To: All Educational Toy Division Engineers  
From: Grace Hopper  
       Chief Executive Officer  
Subject: Ethics presentations  
Date: March 25, 2019  

Introduction  
As part of our ongoing effort to attain excellence in all aspects of engineering, the human resources department of Little Toy Blue is sponsoring a forum on April 8, 2019 to discuss ethics in engineering. At that forum, each team will present to the class an ethical issue relating to computer technology. The purpose of this memo is to describe your presentation.

Presentation Details  
Each team presentation should:

- describe a computer technology  
- describe an ethical issue or societal implication related to that technology  
- describe the categories of people affected by that issue (stakeholders) and how the issue affects each person  
- describe a range of policies or positions one could take on that issue  
- recommend a particular policy or position, and give support for that recommendation

Your team will have three minutes to make its presentation, plus another three minutes for class discussion. Because this is such a small amount of time, we recommend that one student from the team make the entire presentation. However, all students on the team should contribute to the development of the ideas. Presentations will be made without a projector (i.e., no PowerPoint slides).
Suggested Topics
Below are some suggested topics. Your team may also choose a topic that is not on the list, as long as the topic is related to computer technology.

- The FBI obtained a court order requiring Apple to help them gain access to an iPhone owned by San Bernadino shooter Syed Farook, but Apple is contesting the court order.
- Bitcoins can be used to facilitate money laundering and other illegal activity.
- Censorship and surveillance in China is enabled in part by cooperation by major search engines. Google decided to take down its site in China rather than continue participating in this censorship.
- E-mail providers reserve the right to read e-mails under some circumstances. For example, Microsoft recently read the HotMail account of a blogger while pursuing an investigation into a leak of confidential software.
- Human-rights advocates and political protesters disseminate information via social media sites. These sites must formulate policies about what is acceptable speech and content.
- The Stop Online Piracy Act (SOPA) bill was intended to reduce copyright infringement by restricting access to Internet sites that contain pirated material.
- Data mining techniques can be used to discover sensitive information (e.g., medical records) about individuals, even from databases that have been scrubbed of explicit identifiers.
- Personalized news feeds can prevent people from being exposed to viewpoints different than their own.
- Apple restricts which software can run on iPhones, but it is possible to "unlock" the device so it can run unsupported software.
- Some mobile device applications help people avoid law-enforcement activities, such as drunk-driving checkpoints or speedtraps.
- Some mobile device applications help people track the location of police officers, and this may endanger those officers. Ismaaiyl Brinsley allegedly used Waze to track the location of the NYPD officers he shot.
- There is a market for buying and selling discoveries of security vulnerabilities in popular software. Should security researchers participate in this market?
- Some computer games are addictive or encourage violent behavior.
- It is common for software manufacturers to ship software with serious, known bugs.
- Loud volumes on iPods can hurt people's hearing.
- Many people don't apply security updates, and their computers are often compromised and used for criminal activity.
• Facial recognition was used at Super Bowl XXXV to look for criminals.
• Web sites collect and share data about consumer behavior to deliver customized ads.
• Computer security researchers have discovered ways to break into electronic voting machines and change the outcome of elections.
• Peer-to-peer file sharing networks are used primarily to pirate copyrighted material.
• Peer-to-peer file sharing networks make it difficult to censor objectionable material.
• People surf the web via unsecured wireless networks (wardriving).
• Encryption algorithms may be required to have a “backdoor” that enables the government to decrypt data.
• Trusted Platform Module (TPM) can be used for digital rights management (DRM) to identify and restrict which software you run on your computer.
• Legal restrictions (e.g., Child Online Protection Act) and filtering technologies are alternative solutions for protecting minors from harmful material on the Internet.