good is the central concern)

Dark UX Patterns

The change request Stewart received was simple enough: replace the web site's rounded rectangle buttons with arrows and adjust the color palette to one that mixes red and green text. But when Steward looked at the prototype, he found it confusing. The left arrow suggested that the web site would go back to a previous page or cancel some action; instead, this arrow replaced the button for accepting the company's default product. The right arrow, on the other hand, upgraded the user to the more expensive category; it also silently added a protection warranty without asking for confirmation. Stewart suggested to his manager that this confusing design would probably trick users into more expensive options that they didn't want. The response was that these were the changes requested by the client.

Shortly after the updates were released into their production system, Stewart's team was invited to a celebration. As a result of these changes, revenues at their client had increased significantly over the previous quarter. At the celebration, Stewart overheard some of the client's managers discussing the small increase for refunds by users who claimed that they didn't want the protection plan, but there weren't many. One manager noted several complaints from visually impaired users, who noted that the mixture of red and green text obscured important disclaimers about the product. "So what you're saying, then, is that the changes worked as planned," quipped one of the managers.

Analysis

- Max violated 1.1 (contribute to society and human well being), and also failed to comply to 2.2 (maintain high standard of professional competence, conduct, and ethical practice).

- Also 1.5 (respect the work required to produce new ideas, inventions, creative works, and artefacts)

- Also 1.4 (be fair and take action not to discriminate)

- Jean failed to live up to 3.3 (manage personnel and resources to enhance the quality of working life) and 3.4 (articulate, apply, and support the policies and processes reflecting the Code)

Abusive Workplace Behaviour

Diane recently started a new industry research job, joining the interactive technologies team. In graduate school, her advisor had collaborated with several members of the team on a number of 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.

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 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, women team members 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 on stage. Feeling Max's reaction was unprofessional and abusive, Diane approached the team's manager, Jean. Jean agreed that the experience was unpleasant, but that was the price to pay for working in an intense, industry-leading team. Jean's advice to Diane was to "Grow up and get over it."

Analysis

- The client failed to comply to 1.2 (avoid harm) by intentionally harming their users; failed to adhere to 2.2 (maintain high standards of professional conduct)

- By removing names and blocking Diane from appearing on the stage, Max also violated 1.5 (respect the work required to produce new ideas)

- If removal of names was targeted towards women, Max also violated 1.4 (no discrimination)

- As the leader, Jean failed to comply to 3.3 (manage personnel to enhance the quality of working life) and 3.4 (articulate, apply, and support the Code)

2015 San Bernardino Attack and Encryption Row

- On 2 December 2015, there was a mass shooting in San Bernardino, California: 14 were killed, 22 seriously injured (see https://en.wikipedia.org/wiki/2015_San_Bernardino_attack#Motive for details)

- This incident has put the tension between governments and commercial encryption technology in the highlight.

Phone Decryption

- On 9 February 2016, FBI accounted that it cannot unlock the phone used by one of the shooters (iPhone 5C), and asked Apple to create a special version of iOS that opens a back-door

- Apple declined.

- FBI successfully issued a court order, with the deadline of 26 February 2016.

- Apple still declined.

- On 19 February 2016, DoJ asked Apple to install a malware inside Apple's campus, to allow FBI to remotely hack the phone.

