Conflicting Guidelines in the ACM Code of Ethics:

Guideline 1.2 and Guideline 2.6

The Association for Computing Machinery’s (ACM’s) code of ethics and professional conduct specifies several ethical guidelines that members should follow in their professional computing pursuits. However, there are certain professional situations that might force an ACM member to choose between two conflicting guidelines. For example, guideline 1.2 states that members will “avoid harm to others.” The principle states that computing professionals should avoid completing any activities that lead to the, “undesirable loss of information, loss of property, property damage,” or that, “result in harm to … users.” Later in the code of ethics, guideline 2.6 specifies that its members must “honor contracts, agreements, and assigned responsibilities.”1 The two guidelines do not directly contradict one another. However, consider the event that an ACM member’s employer requests the modification of software in such a way that contradicts a security feature that was promised to users. The ACM member must choose between avoiding harm to users and completing the assigned tasks. By modifying software in such a way that undermines security features that users believed were in place when they used a particular software, the ACM member is harming the users. For example, the ACM member could be asked to modify an operating system for a laptop computer or for a smart device, a widely-used email system, a cloud storage platform, or a different type of software. Regardless, the users’ personal information, conversations, or data might then be unsafe.

Guideline 1.2 states that the member must, “carefully consider potential impacts on all those affected by decisions made during design and implementation.” In the case of the development of a “backdoor” through a software’s security features, the designer must consider potential detrimental effects to users such as loss of privacy or security in data storage or personal information. The designer may then take steps to reduce the harmful effects of such a software modification; guideline 2.6 specifies that the designer may compile his or her concerns about the implications of the assignment into a “judgment”, and present the judgment to his or her employer or contractor in an attempt to redesign the assignment to alleviate some of the negative implications for users. However, in the event that that judgment is rejected by the employer or contractor, the member, “may yet be obligated, by contract or by law, to proceed as directed,” according to guideline 2.6.1 At that point, the designer is forced to choose between completing the work assigned to him or her, and not developing (or modifying, in this case) software that could be detrimental to users.

Apple is currently facing a dilemma similar to the generalized scenario described above. Recently, the FBI has requested that Apple build a backdoor into the iPhone to aid in the FBI’s investigation into the couple responsible for the San Bernadino terror attack. Apple has refused, recognizing the implications of building such a software. Apple CEO Tim Cook stated, “In the wrong hands, this software … would have the potential to unlock any iPhone in someone’s physical possession.”2 However, the FBI has gotten a court order demanding that Apple comply with their request. While there are legal implications as well as ethical implications involved in the development of the software, the company will have to choose between avoiding harm to its users and honoring (complying with) a contract (court order).

References

1ACM code of ethics and professional conduct. (n.d.). Retrieved February 23, 2016, from Association for computing machinery website: http://www.acm.org/about-acm/

acm-code-of-ethics-and-professional-conduct

2Thielman, S. (2016, February 20). Apple v the FBI: What's the beef, how did we get here and what's at stake? *The Guardian*. Retrieved from http://www.theguardian.com/technology/

2016/feb/20/apple-fbi-iphone-explainer-san-bernardino