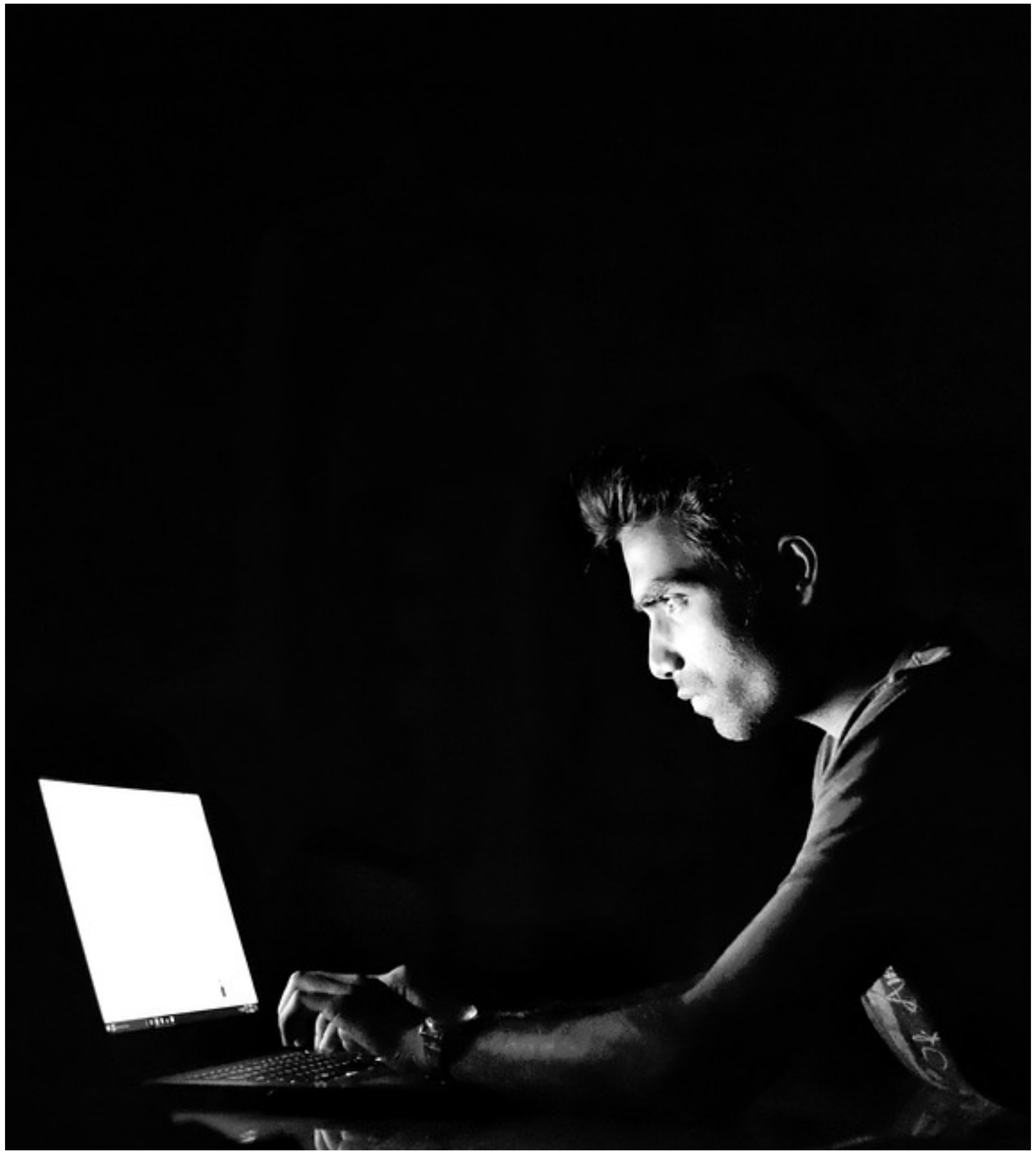
- Apple declined, and announced that, while the company initially cooperated with FBI, one of the promising methods has been rendered useless due to an earlier mistake.

Phone Decryption

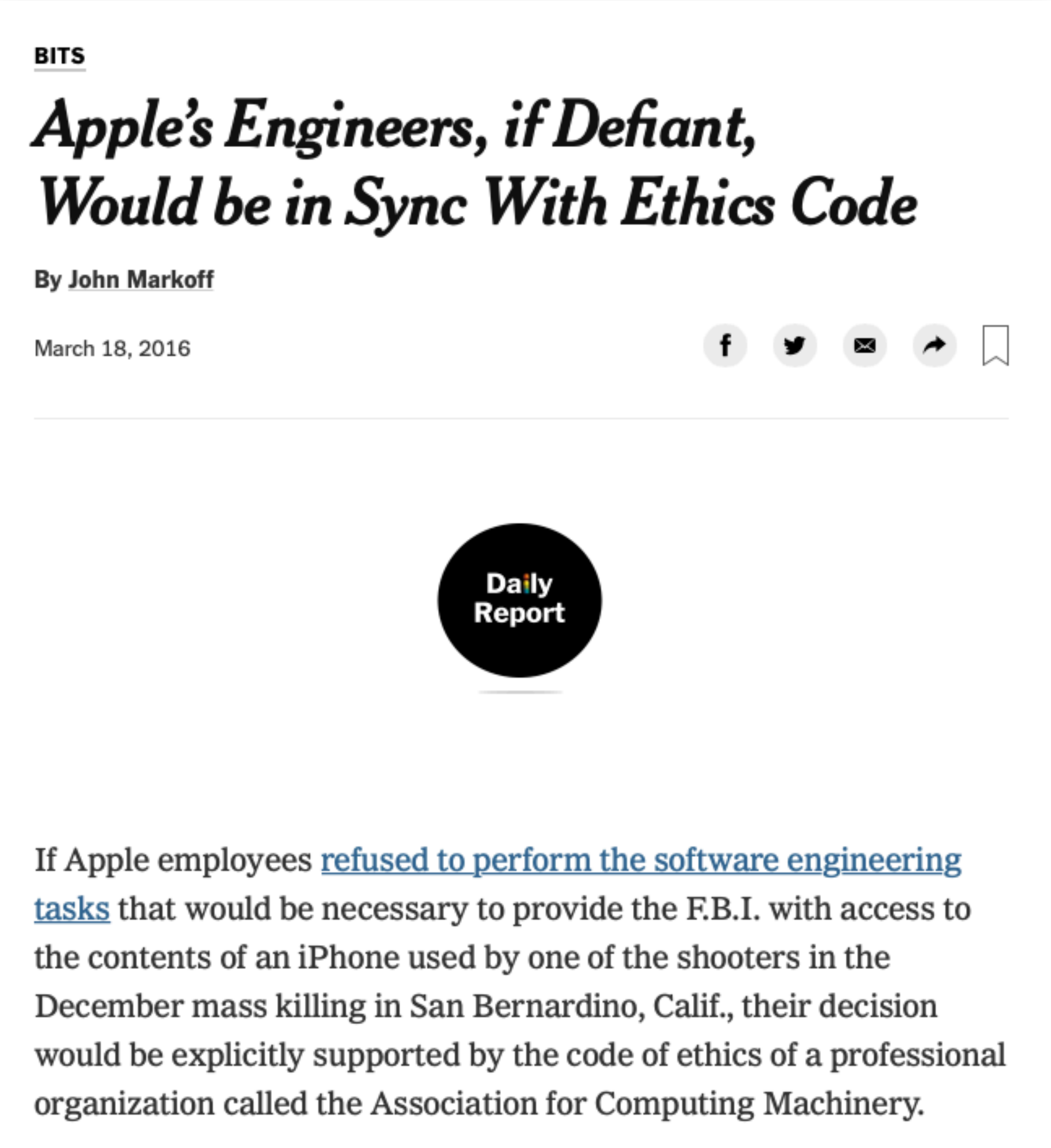
- On 28 March 2016, DoJ announced that it unlocked the iPhone, and dropped the suit against Apple.
    - Some claim that an Israeli company, Cellebrite, helped FBI. There are reports that FBI worked with hackers who exploited a zero-day vulnerability.
- In March 2018, LA Times reported that there was nothing useful for investigation in the phone.

Should Apple have complied?

- Back in 2016, 45% of Americans supported Apple's stance, while 50% supported FBI.
- Do you support Apple, or the US Government?
- Does ACM Code of Ethics have a relevant point here?
- #discussions



https://www.nytimes.com/2016/03/19/technology/apples-engineers-if-defiant-would-be-in-sync-with-ethics-code.html



BITS

Apple's Engineers, if Defiant, Would be in Sync With Ethics Code

By John Markoff

March 18, 2016

If Apple employees refused to perform the software engineering tasks that would be necessary to provide the F.B.I. with access to the contents of an iPhone used by one of the shooters in the December mass killing in San Bernardino, Calif., their decision would be explicitly supported by the code of ethics of a professional organization called the Association for Computing Machinery.

Recommended Reading

- NRP: A Year After San Bernardino And Apple-FBI, Where Are We On Encryption? (https://www.npr.org/sections/alltechconsidered/2016/12/03/504130977/a-year-after-san-bernardino-and-apple-fbi-where-are-we-on-encryption)

- NPR: Judges Have More Power in Granting Warrants to Hack Digital Devices (https://www.npr.org/sections/thetwo-way/2016/12/01/503929928/judges-have-more-power-in-granting-warrants-to-hack-digital-devices)

- Chapter 6: Crypto-Anarchy, *People vs. Tech*, Jamie Bartlett

Whistle-blower

- *n.* a person who informs on a person or organization regarded as engaging in an unlawful or immoral activity.

- Internal conflict: a whistle-blower often knows that his/her alarms pose a threat to anyone who benefits from the ongoing practice

- External conflict: common ethics require loyalty to your profession, but formal code of professional ethics stress responsibility to the public

BART Braking System

- San Francisco Bay Area Rapid Transit (BART) System was opened in 1972. However, in 1969, three engineers who worked on the control system got concerned about its safety. They talked to their supervisors, individually, to no avail. Subsequently they got to know each other, and continued to speak to the management, who ignored them.

- Finally, they interested a member of BART's board of trustees, who brought it up at the meeting. The effort failed, too. After this, all three got fired without any explanation.

- Meanwhile, BART was opened, and the braking system started to malfunction: BART began using human flag system.

- Three engineers turned to California Society of Professional Engineers, who investigated their claims and arrived at the same conclusion. CSPE went to the state government, who also arrived at the same conclusion.

- Three engineers sued BART in 1974, but settled outside the court. Their names got cleared, but they found it difficult to find new jobs and suffered considerable financial damage.

Three Elements of Whistle-Blowing (S. Bok, 1982)

- **Dissent**: whistle-blower publicly disagrees with an authority, or a majority view, usually to highlight a negligence or abuse

- **Breach of Loyalty**: whistle-blower goes against his/her own team, violating the obligation to colleagues

- **Accusation:** whistle-blower is effectively singling out a person or a group to call foul

Secrets: On the Ethics of Concealment and Revelation, Sissela Bok, 1982

Individual Moral Choices

- Certain issues are so outrageous that anyone in the position to warn the public almost have to do so, while other matters are so minor that whistle-blowing may be a disproportionate reaction.

- In the middle likes the wide spectrum of matters that will trouble the whistle-blower.

- The three elements provide guildelines.

Individual Moral Choices

- Of dissent, you need accuracy: can you justify your action with sufficient evidence or expertise? Or do you simply have suspicion? Have you considered the damage a false alarm can do?

- Of breach of loyalty, you need careful consideration of alternatives: have you tried to resolve the issue internally? If resolved internally, you remain loyal to both your profession and the public.

- Of accusation, you need fairness: are you really pointing your finger at the right person?s

What does the Code say?

- 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.**

Concluding Thoughts

- What would you have done if you were at Cambridge Analytica or Facebook?
-